Internet Engineering Task Force (IETF)
Request for Comments: 5860
Category: Standards Track
ISSN: 2070-1721

M. Vigoureux, Ed.
Alcatel-Lucent
D. Ward, Ed.
Juniper Networks
M. Betts, Ed.
M. C. Betts Consulting Ltd.

May 2010

# Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks

## Abstract

This document lists architectural and functional requirements for the Operations, Administration, and Maintenance of MPLS Transport Profile. These requirements apply to pseudowires, Label Switched Paths, and Sections.

## Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5860.

Table of Contents

## 1. Introduction

In the context of MPLS Transport Profile (MPLS-TP, see [9] and [1]), the rationales for Operations, Administration, and Maintenance (OAM) are twofold as it can serve:

- as a network-oriented functionality, used by a transport network operator to monitor his network infrastructure and to implement internal mechanisms in order to enhance the general behavior and the level of performance of his network (e.g., protection mechanism in case of node or link failure). As an example, fault localization is typically associated with this use case.

- as a service-oriented functionality, 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 Agreement (SLA) 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, localization, and handling and diagnosis of defects, as well as by minimizing service interruptions and operational repair times.

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

- meeting 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.

### 1.1. Scope of This Document

This document lists architectural and functional 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 [10].

By covering transport specificities, these requirements complement those identified in RFC 4377 [11]; yet, some requirements may be similar.

This document only lists architectural and functional OAM requirements. It does not detail the implications of their applicability to the various types (e.g., point-to-point, point-to-multipoint, unidirectional, bidirectional, etc.) of PWs, LSPs, and Sections. Furthermore, this document does not provide requirements on how the protocol solution(s) should behave to achieve the functional objectives. Please see [12] for further information.

Note that the OAM functions 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 by detecting failure conditions, but may also be used for performance monitoring 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.

Note also that it is anticipated that implementers may wish to implement OAM message handling in hardware. Although not a requirement, this fact could be taken as a design consideration.

## 1.2. Requirements Language and Terminology

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 [2]. Although this document is not a protocol specification, the use of this language clarifies the instructions to protocol designers producing solutions that satisfy the requirements set out in this document.

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 [3].

- 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 [3].

- refer to OAM actions that are carried out continuously or at least over long periods of time, permitting proactive reporting of fault and/or performance results as proactive OAM.

- refer to OAM actions that are initiated via manual intervention for a limited time to carry out troubleshooting as on-demand OAM.

- 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.

- use the term "node" as a general reference to End Points and Intermediate Points.

- refer to both segment and concatenated segments as segments (see [1] for definitions relating to the term "segment" as well as for other definitions relating to MPLS-TP).

- refer to both single segment PWs and multi-segment PWs as PWs.

- refer to both bidirectional associated LSPs and bidirectional co-routed LSPs as bidirectional LSPs.

## 2. OAM Requirements

This section lists the requirements by which the OAM functionality of MPLS-TP should abide.

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.

RFC 5654 [1] states (Requirement #2) that the MPLS-TP design, SHOULD as far as reasonably possible, reuse existing MPLS standards. This general requirement applies to MPLS-TP OAM. MPLS-TP OAM is defined in this document through a set of functional requirements. These requirements will be met by protocol solutions defined in other documents. The way in which those protocols are operated and the way in which a network operator can control and use the MPLS-TP OAM functions SHOULD be as similar as possible to the mechanisms and techniques used to operate OAM in other transport technologies.

## 2.1. Architectural Requirements

### 2.1.1. Scope of OAM

The protocol solution(s) developed to meet the requirements identified in this document MUST at least be applicable to point-to-point bidirectional PWs, point-to-point co-routed bidirectional LSPs, and point-to-point bidirectional Sections. Section 2.2 provides additional information with regard to the applicability to point-to-point associated bidirectional LSPs, point-to-point unidirectional LSPs, and point-to-multipoint LSPs.

The service emulated by a PW may span multiple domains. An LSP may also span multiple domains. The protocol solution(s) MUST be applicable to end-to-end and to segments. More generally, it MUST be possible to operate OAM functions on a per-domain basis and across multiple domains.

Since LSPs may be stacked, the protocol solution(s) 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 PW or LSP segments.

### 2.1.2. Independence

The protocol solution(s) SHOULD be independent of the underlying tunneling or point-to-point technology or transmission media.

The protocol solution(s) 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 a given LSP (for example) should be used to achieve the OAM objectives for that LSP.

The protocol solution(s) MUST support the capability to be concurrently and independently operated end-to-end and on segments. Therefore, 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.

Note: Independence should not be understood in terms of isolation as there can be interactions between OAM functions operated, for example, on two different LSPs.

### 2.1.3. 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. 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 processing 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.

### 2.1.4. OAM and IP Capabilities

There are environments where IP capabilities are present in the data plane. IP/MPLS environments are examples of such environments. There are also environments where IP capabilities may not be present in the data plane. MPLS-TP environments are examples of environments where IP capabilities might or might not be present.

Note: Presence or absence of IP capabilities is deployment scenario dependent.

It MUST be possible to deploy the OAM functionality in any of these environments. As a result, it MUST be possible to operate OAM functions with or without relying on IP capabilities, and it MUST be possible to choose to make use of IP capabilities when these are present.

Furthermore, the mechanism required for enabling the encapsulation and differentiation of OAM messages (see Section 2.1.3) MUST support the capability to differentiate OAM messages of an OAM function

operated by relying on IP capabilities (e.g., using encapsulation in an IP header) from OAM messages of an OAM function operated without relying on any IP capability.

Note that IP capabilities include the capability to form a standard IP header, to encapsulate a payload in an IP header, to parse and analyze the fields of an IP header, and to take actions based on the content of these fields.

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

### 2.1.5. Interoperability and Interworking

It is REQUIRED that OAM interoperability is achieved between distinct domains materializing the environments described in Section 2.1.4. It is also REQUIRED that the first two requirements of Section 2.1.4 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 [4], MPLS-BFD [13], VCCV [5], and VCCV-BFD [14]).

### 2.1.6. Configuration

OAM functions MUST operate and be configurable even in the absence of a control plane. Conversely, it SHOULD be possible to configure as well as enable/disable the capability to operate OAM functions as part of connectivity management, and it SHOULD also be possible to configure as well as 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.

## 2.2. Functional Requirements

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 select the set of OAM function(s) to use on any PW, LSP, or Section.

It is RECOMMENDED that any protocol solution, meeting one or more functional requirement(s), be the same for PWs, LSPs, and Sections.

It is RECOMMENDED that any protocol solution, meeting one or more functional requirement(s), effectively provides a fully featured function; that is, a function that 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.

For the on-demand OAM functions, the result of which may vary depending on packet size, it SHOULD be possible to perform these functions using different packet sizes.

### 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 nodes. Mechanisms SHOULD exist such that corrective actions can be taken.

Furthermore, mechanisms MUST be available for a service provider to be aware of a fault or defect affecting the service(s) he provides, even if the fault or defect is located outside of his domain.

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

The MPLS-TP OAM toolset MUST provide a function to enable an End Point to monitor the liveness of a PW, LSP, or Section.

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

This function SHOULD be performed proactively.

The protocol solution(s) developed to perform this function MUST also apply to point-to-point associated bidirectional LSPs, point-to-point unidirectional LSPs, and point-to-multipoint LSPs.

### 2.2.3. Connectivity Verifications

The MPLS-TP OAM toolset MUST provide a function to enable an End Point to determine whether or not it is connected to specific End Point(s) by means of the expected PW, LSP, or Section.

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

This function SHOULD be performed on-demand between End Points and Intermediate Points of PWs and LSPs, and between End Points of PWs, LSPs, and Sections.

The protocol solution(s) developed to perform this function proactively MUST also apply to point-to-point associated bidirectional LSPs, point-to-point unidirectional LSPs, and point-to-multipoint LSPs.

The protocol solution(s) developed to perform this function on-demand MAY also apply to point-to-point associated bidirectional LSPs, to point-to-point unidirectional LSPs, and point-to-multipoint LSPs in case a return path exists.

### 2.2.4. Route Tracing

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 generally 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.

The protocol solution(s) developed to perform this function MAY also apply to point-to-point associated bidirectional LSPs, to point-to-point unidirectional LSPs, and point-to-multipoint LSPs in case a return path exists.

### 2.2.5. Diagnostic Tests

The MPLS-TP OAM toolset MUST provide a function to enable conducting diagnostic tests on a PW, LSP, or Section. An example of such a diagnostic test consists of performing a loop-back function at a node such that all OAM and data traffic are looped back to the originating End Point. Another example of such diagnostic test consists 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.

The protocol solution(s) developed to perform this function MAY also apply to point-to-point associated bidirectional LSPs, to point-to-point unidirectional LSPs and point-to-multipoint LSPs, in case a return path exists.

### 2.2.6. Lock Instruct

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 it is expected that only test traffic, if any, and OAM (dedicated to the PW, LSP, or Section) can be mapped on 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.

The protocol solution(s) developed to perform this function MUST also apply to point-to-point associated bidirectional LSPs, point-to-point unidirectional LSPs, and point-to-multipoint LSPs.

### 2.2.7. Lock Reporting

Based on the tunneling capabilities of MPLS, there are cases where Intermediate Point(s) of a PW or of an LSP coincide with End Point(s) of another LSP on which the former is mapped/tunneled. Further, it may happen that the tunnel LSP is out of service as a result of a lock action on that tunnel LSP. By means outside of the scope of this document, the Intermediate Point(s) of the PW or LSP may be aware of this condition. The MPLS-TP OAM toolset MUST provide a function to enable an Intermediate Point of a PW or LSP to report, to an End Point of that same PW or LSP, a lock condition indirectly affecting that PW or LSP.

This function SHOULD be performed proactively.

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

The protocol solution(s) developed to perform this function MUST also apply to point-to-point associated bidirectional LSPs, point-to-point unidirectional LSPs, and point-to-multipoint LSPs.

### 2.2.8. Alarm Reporting

Based on the tunneling capabilities of MPLS, there are cases where Intermediate Point(s) of a PW or of an LSP coincide with End Point(s) of another LSP on which the former is mapped/tunneled. Further, it may happen that the tunnel LSP be out of service as a result of a fault on that tunnel LSP. By means outside of the scope of this document, the Intermediate Point(s) of the PW or LSP may be aware of this condition. 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 indirectly affecting that PW or LSP.

This function SHOULD be performed proactively.

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

The protocol solution(s) developed to perform this function MUST also apply to point-to-point associated bidirectional LSPs, point-to-point unidirectional LSPs, and point-to-multipoint LSPs.

### 2.2.9. Remote Defect Indication

The MPLS-TP OAM toolset MUST provide a function 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 proactively.

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

The protocol solution(s) developed to perform this function MUST also apply to point-to-point associated bidirectional LSPs and MAY also apply to point-to-point unidirectional LSPs and point-to-multipoint LSPs in case a return path exists.

### 2.2.10. Client Failure Indication

The MPLS-TP OAM toolset MUST provide a function to enable the propagation, from edge to edge of an MPLS-TP network, of information pertaining to a client (i.e., external to the MPLS-TP network) defect or fault condition detected at an End Point of a PW or LSP, if the client layer OAM functionality does not provide an alarm notification/propagation functionality.

This function SHOULD be performed proactively.

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

The protocol solution(s) developed to perform this function MUST also apply to point-to-point associated bidirectional LSPs, point-to-point unidirectional LSPs, and point-to-multipoint LSPs.

### 2.2.11. Packet Loss Measurement

The MPLS-TP OAM toolset MUST provide a function to enable the quantification of packet loss ratio over a PW, LSP, or Section.

The loss of a packet is defined in RFC2680 [6] (see Section 2.4). This definition is used here.

Packet-loss ratio is defined here to be the ratio of the number of user packets lost to the total number of user packets sent during a defined time interval.

This function MAY either be performed proactively or on-demand.

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

It SHOULD be possible to rely on user traffic to perform this functionality.

The protocol solution(s) developed to perform this function MUST also apply to point-to-point associated bidirectional LSPs, point-to-point unidirectional LSPs, and point-to-multipoint LSPs.

### 2.2.12. Packet Delay Measurement

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

- The one-way delay is defined in [7] to be 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.

- The two-way delay is defined in [8] to be 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 same End Point.

Two-way delay may be quantified using data traffic loopback at the remote End Point of the PW, LSP, or Section (see Section 2.2.5).

Accurate quantification of one-way delay may require clock synchronization, the means for which are outside the scope of this document.

This function SHOULD be performed on-demand and MAY be performed proactively.

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

The protocol solution(s) developed to perform this function MUST also apply to point-to-point associated bidirectional LSPs, point-to-point unidirectional LSPs, and point-to-multipoint LSPs, but only to enable the quantification of the one-way delay.

## 3. Congestion Considerations

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

## 4. Security Considerations

This document, in 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.

OAM systems (network management stations) SHOULD be designed such that OAM functions cannot be accessed without authorization.

OAM protocol solutions MUST include the facility for OAM messages to authenticated to prove their origin and to make sure that they are destined for the receiving node. The use of such facilities MUST be configurable.

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. Acknowledgements

The editors gratefully acknowledge the contributions of Matthew Bocci, Italo Busi, Thomas Dietz, Annamaria Fulignoli, Huub van Helvoort, Enrique Hernandez-Valencia, Wataru Imajuku, Kam Lam, 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.

## 6. References

### 6.1. Normative References

[1] Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, September 2009.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[3] ITU-T Recommendation G.806, "Characteristics of transport equipment - Description methodology and generic functionality", 2009.

[4] Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures", RFC 4379, February 2006.

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

[6] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Packet Loss Metric for IPPM", RFC 2680, September 1999.

[7] Almes, G., Kalidindi, S., and M. Zekauskas, "A One-way Delay Metric for IPPM", RFC 2679, September 1999.

[8] Almes, G., Kalidindi, S., and M. Zekauskas, "A Round-trip Delay Metric for IPPM", RFC 2681, September 1999.

### 6.2. Informative References

[9] Bocci, M., Ed., Bryant, S., Ed., Frost, D., Ed., Levrau, L., and L. Berger, "A Framework for MPLS in Transport Networks", Work in Progress, May 2010.

[10] 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.

[11] 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.

[12] Busi, I., Ed., Niven-Jenkins, B., Ed., and D. Allan, Ed., "MPLS-TP OAM Framework", Work in Progress, April 2010.

[13] Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow, "BFD For MPLS LSPs", Work in Progress, June 2008.

[14] Nadeau, T., Ed. and C. Pignataro, Ed., "Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)", Work in Progress, July 2009.

## Authors' Addresses

Martin Vigoureux (editor)
Alcatel-Lucent
Route de Villejust
Nozay 91620
France

EMail: martin.vigoureux@alcatel-lucent.com

David Ward (editor)
Juniper Networks

EMail: dward@juniper.net

Malcolm Betts (editor)
M. C. Betts Consulting Ltd.

EMail: malcolm.betts@rogers.com