MPLS Working Group
Internet-Draft
Intended status: Informational
Expires: September 10, 2009

M. Vigoureux, Ed.
Alcatel-Lucent
D. Ward, Ed.
Cisco Systems, Inc.
M. Betts, Ed.
Nortel Networks

March 9, 2009

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

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, functional and operational requirements are covered in this document.

Requirements Language

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

In the context of MPLS Transport Profile (MPLS-TP, see [5] and [6]), 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 to this use case.

- as a service-oriented mechanism (used by a transport service provider) to monitor 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 Service Level Agreements (SLAs) parameters (e.g., using 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:

- 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, and faults, 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, 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 a set of requirements specified by ITU-T and first published in the ITU-T Supplement Y.Sup4 [7].

By covering transport specificities, these requirements stand as a

complement to those identified in RFC 4377 [8].

1.1. 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 [2].

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 [2].

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 any 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 referral to End

Points and Intermediate Points.

Other definitions, relating to MPLS-TP, can be found in [6].

1.2. Contributing Authors

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.

2. OAM Requirements

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].

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

2.1.1. Independence

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 PW may emulate.

The set of OAM functions operated on a PW, LSP or Section SHOULD be independent of the set of OAM functions operated on a different PW, LSP or Section. In other words, only the OAM functions available for e.g., a 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., a LSP and on another LSP or on a PW.

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 (e.g., LSP or PW) management. Means for configuring OAM functions and for connectivity management are outside the scope of this document.

2.1.2. Addressing, Routing and Forwarding

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 this case, the OAM functionality MUST support the use of IP routing and forwarding capabilities.

- In some environments (e.g., MPLS-TP environments), IP routing and forwarding capabilities may not necessarily be present. In this case, the OAM functions and their operation MUST NOT require relying on IP routing and forwarding capabilities.

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

2.1.3. Interoperability and Interworking

It is REQUIRED by this document that OAM interoperability is achieved across the environments described in Section 2.1.2. It is also REQUIRED by this document that the two first requirements of Section 2.1.2 still hold and MUST thus 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 functionalities (e.g., LSP-Ping [3], MPLS-BFD [9], VCCV [4] and VCCV-BFD [10]).

The protocol solution(s) developed to meet the requirements listed in

this document MUST interwork with the existing IP/MPLS and PW OAM protocols.

2.1.4. Data Plane

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.

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 solutions for MPLS-TP, a mechanism enabling to encapsulate and differentiate OAM messages, on a PW, LSP or Section, MUST be provided. Such mechanism MUST also support the encapsulation and differentiation of existing IP/MPLS and PW OAM messages.

2.1.5. Scope

The service emulated by a single segment or a multi-segment PW 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 (e.g., LSR or S-PE) of a LSP or of PW. This is referred to as (concatenated) segment monitoring.

2.2. Functional Requirements

Hereafter are listed the required functions 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 functions, in the future.

The design of OAM mechanisms, for MPLS-TP, MUST allow the ability to

support vendor specific and experimental OAM functions. These

functions MUST be disabled by default.

The use of any OAM function MUST be optional for the service provider or network operator and a network operator or service provider MUST be able to choose which OAM function(s) to use and on which PW, LSP or Section to apply it(them) to.

It is RECOMMENDED by this document that a protocol solution, realizing a given function, effectively provides a fully featured function, i.e., a function which is applicable to all the cases identified in the table in Section 2.3, for that function.

The OAM functions MUST be able to be operated on PWs, LSPs and Sections.

Note that the functions listed below can 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 function should be used for which application.

2.2.1. General Requirements

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 entities. Corrective actions SHOULD be taken according to the type of defect or fault.

Furthermore, in case of a fault or defect, affecting a service provided by a service provider, mechanisms MUST be available for the service provider to be informed of the fault or defect even if the fault or defect is located outside of his domain.

2.2.2. Continuity Checks

The MPLS-TP OAM toolset MUST provide a function to enable service providers and network operators to detect loss of continuity, but also unintended connectivity, on a PW, LSP or Section.

This function SHOULD be performed pro-actively.

This function SHOULD be performed between End Points of PWs, LSPs and Sections.

Means MUST be available to parameterize the frequency at which is performed this function as well as to parameterize the criteria, if any (e.g., number of consecutive OAM messages not received), based on which loss of continuity or unintended connectivity is detected. A default value MAY be defined.

2.2.3. Connectivity Verifications

The MPLS-TP OAM toolset MUST provide a function to enable service providers and network operators to verify the connectivity of a PW, LSP or Section.

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.

Note that, this function is sometime referred to as loopback as End Points expect to receive some level of information as a result of their action.

2.2.4. Diagnostic

The MPLS-TP OAM toolset MAY provide a function to enable service providers and network operators to perform diagnostic tests (e.g., verify bandwidth throughput) on a PW, LSP or Section.

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.

This function MAY be provided as part of the Connectivity Verifications function (see Section 2.2.3).

2.2.5. Adjacency

The MPLS-TP OAM toolset MUST provide a function to enable an End Point to request, to, and receive from, any node along a PW, LSP or Section, a certain level of information (e.g., identification, distance in hops).

This function SHOULD be performed on-demand.

This function SHOULD be performed between End Points and any node of a PW, LSP and Section.

This function MAY be provided jointly with the Route Tracing function (see Section 2.2.6).

2.2.6. Route Tracing

The MPLS-TP OAM toolset MUST provide a function to enable service providers and network operators to trace the route a PW, LSP or Section. The information collected SHOULD include identifiers related to the nodes composing that route and MAY include interface identifiers.

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.

This function MAY be provided jointly with the Adjacency function (see Section 2.2.5).

2.2.7. Lock

The MPLS-TP OAM toolset MAY provide a function enabling to administratively shut down a PW, LSP or Section; that is, to stop user traffic being sent over that PW, LSP or Section.

This function SHOULD be performed on-demand.

This function SHOULD be performed between End Points of PWs, LSPs and Sections.

2.2.8. Alarm Notification

The MPLS-TP OAM toolset MUST provide a function to enable server layer End Points to notify a fault condition or an administrative locking to the client layer End Points affected by this status. This would enable to suppress alarms that may be generated in the client layer as a result of the fault condition or of the administrative locking in the server layer.

The MPLS-TP OAM toolset MUST allow for the distinction between a fault condition and an administrative locking action.

The server layer End Points generating the notification and the client layer End Points receiving the notification may or may not be the same nodes. A mechanism MUST be provided to support both cases.

This function SHOULD be performed pro-actively.

This function SHOULD be performed between the End Points of PWs, LSPs and Sections and the End Points of the PWs and/or LSPs affected by the fault condition or administrative locking.

2.2.9. Client Failure Indication

The MPLS-TP OAM toolset MUST provide a function to enable the propagation of client fault condition information, across the MPLS-TP network, 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, LSPs and Sections.

2.2.10. Remote Defect Indication

The MPLS-TP OAM toolset MUST provide a function to enable an End Point to notify its associated End Point of the detection of a fault or defect that it detects on a PW, LSP or Section between them.

This function SHOULD be performed pro-actively.

This function SHOULD be performed between End Points of PWs, LSPs and Sections.

2.2.11. Packet Loss

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.

The MPLS-TP OAM toolset MUST provide a function to enable service providers and network operators to derive packet loss ratio over a PW, LSP or Section.

This OAM function MUST support the configurability of the interval of time during which the measure is performed.

This function SHOULD be performed pro-actively.

This function SHOULD be performed between End Points of PWs, LSPs and Sections.

2.2.12. Delay Measurement

The MPLS-TP OAM toolset MUST provide a function to enable service providers and network operators to measure 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 an OAM packet by an End Point until the reception of the last bit of that OAM packet by the other End Point.

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

This function SHOULD be performed on-demand.

This function SHOULD be performed between End Points of PWs, LSPs and Sections.

2.3. Operational Requirements

The OAM functions MUST NOT rely on user traffic to achieve their objectives; that is, dedicated OAM messages MUST be used.

Some OAM functions require certain parameters for their operation. These parameters MUST be configurable. A default value MAY be defined.

The specification of certain parameters' values SHOULD be such that it accounts, at the design phase, for various possible network conditions (e.g., the continuity check function should continue to meet its objective (i.e. detect failures) even in the context of high traffic load (e.g., congestion)).

This document does not mandate the use of a particular OAM function. However, it is RECOMMENDED that MPLS-TP enables continuity checks to be performed on every PW, LSP and Section in order to reliably detect connectivity defects and faults.

OAM functions MUST be applicable to bidirectional point-to-point PWs, LSPs and Sections, and a subset of these OAM functions MUST be applicable to unidirectional point-to-point and point-to-multipoint PWs, LSPs and Sections. 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, between which points of PWs, LSPs and Sections SHOULD the required OAM functions be applied. In these tables U stands for unidirectional; B stands for bidirectional; EP stands for an OAM function being performed between End Points; IP stands for an OAM function being performed between End Points and Intermediate Points. 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				pro-active			
	MEP		MIP		MEP		MIP	
	P2P	P2MP	P2P	P2MP	P2P	P2MP	P2P	P2MP
	U	B	U	U	B	U	U	B	U	U	B	U	U	B	U	U

c. checks								x	x	x				
c. verifications		1	x	1		1	x	1							
diagnostic		x	x	x		2	2	2							
adjacency		1	x	1		1	x	1							
route tracing		1	x	1		1	x	1							
lock	|x |x	x											
alarm notification									|x |x	x			
client fail. indic.									|2 |x	2			
remote defect indic.									|1 |x	1			
packet loss		2	3	2						x	4	x			
delay measurement		x	x	x						2	2	2			

1: the function MAY be provided if a return path exists
2: the function MAY be performed
3: the function SHOULD be performed in one direction
4: the function SHOULD be performed in both directions

OAM functions and their applicability scope

3. Congestion Considerations

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

4. Security Considerations

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

There are no IANA actions required by this draft.

6. Acknowledgements

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

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 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.

[4] Nadeau, T. and C. Pignataro, "Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires", RFC 5085, December 2007.

7.2. Informative References

[5] Bocci, M., Bryant, S., and L. Levrau, "A Framework for MPLS in Transport Networks", draft-ietf-mpls-tp-framework-00 (work in progress), November 2008.

[6] Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., and S. Ueno, "MPLS-TP Requirements", draft-ietf-mpls-tp-requirements-04 (work in progress), February 2009.

[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.

[9] Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow, "BFD For MPLS LSPs", draft-ietf-bfd-mpls-07 (work in progress), June 2008.

[10] Nadeau, T. and C. Pignataro, "Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)", draft-ietf-pwe3-vccv-bfd-03 (work in progress), February 2009.

Authors' Addresses

Martin Vigoureux (editor)
Alcatel-Lucent

Email: martin.vigoureux@alcatel-lucent.com

David Ward (editor)
Cisco Systems, Inc.

Email: dward@cisco.com

Malcolm Betts (editor)
Nortel Networks

Email: betts01@nortel.com