Network Working Group Internet Draft Intended status: Informational Expires: September 14, 2011

Luyuan Fang Dan Frost Cisco Systems Nabil Bitar Verizon Raymond Zhang BT Lei Wang Telenor Kam Lee Yap X0 Communications Michael Fargano Qwest John Drake Juniper Thomas Nadeau

March 14, 2011

MPLS-TP OAM Toolset draft-fang-mpls-tp-oam-toolset-01.txt

Abstract

This document provides an overview of the MPLS-TP OAM toolset, which consists of MPLS-TP fault management and performance monitoring. This overview includes a brief recap of MPLS-TP OAM requirements and functions, and of the generic mechanisms created in the MPLS data plane to support in-band OAM. The importance of using IANA assigned code point under G-Ach when supporting MPLS-TP OAM is also discussed. The protocol definitions for each individual MPLS-TP OAM tool are specified in separate RFCs or Working Group documents which are referenced by this document.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of $\underline{BCP 78}$ and $\underline{BCP 79}$.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents

[Page 1]

at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress.

This Internet-Draft will expire on September 14, 2011.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to <u>BCP 78</u> and the IETF Trust's Legal Provisions Relating to IETF Documents

(<u>http://trustee.ietf.org/license-info</u>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the <u>Trust Legal Provisions</u> and are provided without warranty as described in the Simplified BSD License..

Table of Contents

<u>1</u> . Introduction <u>3</u>
<u>2</u> . Terminology <u>3</u>
<u>3</u> . Brief Overview of MPLS-TP OAM Requirements <u>6</u>
3.1. Architectural Requirements <u>6</u>
3.2. Functional Requirements <u>6</u>
4. MPLS-TP OAM Mechanisms and Toolset Summary
4.1. In-band OAM Mechanisms8
<u>4.2</u> . Fault Management Toolset8
<u>4.3</u> . Performance Monitoring Toolset <u>10</u>
<u>5</u> . OAM Toolset Utilization and Protocol Definitions <u>10</u>
<u>5.1</u> . Connectivity Check and Connectivity Verification <u>10</u>
5.2 Diagnostic Tests and Lock Instruct11
<u>5.3</u> . Lock Reporting <u>11</u>
5.4. Alarm Reporting and Link down Indication12
<u>5.5</u> . Remote Defect Indication <u>12</u>
5.6. Packet Loss and Delay Measurement13
6. IANA assigned code points under G-Ach14
<u>7</u> . Security Considerations <u>15</u>
<u>8</u> . IANA Considerations <u>15</u>

[Page 2]

<u>9</u> .	Normative References	<u>15</u>
<u>10</u> .	Informative References	<u>16</u>
<u>11</u> .	Authors' Addresses	<u>17</u>

Requirements Language

Although this document is not a protocol specification, 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 <u>RFC 2119</u> [RFC 2119].

1. Introduction

The Operations, Administration, and Maintenance (OAM) Requirements for Transport Profile of Multiprotocol Label Switching (MPLS-TP) networks are defined in <u>RFC 5860</u> [<u>RFC 5860</u>]. MPLS-TP OAM mechanisms and multiple OAM tools have been developed based on MPLS-TP OAM requirements.

This document provides an overview of the MPLS-TP OAM toolset, which consists of MPLS-TP fault management and performance monitoring. This overview includes a brief recap of MPLS-TP OAM requirements and functions, and of the generic mechanisms created in the MPLS data plane to support in-band OAM. The importance of using IANA assigned code point under G-Ach when supporting MPLS-TP OAM is also discussed.

The protocol definitions for each individual MPLS-TP OAM tool are specified in separate RFCs or Working Group documents while this document is work in progress, which are referenced by this document.

The protocol definitions for each individual MPLS-TP OAM tool are defined in separate RFCs (or Working Group documents while this document is work in progress) referenced by this document.

2. Terminology

This document uses MPLS-TP OAM specific terminology.

Term Definition AC Attachment Circuit AIS Alarm indication signal

- APS Automatic Protection Switching
- ATM Asynchronous Transfer Mode
- BFD Bidirectional Forwarding Detection
- CC Continuity Check
- CE Customer-Edge device
- CM Configuration Management
- CoS Class of Service
- CV Connectivity Verification
- FM Fault Management
- GAL Generic Alert Label
- G-ACH Generic Associated Channel
- GMPLS Generalized Multi-Protocol Label Switching
- LDI Link Down Indication
- LDP Label Distribution Protocol
- LER Label Edge Router
- LKR Lock Report
- LM Loss Measurement
- LMEG LSP ME Group
- LOC Loss of Continuity
- LSP Label Switched Path
- LSR Label Switching Router
- LSME LSP SPME ME
- LSMEG LSP SPME ME Group
- ME Maintenance Entity

- MEG Maintenance Entity Group
- MEP Maintenance Entity Group End Point
- MIP Maintenance Entity Group Intermediate Point
- MPLS MultiProtocol Label Switching
- NMS Network Management System
- NTP Network Time Protocol
- OAM Operations, Administration, and Management
- PE Provider Edge
- PM Performance Monitoring
- PME PW Maintenance Entity
- PMEG PW ME Group
- PSME PW SPME ME
- PSMEG PW SPME ME Group
- PW Pseudowire
- QoS Quality of Service
- RDI Remote Defect Indication
- SDH Synchronous Digital Hierarchy
- SLA Service Level Agreement
- SME Section Maintenance Entity
- SMEG Section ME Group
- SONET Synchronous Optical Network
- SPME Sub-path Maintenance Element
- S-PE Switching Provider Edge
- SRLG Shared Risk Link Group
- TC Traffic Class

T-PE Terminating Provider Edge

3. Brief Overview of MPLS-TP OAM Requirements

This following Architectural and Functional Requirements are defined by $\frac{\text{RFC} 5860}{\text{Def}}$. They are captured here for easy reading before discussing the toolset.

3.1. Architectural Requirements

The MPLS-TP OAM Supports point-to-point bidirectional PWs, pointto-point co-routed bidirectional LSPs, point-to-point bidirectional Sections, point-to-point associated bidirectional LSPs, point-topoint unidirectional LSPs, and point-to-multipoint LSPs. In addition, MPLS-TP OAM supports these LSPs and PWs when they span single domain or multiple domains.

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.

In-band OAM MUST be implemented. OAM packets for a specific PW, LSP, or Section MUST follow the exact same data path as user traffic of the same.

The solutions MUST support OAM functions with or without relying on IP capabilities.

It is REQUIRED that OAM interoperability be achieved between distinct domains with different operational models, e.g. with IP or without IP support in the data plane.

And OAM functions MUST be configurable even in the absence of a control plane.

3.2. Functional Requirements

In general, MPLS-TP OAM tools MUST provide functions to detect, diagnose, localize, and notify the faults when occur. The mechanism for correction actions trigged by fault detection SHOULD be provided.

The following are the fault detection functional requirements

- Continuity Checks: a function to enable an End Point to monitor the liveness of a PW, LSP, or Section.

- Connectivity Verifications: 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.

- Route Tracing: the functionality to enable an End Point to discover the Intermediate (if any) and End Point(s) along a PW, LSP, or Section, and more generically to trace the route of a PW, LSP or Section.

- Diagnostic Tests: a function to enable conducting diagnostic tests on a PW, LSP, or Section. For example, a loop-back function.

- Lock Instruct: the 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.

- Lock Reporting: 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.

- Alarm Reporting: the 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.

- Remote Defect Indication: 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.

- Client Failure Indication: a function to enable the propagation, from edge to edge of an MPLS-TP network, of information pertaining to a client fault condition detected at an End Point of a PW or LSP, if the client layer OAM does not provide alarm notification.

- Packet Loss Measurement: a function to enable the quantification of packet loss ratio over a PW, LSP, or Section.

- Packet Delay Measurement: a function to enable the quantification of the one-way, and if appropriate, the two-way, delay ratio of a PW, LSP, or Section.

<u>4</u>. MPLS-TP OAM Mechanisms and Toolset Summary

The following subsections provide the summary of MPLS-TP OAM Fault Management and Performance Management toolset, with indication of the corresponding IETF RFCs (or Internet drafts while this document

is work in progress) to support the MPLS-TP OAM functions defined in <u>RFC 5860</u>.

4.1. In-band OAM Mechanisms

To meet the In-band OAM requirements for MPLS-TP, Generic Associated Channel is created [<u>RFC 5586</u>]. It generalizes the applicability of the Pseudowire (PW) Associated Channel Header (ACH) to MPLS Label Switching Paths (LSPs), and Sections.

The Generic Associated Label (GAL) [<u>RFC 5586</u>] is defined by assigning one of the reserved MPLS label values to the G-Ach, GAL identifies the presence of the Associated Channel Header following the label stack.

The creation of G-Ach and GAL provided the necessary mechanisms for building in-band OAM MPLS-TP toolset.

<u>RFC 5718</u> [<u>RFC 5718</u>] An-In-Band Data Communication Network for the MPLS Transport Profile describes how the G-Ach may be used for Management and Signaling Communication.

4.2. Fault Management Toolset

The following tables provide the summary of MPLS-TP OAM toolset.

Table 1 provides the summary of MPLS-TP OAM Fault Management toolset functions, associated tool/protocol, and the corresponding IETF RFCs or Internet drafts where they are defined.

Table 2 provides the Performance Monitoring Functions, associated tool/protocol definitions, and the corresponding IETF RFCs or Internet Drafts where they are defined.

The following table provide the Performance Monitoring Functions, protocol definitions, and corresponding RFCs or Internet Drafts.

(Editor's note: only RFCs will be referenced in the final version of the document).

Proactive Fault Management OAM Toolset					
OAM Functions	OAM Tools/Protocols	RFCs / IDs			
Continuity Check (CV) & Continuity Verification(CV)	Bidirectional Forwarding Detection (BFD)	<u>draft-ietf-mpls-tp</u> -cc-cv-rdi [<u>cc-cv</u>]			
Remote Defect Indication (RDI)	 Bidirectional Forwarding Detection (BFD)	<u>draft-ietf-mpls-tp</u> -cc-cv-rdi [<u>cc-cv</u>]			
Alarm Indication Signal (AIS)	AIS message under G-Ach 	<u>draft-ietf-mpls-tp</u> -fault [<u>fault</u>]			
Link Down Indication (LDI)	Flag in AIS message 	<u>draft-ietf-mpls-tp</u> -fault [<u>fault</u>]			
Lock Report (LKR)	LKR message under G-Ach 	<u>draft-ietf-mpls-tp</u> -fault [<u>fault</u>]			

Table 1. Proactive Fault Management OAM Toolset

On Demand Fault Management OAM Toolset				
OAM Functions	OAM Tools/Protocols	RFCs / IDs		
Continuity Verification(CV)	LSP Ping and BFD 	<u>draft-ietf-mpls-tp</u> -cc-cv-rdi [<u>cc-cv</u>]		
Diagnostic: Loopback, Lock and LSP Ping	<pre> 1) In-band Loopback and Lock Instruct 2) LSP Ping</pre>	<u>draft-ietf-mpls-tp</u> -li-lb [<u>li-lb</u>]		
Lock Instruct Llock Instruct	In-band lock message in G-Ach	<u>draft-ietf-mpls-tp</u> -li-lb [<u>li-lb</u>]		

Table 2. On Demand Fault Management OAM Toolset

4.3. Performance Monitoring Toolset

Table 3 provides the Performance Monitoring Fuctions, protocol definitions, and corresponding RFCs or Internet Drafts.

Performance Monitoring OAM Toolset					
OAM Functions	Protocols Definitions	RFCs / IDs			
Packet loss measurement (LM)	LM & DM query messages 	<u>draft-ietf-mpls-tp</u> -loss-delay [<u>lo-de</u>]			
 Packet delay (DM) measurement 	LM & DM query messages 	<pre>draft-ietf-mpls-tp -loss-delay -profile [tp-lo-de]</pre>			
Throughput measurement 	derived from Loss measurement				
Delay Variation measurement +	Supported from Delay measurement				

Table 3. Performance Monitoring OAM Toolset

5. OAM Toolset Utilization and Protocol Definitions

5.1. Connectivity Check and Connectivity Verification

Continuity Check (CC) and Proactive Connectivity Verification (CV) functions are used to detect loss of continuity (LOC), and unintended connectivity between two MEPs.

Loss of connectivity, mis-merging, mis-connectivity, or unexpected Maintenance Entity Group End Points (MEPs) can be detected using the CC/CV tools.

The CC/CV tools are used to support MPLS-TP fault management, performance management, and protection switching.

Bidirectional Forwarding Detection (BFD) and LSP Ping are defined to support the CC/CV functions [cc-cv].

BFD control packets are sent by the source MEP to sink MEP. The sink MEP monitors the arrival of the BFD control packets and detects the defect.

The interval of BFD control packet can be configured. For example:

- 3.3ms is the default interval for protection switching.
- 100ms is the default interval for performance monitoring.
- 1s is the default interval for fault management.

5.2. Diagnostic Tests and Lock Instruct

The OAM functions to support diagnostic tests are required in the transport environment.

The Loopback mode is defined for management purpose in [<u>li-lb</u>]. The mechanism is provided to Lock and unlock traffic (e.g. data and control traffic) or specific OAM traffic at a specific LSR on the path of the MPLS-TP LSP to allow loop back it to the source by [li-lb].

These diagnostic functions apply to associated bidirectional MPLS-TP LSPs, including MPLS-TP LSPs, bi-directional RSVP-TE tunnels (which is relevant for MPLS-TP dynamic control plane option with GMPLS), and single segment and multi-segment pseudowires.

The Lock operation instruction is carried in an MPLS Loopback request message sent from a MEP to a trail-end MEP of the LSP to request that the LSP be taken out of service. In response, the Lock operation reply is carried in a Loopback response message sent from the trail-end MEP back to the originating MEP to report the result.

The loopback operations include [<u>li-lb</u>]:

- Lock: take an LSP out of service for maintenance.
- Unlock: Restore a previously locked LSP to service.
- Set Full Loopback and Set OAM Loopback
- Unset Full Loopback and Set OAM Loopback

Operators can use the loopback mode to test the connectivity or performance (loss, delay, delay variation, and throughput) of given LSP upto a specific node on the path of the LSP.

5.3. Lock Reporting

The Lock Report (LKR) function is used to communicate to the client (sub-) layer MEPs the administrative locking of a server (sub-) layer MEP, and consequential interruption of data traffic forwarding in the client (sub-) layer [fault].

When operator is taking the LSP out of service for maintenance other operational reason, using the LKR function can help to

distinguish the condition as administrative locking from defect condition.

The Lock Report function would also serve the purpose of alarm suppression in the MPLS-TP network above the level of the Lock is occurred. The receipt of an LKR message MAY be treated as the equivalent of loss of continuity at the client layer [fault].

5.4. Alarm Reporting and Link down Indication

Alarm Indication Signal (AIS) message serves the purpose of alarm suppression upon the failure detection in the server (-sub) layer. When the Link Down Indication (RDI) is set, the AIS message MAY be used to trigger recovery mechanisms [fault].

When a server MEP detects the failure, it asserts Loss of Continuity (LOC) or signal fail which sets the flag up to generate OAM packet with AIS message. The AIS message is forwarded to downstream sink MEP in the client layer. This would enable the client layer to suppress the generation of secondary alarms.

A Link Down Indication (LDI) flag is defined in the AIS message. The LDI flag is set in the AIS message in response to detecting a fatal failure in the server layer. Receipt of an AIS message with this flag set MAY be interpreted by a MEP as an indication of signal fail at the client layer. [fault]

Fault OAM messages are generated by intermediate nodes where an LSP is switched, and propagated to the end points (MEPs).

From practical point of view, when both proactive CC functions and LDI are used, one may consider to run the proactive CC functions at a slower rate (e.g. longer BFD hello intervals), and reply on LDI to trigger fast protection switch over upon failure detection in a given LSP.

5.5. Remote Defect Indication

Remote Defect Indication (RDI) function enables an End Point to report to the other End Point that a fault or defect condition is detected on the PW, LSP, or Section they are the End Points.

The RDI OAM function is supported by the use of Bidirectional Forwarding Detection (BFD) Control Packets [<u>cc-cv</u>]. RDI is only used for bidirectional connections and is associated with proactive CC/CV activation. When an end point (MEP) detects a signal failure condition, it sets the flag up by setting the diagnostic field of the BFD control packet to a particular value to indicate the failure condition on the associated PW, LSP, or Section, and transmitting the BFD control packet with the failure flag up to the other end point (its peer MEP).

RDI function can be used to facilitate the protection switching by synchronizing the two end points when unidirectional failure occurs and is detected by one end.

5.6. Packet Loss and Delay Measurement

Packet loss and delay measurement toolset enables operators to measure the quality of the packet transmission over a PW, LSP, or Section.

The protocol for MPLS-TP loss and delay measurement functions is defined in [lo-de] as profiled in [tp-lo-de]. These documents specify how to measure Packet Loss, Packet Delay, Packet Delay Variation, and Throughput.

The loss and delay protocols have the following characteristics and capabilities:

- Support measurement of packet loss, delay and throughput over Label Switched Paths (LSPs), pseudowires, and MPLS sections (links).
- The same LM and DM protocols can be used for both continuous/proactive and selective/on-demand measurement.
- The LM and DM protocols use a simple query/response model for bidirectional measurement that allows a single node the querier - to measure the loss or delay in both directions.
- The LM and DM protocols use query messages for unidirectional loss and delay measurement. The measurement can either be carried out at the downstream node(s) or at the querier if an out-of-band return path is available.
- The LM and DM protocols do not require that the transmit and receive interfaces be the same when performing bidirectional measurement.

- The LM protocol supports both 32-bit and 64-bit counters although for simplicity only 32-bit packet counters are currently included in the MPLS-TP profile.
- The LM protocol supports measurement in terms of both packet counts and octet counts although for simplicity only packet counters are currently included in the MPLS-TP profile.
- The LM protocol can be used to measure channel throughput as well as packet loss.
- The DM protocol supports varying the measurement message size in order to measure delays associated with different packet sizes.

<u>6</u>. IANA assigned code points under G-Ach

OAM toolset/functions defined under G-Ach MUST use IANA assigned code points, using Experimental Code Point under G-Ach is inappropriate and it can lead to interoperability problems and potential Code Point collision in production network.

<u>RFC 5586</u> "MPLS Generic Associated Channel" stated the following in IANA consideration section: A requirement has emerged (see [RFC 5860]) to allow for optimizations or extensions to OAM and other control protocols running in an associated channel to be experimented without resorting to the IETF standards process, by supporting experimental code points. This would prevent code points used for such functions from being used from the range allocated through the IETF standards and thus protects an installed base of equipment from potential inadvertent overloading of code points. In order to support this requirement, IANA has changed the code point allocation scheme for the PW Associated Channel as follows:

0 - 32751: IETF Review 32760 - 32767: Experimental

Code points in the experimental range MUST be used according to the guidelines of $\frac{\text{RFC } 3692}{\text{MUST}}$ [$\frac{\text{RFC } 3692}{\text{FC}}$]. Functions using experimental G-Ach code points MUST be disabled by default.

The guidelines on the usage of experimental numbers are defined in IETF <u>RFC 3692</u>. As indicated by <u>RFC 3692</u>: The experimental numbers are useful when experimenting new protocols or extending existing protocols in order to test and experiment with the new functions, as part of implementation. <u>RFC 3692</u> reserves a range of numbers for

experimentation when the need of such experimentation has been identified.

However, the experimental numbers "are reserved for generic testing purposes, and other implementations may use the same numbers for different experimental uses." "Experimental numbers are intended for experimentation and testing and are not intended for wide or general deployments." "Shipping a product with a specific value pre-enabled would be inappropriate and can lead to interoperability problems when the chosen value collides with a different usage, as it someday surely will."

Further more, "it would be inappropriate for a group of vendors, a consortia, or another Standards Development Organization to agree among themselves to use a particular value for a specific purpose and then agree to deploy devices using those values." Experimental numbers are not guaranteed to be unique by definition. There is the risk of code point collision when using Experimental Code Point in production networks.

Similar statements can also be found in <u>RFC4929</u> "Change Process for Multiprotocol Label Switching (MPLS) and Generalized MPLS (GMPLS) Protocols and Procedures". As described in [<u>RFC 4775</u>], "nonstandard extensions, including experimental values, are not to be portrayed as industrial standards whether by an individual vendor, an industry forum, or a standards body."

7. Security Considerations

The document provides overview of MPLS-TP OAM requirements, functions, protocol, and solution considerations. The actual protocols for the OAM toolset are defined in separate documents and referenced by this document.

The general security considerations are provided in Security Framework for MPLS and GMPLS Networks [<u>RFC 5920</u>], and MPLS-TP Security Framework [<u>tp-sec-fr</u>].

<u>8</u>. IANA Considerations

This document contains no new IANA considerations.

9. Normative References

[<u>RFC 5586</u>], M. Bocci, M. Vigoureux, S. Bryant, "MPLS Generic Associated Channel", <u>RFC 5586</u>, June 2009.

[<u>RFC 5654</u>], Niven-Jenkins, B., et al, "MPLS-TP Requirements", <u>RFC 5654</u>, September 2009.

[<u>RFC 5718</u>], D. Beller, and A. Farrel, "An In-Band Data Communication Network For the MPLS Transport Profile", <u>RFC 5718</u>, Jan 2010.

[<u>RFC 5860</u>], M. Vigoureux, D. Ward, M. Betts, "Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks", <u>RFC 5860</u>, May 2010.

[cc-cv] D. Allan, G. Swallow, J. Drake, Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile, <u>draft-ietf-mpls-tp-cc-cv-rdi-03</u>, Feb. 2011.

[fault] G. Swallow, A. Fulignoli, M. Vigoureux, MPLS Fault Management OAM, <u>draft-ietf-mpls-tp-fault-01</u>, March 2011.

[li-lb] S. Boutros, S. Sivabalan, et,al., MPLS Transport Profile Lock Instruct and Loopback Functions <u>draft-ietf-mpls-tp-li-lb-</u> 01.txt, March 2011.

[loopback] S. Boutros, S. Sivabalan, G. Swallow, R. Aggarwal, M. Vigoureux, Operating MPLS Transport Profile LSP in Loopback Mode, draft-boutros-mpls-tp-loopback-03.txt, March 2011.

[lo-de] D. Frost, S. Bryant, Packet Loss and Delay Measurement for the MPLS Networks, <u>draft-ietf-mpls-loss-delay-01</u>, Feb. 2011.

[tp-lo-de] D. Frost, S. Bryant, A Packet Loss and Delay Measurement Profile for MPLS-based Transport Networks, <u>draft-frost-mpls-tp-loss-</u> <u>delay-profile-02</u>, Feb. 2011.

<u>10</u>. Informative References

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

[RFC 3692] T. Narten, "Assigning Experimental and Testing Numbers Considered Useful", <u>RFC 3692</u>, Jan. 2004.

[RFC 4775] S. Bradner, "Procedures for Protocol Extensions and Variations", <u>RFC 4775</u>, Dec. 2006.

[Page 16]

[RFC 5920] L. Fang, et al, Security Framework for MPLS and GMPLS Networks, July 2010.

[MPLS-TP NM REQ] Hing-Kam Lam, Scott Mansfield, Eric Gray, MPLS TP Network Management Requirements, <u>draft-ietf-mpls-tp-nm-req-06.txt</u>, October 2009.

[tp-sec-fr] L. Fang, Niven-Jenkins, S. Mansfield, et. Al. MPLS-TP Security Framework, <u>draft-ietf-mpls-tp-security-framework-00</u>, Feb. 2011.

11. Authors' Addresses

Luyuan Fang Cisco Systems 111 Wood Avenue South Iselin, NJ 08830 USA Email: lufang@cisco.com Dan Frost Cisco Systems Email: danfrost@cisco.com Nabil Bitar Verizon 40 Sylvan Road Waltham, MA 02145 USA Email: nabil.bitar@verizon.com Raymond Zhang British Telecom BT Center 81 Newgate Street London, EC1A 7AJ United Kingdom Email: raymond.zhang@bt.com Lei Wang Telenor Telenor Norway Office Snaroyveien 1331 Fornedbu

Email: Lei.wang@telenor.com

Kam Lee Yap

March 2011

XO Communications 13865 Sunrise Valley Drive, Herndon, VA 20171 Email: klyap@xo.com

Michael Fargano Qwest 5325 Zuni St, 224 Denver CO 80221-1499 Email: Michael.Fargano@qwest.com

John Drake Juniper Email: jdrake@juniper.net

Thomas Nadeau Email: tnadeau@lucidvision.com