MPLS Working Group	M. Vigoureux, Ed.
Internet-Draft	Alcatel-Lucent
Intended status: Standards Track	D. Ward, Ed.
Expires: December 30, 2009	Cisco Systems, Inc.
	M. Betts, Ed.
	Huawei
	June 28, 2009

Requirements for OAM in MPLS Transport Networks
draft-ietf-mpls-tp-oam-requirements-02

Status of this Memo

Copyright Notice

Abstract

This document lists the requirements for the Operations, Administration and Maintenance functionality of MPLS Transport Profile. These

requirements apply to pseudowires, Label Switched Paths, and Sections. Architectural and functional requirements are covered in this document.

Table of Contents

---

1. Introduction

TOC

In the context of MPLS Transport Profile (MPLS-TP, see [5] (Bocci, M., Bryant, S., Frost, D., Levrau, L., and L. Berger, “A Framework for MPLS in Transport Networks,” April 2010.) and [6] (Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., and S. Ueno, “MPLS-TP Requirements,” August 2009.)), the rationales for Operations, Administration and Maintenance (OAM) mechanisms are twofold as they can serve:

* 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 with this use case.

* as a service-oriented mechanism (used by a transport service provider) to monitor services offered 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 Service Level Agreements (SLAs) parameters (e.g., using performance monitoring) negotiated with the end customers. Note that a transport service could be provided over several networks or administrative domains that may not all be 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:

* the reduction of operational complexity and costs, by allowing for efficient and automatic detection, localisation, handling, and diagnosis of defects, and by minimizing service interruptions and operational repair times.

* the enhancement of network availability, by ensuring that defects, for example resulting in misdirected customer traffic, and faults, are detected, diagnosed and dealt with before a customer reports the problem.

* meet service and performance objectives, as the OAM functionality allows for SLA verification in a multi-maintenance domain environment and allows for the determination of service degradation due, for example, to packet delay or packet loss.

This document lists the requirements for the OAM functionality of MPLS-TP. These requirements apply to pseudowires (PWs), Label Switched Paths (LSPs), and Sections.
These requirements are derived from the set of requirements specified by ITU-T and published in the ITU-T Supplement Y.Sup4 [7] (ITU-T Supplement Y.Sup4, “ITU-T Y.1300-series: Supplement on transport requirements for T-MPLS OAM and considerations for the application of IETF MPLS technology,” 2008.).
By covering transport specificities, these requirements complement those identified in RFC 4377 [8] (Nadeau, T., Morrow, M., Swallow, G., Allan, D., and S. Matsushima, “Operations and Management (OAM)

Requirements for Multi-Protocol Label Switched (MPLS) Networks," February 2006.).

Note that the OAM functionalities identified in this document may be used for fault management, performance monitoring and/or protection switching applications. For example, connectivity verification can be used for fault management application by detecting failure conditions, but may also be used for performance monitoring 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 functionality should be used for which application.

1.1. Requirements Language and Terminology

TOC

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] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.).

In this document we refer to the inability of a function to perform a required action, as a fault. This does not include an inability due to preventive maintenance, lack of external resources, or planned actions. See also ITU-T G.806 [2] (ITU-T Recommendation G.806, "Characteristics of transport equipment - Description methodology and generic functionality," 2009.).

In this document we refer to the situation in which the density of anomalies has reached a level where the ability to perform a required function has been interrupted, as a defect. See also ITU-T G.806 [2] (ITU-T Recommendation G.806, "Characteristics of transport equipment - Description methodology and generic functionality," 2009.).

In this document we refer to a Label Edge Router (LER), for a given LSP or Section, and to a PW Terminating Provider Edge (T-PE), for a given PW, as an End Point. Further, we refer to a Label Switching Router (LSR), for a given LSP, and to a PW Switching Provider Edge (S-PE), for a given PW, as an Intermediate Point. This document does not make a distinction between End Points (e.g., source and destination) as it can be inferred from the context of the sentences.

In this document we use the term "node" as a general reference to End Points and Intermediate Points.

In this document we refer to both segment and concatenated segments as segments (see [6] (Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., and S. Ueno, "MPLS-TP Requirements," August 2009.) for definitions relating to the term "segment" as well as for other definitions relating to MPLS-TP).

---

2. OAM Requirements

TOC

This section lists the requirements by which the OAM functionality of MPLS-TP should abide. Note that some requirements for this application of MPLS are similar to some of those listed in RFC 4377 [8] (Nadeau, T., Morrow, M., Swallow, G., Allan, D., and S. Matsushima, “Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks,” February 2006.).
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.

2.1. Architectural Requirements

TOC

2.1.1. Scope of OAM

TOC

The protocol solutions developed to meet the requirements identified in this document MUST be applicable to point-to-point bidirectional PWs, point-to-point bidirectional LSPs, and point-to-point bidirectional Sections and SHOULD additionaly be applicable to unidirectional point-to-point and point-to-multipoint LSPs.
The service emulated by a single segment or a multi-segment PW may span multiple domains. An LSP may also span multiple domains. It MUST be possible to operate OAM functions on a per domain basis. More generally, the protocol solutions MUST be applicable end-to-end and to segments.
Since LSPs may be stacked, the protocol solutions MUST be applicable on any LSP, regardless of the label stack depth. Furthermore it MUST be possible to estimate OAM fault and performance metrics of a single PW or LSP segment or of an aggregate of PWs or LSPs segments.

2.1.2. Independence

TOC

The protocol solutions SHOULD be independent of the underlying tunnelling or point-to-point technology or transmission media.
The protocol solutions SHOULD be independent of the service a PW may emulate.
Any OAM function operated on a PW, LSP or Section SHOULD be independent of the OAM function(s) operated on a different PW, LSP or Section. In

other words, only the OAM functions operated on e.g., a given LSP should be used to achieve the OAM objectives for that LSP. Note that independence should not be understood here in terms of isolation as there can be interactions between OAM functions operated on e.g., an LSP, and on another LSP or a PW.

Likewise, any OAM function applied to segment(s) of a PW or LSP SHOULD be independent of the OAM function(s) operated on the end-to-end PW or LSP. It SHOULD also be possible to distinguish an OAM packet running over a segment of a PW or LSP from another OAM packet running on the end-to-end PW or LSP. Furthermore, any OAM function applied to segment(s) of a PW or LSP SHOULD be independent of the OAM function(s) applied to other segment(s) of the same PW or LSP. Finally, the protocol solutions MUST support the capability to be concurrently and independently operated end-to-end and on segments.

OAM functions MUST operate and be configurable even in the absence of a control plane. Conversely, it SHOULD be possible to enable/disable the capability to operate OAM functions as part of connectivity management and it SHOULD also be possible to enable/disable the capability to operate OAM functions after connectivity has been established. In the latter case, the customer MUST NOT perceive service degradation as a result of OAM enabling/disabling. Ideally OAM enabling/disabling should take place without introducing any customer impairments (e.g., no customer packet losses). Procedures aimed to prevent any traffic impairment MUST be defined for the enabling/disabling of OAM functions. Means for configuring OAM functions and for connectivity management are outside the scope of this document.

2.1.3. Addressing, Routing and Forwarding

TOC

The OAM functionality may be deployed in a variety of environments.

* In some environments (e.g., IP/MPLS environments), IP routing and forwarding capabilities are inherently present in the forwarding plane. In this case, it MUST be possible to operate the OAM functions by relying on IP routing and forwarding capabilities.

* In some environments (e.g., MPLS-TP environments), IP routing and forwarding capabilities may not necessarily be present in the user plane. In this case, it MUST be possible to operate the OAM functions without relying on IP routing and forwarding capabilities.

In cases where OAM messages need to incorporate identification information (e.g., source and/or destination nodes), the protocol solution(s) MUST at least support an IP addressing structure and MUST also be extensible to support additional identification schemes.

2.1.4. Interoperability and Interworking

TOC

It is REQUIRED that OAM interoperability is achieved across the environments described in Section 2.1.3 (Addressing, Routing and Forwarding). It is also REQUIRED that the two first requirements of Section 2.1.3 (Addressing, Routing and Forwarding) still hold and MUST still be met when interoperability is achieved.

When MPLS-TP is run with IP routing and forwarding capabilities, it MUST be possible to operate any of the existing IP/MPLS and PW OAM protocols (e.g., LSP-Ping [3] (Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures," February 2006.), MPLS-BFD [9] (Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow, "BFD For MPLS LSPs," June 2008.), VCCV [4] (Nadeau, T. and C. Pignataro, "Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires," December 2007.) and VCCV-BFD [10] (Nadeau, T. and C. Pignataro, "Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)," July 2009.)).

2.1.5. Data Plane

TOC

OAM functions operate in the data plane. OAM packets MUST run in-band; that is, OAM packets for a specific PW, LSP or Section MUST follow the exact same data path as user traffic of that PW, LSP or Section. This is often referred to as fate sharing.

It MUST be possible to discriminate user 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 nodes targeted by these OAM packets.

As part of the design of OAM protocol solution(s) for MPLS-TP, a mechanism, for enabling the encapsulation and differentiation of OAM messages on a PW, LSP or Section, MUST be provided. Such mechanism SHOULD also support the encapsulation and differentiation of existing IP/MPLS and PW OAM messages.

2.2. Functional Requirements

TOC

Hereafter are listed the required functionalities composing the MPLS-TP OAM toolset. 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 functionalities, in the future.

The design of OAM mechanisms for MPLS-TP, MUST allow for the ability to support experimental OAM functions. These functions MUST be disabled by default.
The use of any OAM function MUST be optional and it MUST be possible to choose which OAM function(s) to use and on which PW, LSP or Section to apply it(them) to.
It is RECOMMENDED that the protocol solution, meeting one or more functional requirement(s), be the same for PWs, LSPs and Sections.
It is RECOMMENDED that the protocol solution, meeting one or more functional requirement(s), effectively provides a fully featured function; that is, a function which is applicable to all the cases identified for that functionality. In that context, protocol solution(s) MUST state their applicability.
Unless otherwise stated, the OAM functionalities MUST NOT rely on user traffic; that is, only OAM messages MUST be used to achieve the objectives.

2.2.1. General Requirements

TOC

If a defect or fault occurs on a PW, LSP or Section, mechanisms MUST be provided to detect it, diagnose it, localize it, and notify the appropriate nodes. Mechanisms SHOULD exist such that corrective actions can be taken.
Furthermore, mechanisms MUST be available for a service provider to be informed of a fault or defect affecting the service(s) it provides, even if the fault or defect is located outside of his domain.
The protocol solution(s) developed to meet these requirements may rely on information exchange. Information exchange between various nodes involved in the operation of an OAM function SHOULD be reliable such that, for example, defects or faults are properly detected or that state changes are effectively known by the appropriate nodes.

2.2.2. Continuity Checks

TOC

The MPLS-TP OAM toolset MUST provide functionality to enable the verification of the continuity of a PW, LSP or Section.
This function SHOULD be performed between End Points of PWs, LSPs and Sections.
This function SHOULD be performed pro-actively.

TOC

2.2.3. Connectivity Verifications

The MPLS-TP OAM toolset MUST provide functionality to enable the verification of the connectivity of a PW, LSP or Section.
This function SHOULD be performed between End Points and Intermediate Points of PWs and LSPs, and between End Points of PWs, LSPs and Sections.
This function SHOULD be performed on-demand. This function SHOULD be performed pro-actively only between End Points of PWs, LSPs and Sections.

2.2.4. Diagnostic

TOC

The MPLS-TP OAM toolset MAY provide functionality to enable the conduction of diagnostic tests on a PW, LSP or Section. An example of such diagnotic test would consist in looping the traffic at an Intermediate Point, back to the End Point it originates from. Another example of such diagnotic test would consist in estimating the bandwidth of e.g., an LSP.
This function SHOULD be performed on-demand.
This function SHOULD be performed between End Points and Intermediate Points of PWs and LSPs, and between End Points of PWs, LSPs and Sections.

2.2.5. Route Tracing

TOC

The MPLS-TP OAM toolset MUST provide functionality to enable an End Point to discover the Intermediate (if any) and End Point(s) along a PW, LSP or Section, and more generaly to trace the route of a PW, LSP or Section. The information collected MUST include identifiers related to the nodes and interfaces composing that route.
This function SHOULD be performed on-demand.
This function SHOULD be performed between End Points and Intermediate Points of PWs and LSPs, and between End Points of PWs, LSPs and Sections.

2.2.6. Lock Instruct

TOC

The MPLS-TP OAM toolset MUST provide functionality to enable an End Point of a PW, LSP or Section to instruct its associated End Point(s) to lock the PW, LSP or Section. Note that lock corresponds to an

administrative status in which forwarding traffic on and from the PW, LSP or Section is disabled.
This function SHOULD be performed on-demand.
This function SHOULD be performed between End Points of PWs, LSPs and Sections.

2.2.7. Lock Reporting

TOC

The MPLS-TP OAM toolset MUST provide functionality to enable an Intermediate Point of a PW or LSP to report, to an End Point of that same PW or LSP, an external lock condition affecting that PW or LSP.
This function SHOULD be performed pro-actively.
This function SHOULD be performed between Intermediate Points and End Points of PWs and LSPs.

2.2.8. Alarm Reporting

TOC

The MPLS-TP OAM toolset MUST provide functionality to enable an Intermediate Point of a PW or LSP to report, to an End Point of that same PW or LSP, a fault or defect condition affecting that PW or LSP.
This function SHOULD be performed pro-actively.
This function SHOULD be performed between Intermediate Points and End Points of PWs and LSPs.

2.2.9. Remote Defect Indication

TOC

The MPLS-TP OAM toolset MUST provide functionality to enable an End Point to report, to its associated End Point, a fault or defect condition that it detects on a PW, LSP or Section for which they are the End Points.
This function SHOULD be performed pro-actively.
This function SHOULD be performed between End Points of PWs, LSPs and Sections.

2.2.10. Client Failure Indication

TOC

The MPLS-TP OAM toolset MUST provide functionality to enable the propagation, across an MPLS-TP network, of information pertaining to a client defect of fault condition detected at an End Point of a PW or

LSP, if the client layer OAM mechanisms do not provide an alarm notification/propagation mechanism.
This function SHOULD be performed pro-actively.
This function SHOULD be performed between End Points of PWs and LSPs.

2.2.11. Packet Loss

TOC

The MPLS-TP OAM toolset MUST provide functionality to enable the quantification of packet loss ratio over a PW, LSP or Section.
Note that packet loss ratio is the ratio of the user packets not delivered to the total number of user packets transmitted during a defined time interval. The number of user packets not delivered is the difference between the number of user packets transmitted by an End Point and the number of user packets received at an End Point.
This function MAY either be performed pro-actively or on-demand.
This function SHOULD be performed between End Points of PWs, LSPs and Sections.
It SHOULD be possible to rely on user-plane traffic to achieve that functionality.

2.2.12. Delay Measurement

TOC

The MPLS-TP OAM toolset MUST provide functionality to enable the quantification of the one-way, and if appropriate, the two-way, delay of a PW, LSP or Section.

- One-way delay is the time elapsed from the start of transmission of the first bit of a packet by an End Point until the reception of the last bit of that packet by the other End Point.

- Two-way delay is the time elapsed from the start of transmission of the first bit of a packet by a End Point until the reception of the last bit of that packet by the same End Point, when loopback is performed at the other End Point.

This function SHOULD be performed on-demand and MAY be perform pro-actively.
This function SHOULD be performed between End Points of PWs, LSPs and Sections.
It SHOULD be possible to rely on user-plane traffic to achieve that functionality.

---

3. Congestion Considerations

[TOC]

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

---

4. Security Considerations

[TOC]

This document, as itself, does not imply any security consideration but OAM, as such, is subject to several security considerations. OAM messages can reveal sensitive information such as passwords, performance data and details about e.g., the network topology.
The nature of OAM therefore suggests having some form of authentication, authorization and encryption in place. This will prevent unauthorized access to MPLS-TP equipment and it will prevent third parties from learning about sensitive information about the transport network.
In general, mechanisms SHOULD be provided to ensure that OAM functions cannot be accessed unauthorized.
Further, OAM messages MAY be authenticated to prove their origin and to make sure that they are destined for the receiving node.
An OAM packet received over a PW, LSP or Section MUST NOT be forwarded beyond the End Point of that PW, LSP or Section, so as to avoid that the OAM packet leaves the current administrative domain.

---

5. IANA Considerations

[TOC]

There are no IANA actions required by this draft.

---

6. Acknowledgements

[TOC]

The editors gratefully acknowledge the contributions of Matthew Bocci, Italo Busi, Thomas Dietz, Huub van Helvoort, Wataru Imajuku, Marc Lasserre, Lieven Levrau, Han Li, Julien Meuric, Philippe Niger, Benjamin Niven-Jenkins, Jing Ruiquan, Nurit Sprecher, Yuji Tochio, Satoshi Ueno and Yaacov Weingarten.
The authors would like to thank all members of the teams (the Joint Working Team, the MPLS Interoperability Design Team in IETF and the MPLS-TP Ad Hoc Group in ITU-T) involved in the definition and specification of MPLS-TP.

---

7. References

TOC

7.1. Normative References

TOC

[1]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[2]	ITU-T Recommendation G.806, "Characteristics of transport equipment - Description methodology and generic functionality," 2009.
[3]	Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures," RFC 4379, February 2006 (TXT).
[4]	Nadeau, T. and C. Pignataro, "Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires," RFC 5085, December 2007 (TXT).

7.2. Informative References

TOC

[5]	Bocci, M., Bryant, S., Frost, D., Levrau, L., and L. Berger, "A Framework for MPLS in Transport Networks," draft-ietf-mpls-tp-framework-11 (work in progress), April 2010 (TXT).
[6]	Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., and S. Ueno, "MPLS-TP Requirements," draft-ietf-mpls-tp-requirements-10 (work in progress), August 2009 (TXT).
[7]	ITU-T Supplement Y.Sup4, "ITU-T Y.1300-series: Supplement on transport requirements for T-MPLS OAM and considerations for the application of IETF MPLS technology," 2008.
[8]	Nadeau, T., Morrow, M., Swallow, G., Allan, D., and S. Matsushima, "Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks," RFC 4377, February 2006 (TXT).
[9]	Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow, "BFD For MPLS LSPs," draft-ietf-bfd-mpls-07 (work in progress), June 2008 (TXT).
[10]	Nadeau, T. and C. Pignataro, "Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)," draft-ietf-pwe3-vccv-bfd-07 (work in progress), July 2009 (TXT).

Authors' Addresses

TOC

	Martin Vigoureux (editor)
	Alcatel-Lucent
	Route de Villejust
	Nozay, 91620
	France
Email:	martin.vigoureux@alcatel-lucent.com
	David Ward (editor)
	Cisco Systems, Inc.
	170 W. Tasman Dr.
	San Jose, CA 95134
	USA
Email:	dward@cisco.com
	Malcolm Betts (editor)
	Huawei
Email:	malcolm.betts@huawei.com