Network Working Group
Internet Draft
Intended status: Standards Track
Expires: January 5, 2011

Sami Boutros (Ed.)
Siva Sivabalan (Ed.)
Cisco Systems, Inc.

Rahul Aggarwal (Ed.)
Juniper Networks, Inc.

Martin Vigoureux (Ed.)
Alcatel-Lucent

Xuehui Dai (Ed.)
ZTE Corporation

July 5, 2010

MPLS Transport Profile Lock Instruct and Loopback Functions
draft-boutros-mpls-tp-li-lb-01.txt

Status of this Memo

Abstract

This document specifies an extension to MPLS Operation, administration, and Maintenance (OAM) to operate an MPLS Transport Profile (MPLS-TP) Label Switched Path (LSP), bi-directional RSVP-TE tunnels, pseudowires (PW), or Multi-segment PWs in loopback mode for management purpose. This extension includes mechanism to lock and unlock MPLS-TP Tunnels (i.e. data and control traffic) and can be used to loop all traffic (i.e, data and control traffic) at a specified LSR on the path of the MPLS-TP LSP back to the source.

Table of Contents

1. Introduction

In traditional transport networks, circuits are provisioned across multiple nodes and service providers have the ability to operate the transport circuit such as T1 line in loopback mode for management purposes, e.g., to test or verify connectivity of the circuit up to a specific node on the path of the circuit, to test the circuit performance with respect to delay/jitter, etc. MPLS-TP bidirectional LSP emulating traditional transport circuits need to provide the same loopback capability. The mechanisms in this document apply to associated bidirectional paths as defined in [7], which include MPLS-TP LSPs, bi-directional RSVP-TE tunnels, pseudowires (PW), and Multi-segment PWs.

To describe the loopback functionality, let us assume a bi-directional MPLS-TP LSP A <---> B <---> C <---> D where A, B, C, and D are MPLS capable nodes. Also, let us assume that the network operator requires C to loop, back to A, the packets sent from A. In this example, A and D acts as Maintenance End Points (MEPs) and C acts as a Maintenance Intermediate Point (MIP). The operator can setup the MPLS-TP LSP into loopback mode such that C loops all the packets (regardless of whether they are data or control packets) generated by node A back to A. The packets are not also forwarded towards D. Similarly, any traffic received by C from the reverse direction will be dropped.

The operator must take the MPLS-TP LSP out of service before setting up the MPLS-TP LSP in loopback mode. This is accomplished by the MEP establishing the loopback first sending a Lock command to the remote MEP(s). In the case above, A sends a Lock request message along the MPLS-TP LSP and destined to D to lock the MPLS-TP LSP. The message will be intercepted by D since it is at the end of the LSP. D responds to the lock request with a reply message specifying whether it can take the LSP out of service or not.

In order to set the MPLS-TP LSP in loopback mode, A sends a Loopback request message to the MIP or MEP where the loopback is to be enabled. In the above example, the MPLS TTL value is set so that the message will be intercepted by C.

This message contains a request to instruct C to operate the corresponding MPLS-TP LSP in Loopback mode. C responds to the Loopback request with a reply message back to A to indicate whether or not it has successfully set the MPLS-TP LSP into the loopback mode. If the loopback cannot be set, the reply message would contain an error code. Upon receiving such a reply to the loopback request, A logs the event and takes further reporting actions as necessary. If the MPLS-TP LSP was previously locked, A sends another request message to D to unlock it.

If the loopback request can be performed, the input LSP from the direction of A is directly cross-connected to the output LSP towards A. All the packets generated by node A (data and control) are looped back at C, excepting the case of TTL expiration.

When the loopback operation is no longer required, A sends a request message to remove the loopback and thus restore the LSP to its original forwarding state. In this example the MPLS TTL is set such that this message is intercepted by C. It is expected that C sends a reply back to A to with a return code either ACKing or NAK the loopback removal request. Upon getting an ACK response to loopback mode removal request, A sends another request message to unlock the MPLS-TP LSP. The packet is intercepted by D as it is at the end of the MPLS-TP LSP.

The proposed mechanism is based on a new set of messages and TLVs which can be transported using one of the following methods:

(1) An in-band MPLS message transported using a new ACH code point, the message will have different types to perform the loopback request/remove and Lock/unlock functions, and may carry new set of TLVs.

(2) A new set of TLVs which can be transported using LSP-Ping extensions defined in [4], and in compliance to specifications [5].

Method (1) and (2) are referred to as "in-band option" and "LSP-Ping option" respectively in the rest of the document.

Conventions used in this document

In examples, "C:" and "S:" indicate lines sent by the client and server respectively.

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 [3].

2. Terminology

ACH: Associated Channel Header

LSR: Label Switching Router

MEP: Maintenance Entity Group End Point

MIP: Maintenance Entity Group Intermediate Point.

MPLS-TP: MPLS Transport Profile

MPLS-OAM: MPLS Operations, Administration and Maintenance

MPLS-TP LSP: Bidirectional Label Switch Path representing a circuit

NMS: Network Management System

TLV: Type Length Value

TTL: Time To Live

LI-LB: Lock instruct-Loopback

3. MPLS-TP Loopback/Lock Mechanism

For the in-band option, the proposed mechanism uses a new code point in the Associated Channel Header (ACH) described in [6].

3.1. In-band Message Identification

In the in-band option, the MPLS-TP LI-LB channel is identified by the ACH as defined in RFC 5586 [6] with the Channel Type set to the MPLS-TP LI-LB code point = 0xHH. [HH to be assigned by IANA from the PW Associated Channel Type registry] The LI-LB Channel does not use ACH TLVs and MUST not include the ACH TLV header. The LI-LB ACH Channel is shown below.

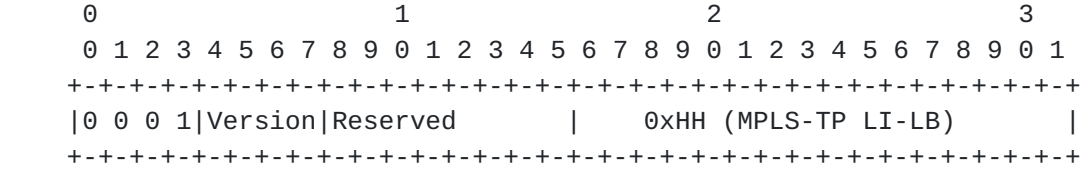
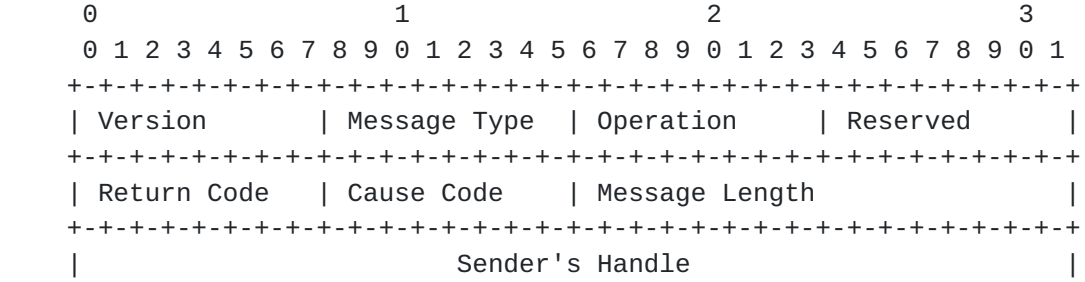


Figure 1: ACH Indication of MPLS-TP LI-LB

The LI-LB Channel is 0xHH (to be assigned by IANA)

3.2. MPLS LI-LB Message Format

The format of an MPLS-TP LI-LB Message is shown below.



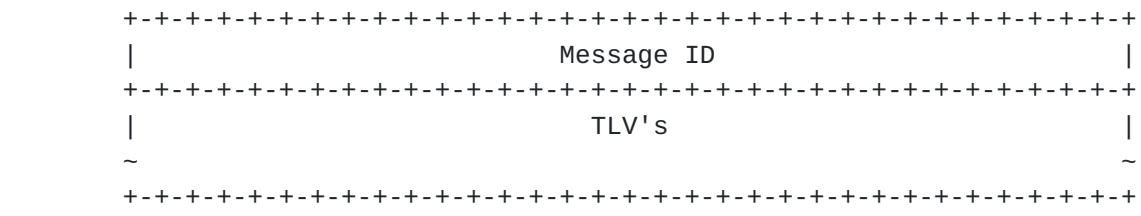


Figure 2: MPLS LI-LB Message Format

Version: The Version Number is currently 1. (Note: the version number is to be incremented whenever a change is made that affects the ability of an implementation to correctly parse or process the request/response message. These changes include any syntactic or semantic changes made to any of the fixed fields, or to any Type-Length-Value (TLV) or sub-TLV assignment or format that is defined at a certain version number. The version number may not need to be changed if an optional TLV or sub-TLV is added.)

Message Type

Two message types are defined as shown below.

Message Type	Description
0x0	LI-LB request
0x1	LI-LB response

Operation

Four operations are defined as shown below. The operations can appear in a Request or Response message.

Operation	Description
0x1	Lock
0x2	Unlock
0x3	Set_Loopback
0x4	Unset_Loopback

Message Length

The total length of any included TLVs.

Sender's Handle

The Sender's Handle is filled in by the sender, and returned unchanged by the receiver in the MPLS response message (if any).

There are no semantics associated with this handle, although a sender may find this useful for matching up requests with replies.

Message ID

The Message ID is set by the sender of an MPLS request message. It MUST be copied unchanged by the receiver in the MPLS response message (if any). A sender SHOULD increment this value on each new message. A retransmitted message SHOULD leave the value unchanged.

Return code

Value	Meaning
0	Informational
1	Success
2	Failure

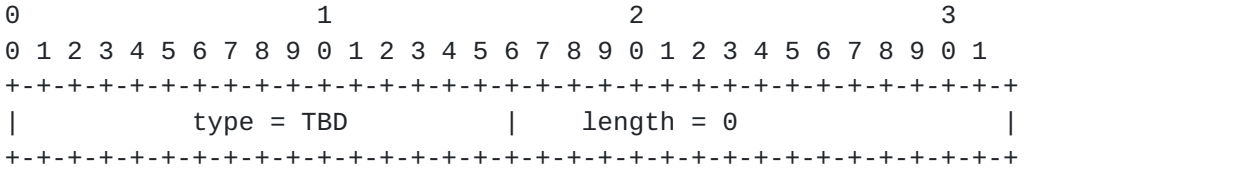
Cause code

Value	Meaning
0	No cause code
1	Fail to match target MIP/MEP ID
2	Malformed request received
3	One or more of the TLVs is/are unknown
4	Authentication failed
5	MPLS-TP LSP/PW already locked
6	MPLS-TP LSP/PW already unlocked
7	Fail to lock MPLS-TP LSP/PW
8	Fail to unlock MPLS-TP LSP/PW
9	MPLS-TP LSP/PW already in loopback mode
10	MPLS-TP LSP/PW is not in loopback mode
11	Fail to set MPLS-TP LSP/PW in loopback mode
12	Fail to remove MPLS-TP/PW from loopback mode
13	No label binding for received message

The Return code and Cause code only have meaning in a Response message. In a request message the Return code and Cause code must be set to zero and ignored on receipt.

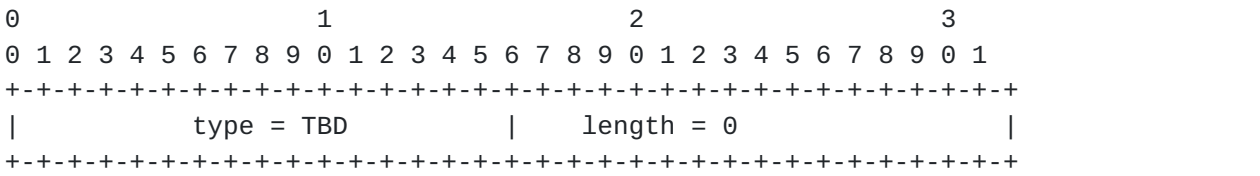
3.3. LSP Ping Extensions

3.3.1. Lock Request TLV



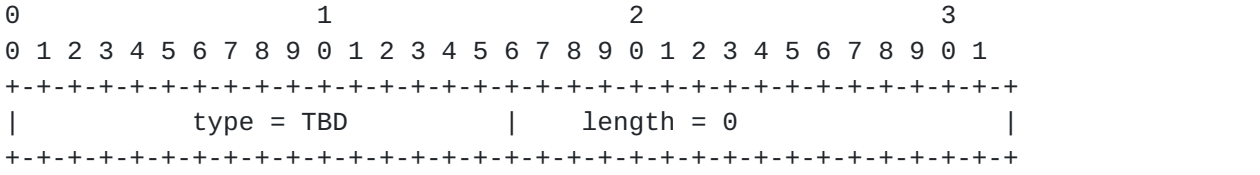
A MEP includes a Lock Request TLV in the MPLS LSP Ping echo request message to request the MEP on the other side of the MPLS-TP LSP to take the LSP out of service.

3.3.2. Unlock Request TLV



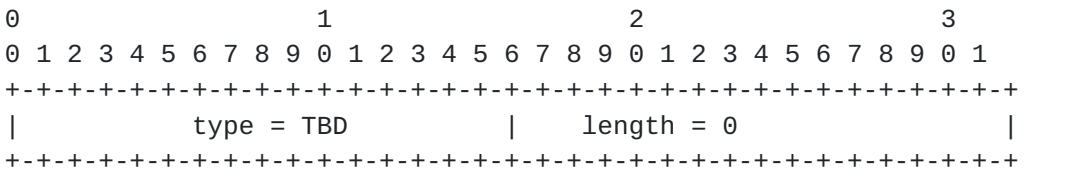
The Unlock Request TLV is sent from the MEP which has previously sent lock request. Upon receiving the LSP Ping Echo request message with the unlock request TLV, the receiver MEP brings the MPLS-TP LSP back in service.

3.3.3. Loopback Request TLV



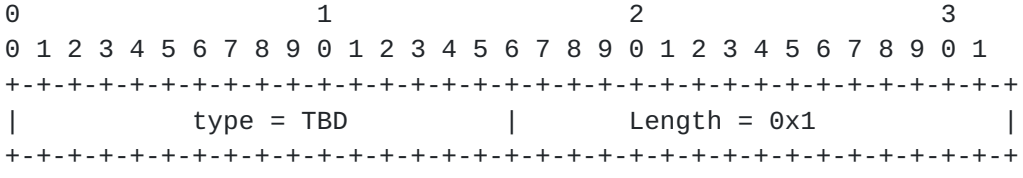
When a MEP wants to put an MPLS-TP LSP in loopback mode, it sends a MPLS LSP Ping echo request message with Loopback Request TLV. The message can be intercepted by either a MIP or a MEP depending on the MPLS TTL value. The receiver puts in corresponding MPLS-TP LSP in loopback mode.

3.3.4. Loopback Removal TLV



When loopback mode operation of an MPLS-TP LSP is no longer required, the MEP that previously sent the MPLS LSP Ping echo request message with a loopback TLV, sends another MPLS LSP Ping echo request message with a Loopback Removal TLV. The receiver MEP changes the MPLS-TP LSP from loopback mode to normal mode of operation.

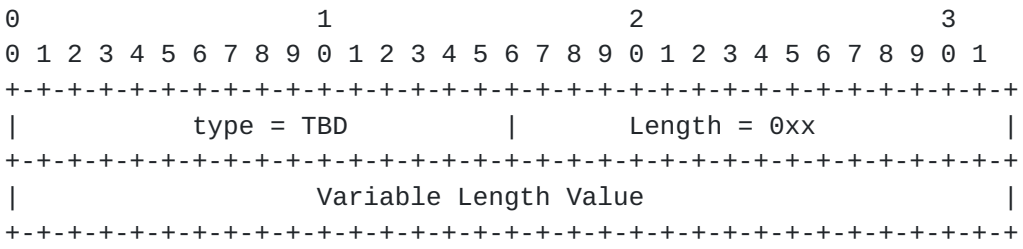
3.3.5. Response TLV



Value	Return code Meaning
0	Success
1	Fail to match target MIP/MEP ID
2	Malformed loopback request received
3	One or more of the TLVs is/are unknown
4	Authentication failed
5	MPLS-TP LSP/PW already locked
6	MPLS-TP LSP/PW already unlocked
7	Fail to lock MPLS-TP LSP/PW
8	Fail to unlock MPLS-TP LSP/PW
9	MPLS-TP LSP/PW already in loopback mode
10	MPLS-TP LSP/PW is not in loopback mode
11	Fail to set MPLS-TP LSP/PW in loopback mode
12	Fail to remove MPLS-TP LSP/PW from loopback mode
13	No label binding for received message

Note that in the case of error code 3, the unknown TLV can also be optionally included in the response TLV.

3.3.6. Authentication TLV



Mechanisms similar to PPP Chap can be used to authenticate the Loopback request. A variable length key can be carried in an optional authentication TLV which can be included in the MPLS OAM LSP Ping echo request message containing a loopback request TLV or the LI-LB Message. The use of authentication key is outside the scope of the document.

4. Loopback/Lock Operations

4.1. Lock Request

Lock Request is used to request a MEP to take an MPLS-TP LSP out of service so that some form of maintenance can be done.

The receiver MEP MUST send either an ACK or a NAK response to the sender MEP. Until the sender MEP receives an ACK, it MUST NOT assume that the receiver MEP has taken the MPLS-TP LSP out of service. A receiver MEP sends an ACK only if it can successfully lock the MPLS-TP LSP. Otherwise, it sends a NAK.

4.2. Unlock Request

The Unlock Request is sent from the MEP which has previously sent lock request. Upon receiving the unlock request message, the receiver MEP brings the MPLS-TP LSP back in service.

The receiver MEP MUST send either an ACK or a NAK response to the sender MEP. Until the sender MEP receives an ACK, it MUST NOT assume that the MPLS-TP LSP has been put back in service. A receiver MEP sends an ACK only if the MPLS-TP LSP has been unlocked, and unlock operation is successful. Otherwise, it sends a NAK.

4.3. Loopback Request

When a MEP wants to put an MPLS-TP LSP in loopback mode, it sends a Loopback request message. The message can be intercepted by either a MIP or a MEP depending on the MPLS TTL value. The receiver puts in corresponding MPLS-TP LSP in loopback mode.

The receiver MEP or MIP MUST send either an ACK or NAK response to the sender MEP. An ACK response is sent if the MPLS-TP LSP is successfully put in loopback mode. Otherwise, a NAK response is sent. Until an ACK response is received, the sender MEP MUST NOT assume that the MPLS-TP LSP can operate in loopback mode.

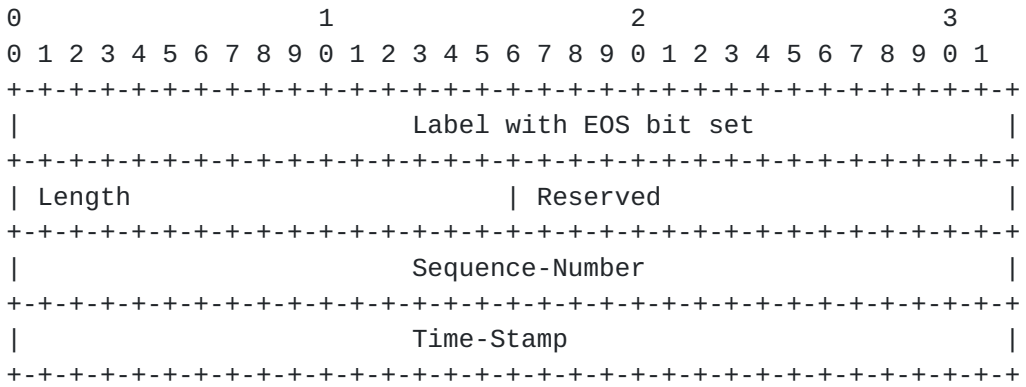
4.4. Loopback Removal

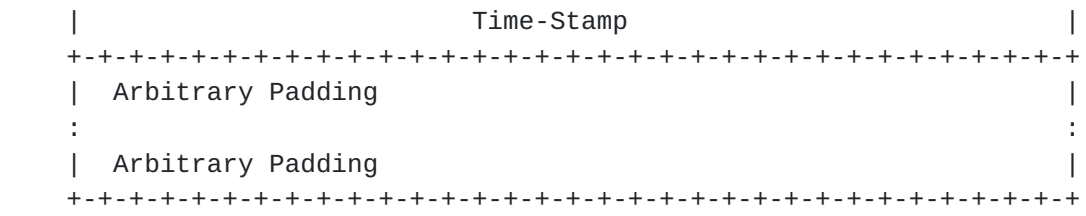
When loopback mode operation of an MPLS-TP LSP is no longer required, the MEP that previously sent the Loopback request message sends another Loopback Removal message. The receiver MEP changes the MPLS-TP LSP from loopback mode to normal mode of operation.

The receiver MEP or MIP MUST send either an ACK or NAK response to the sender MEP. An ACK response is sent if the MPLS-TP LSP is already in loopback mode, and if the MPLS-TP LSP is successfully put back in normal operation mode. Otherwise, a NAK response is sent. Until an ACK response is received, the sender MEP MUST NOT assume that the MPLS-TP LSP is put back in normal operation mode.

5. Data packets

Data packets sent from the sender MEP will be looped back to that sender MEP. In order for the sender MEP node to make sure that no data packets are dropped, each data MPLS packets may contain a sequence-id right after the label stack. A time-stamp fields in the data packets can help calculate the Round trip delay of datapackets. The Local Time-Stamp is set by the sender, and can be used to calculate the round trip delay after the message is looped back.





6. Operation

6.1. General Procedures

When placing an LSP into Loopback mode, the operation MUST first be preceded by a Lock operation.

Sending LSP Ping Echo Request message with Loopback Request/Removal or in-Band Loopback Request/Removal Message

The TTL of the topmost label is set as follows:-

If the target node is a MIP, the TTL MUST be set to the exact number of hops required to reach that MIP.

If the target node is a MEP, the value MUST be set to at least the number of hops required to reach that MEP. For most operations where the target is a MEP, the TTL MAY be set to 255.

However, to remove a MEP from Loopback mode, the sending MEP MUST set the TTL to the exact number of hops required to reach the MEP (if the TTL were set higher, the Loopback removal message would be looped back toward the sender). It is RECOMMENDED that the TTL be set to the exact number of hops required to reach the MEP.

6.2. Example Topology

The next four sections discuss the procedures for Locking, Unlocking, setting an LSP into loopback, and removing the loopback. The description is worded using an example. Assume an MPLS-TP LSP traverses nodes A <--> B <--> C <--> D. We will refer to the Maintenance Entities involved as MEP-A, MIP-B, MIP-C, and MEP-D respectively. Suppose a maintenance operation invoked at node A requires a loopback be set at node C. To invoke Loopack mode at node C, A would first need to lock the LSP. Then it may proceed to set the loopback at C. Following the loopback operation, A would need to remove the loopback at C and finally unlock the LSP.

The following sections describe MEP-A setting and unsetting a lock at MEP-D and then setting and removing a loopback at MIP-C.

6.3. Locking an LSP

1. MEP-A sends an MPLS LSP Ping Echo request message with the Lock TLV or an in-Band Lock request Message. Optionally, an authentication TLV MAY be included.

2. Upon receiving the request message, D uses the received label stack and the Target FEC/source MEP-ID to identify the LSP. If no label binding exists or there is no associated LSP back to the originator, the event is logged. Processing ceases. Otherwise the message is delivered to the target MEP.

a. if the source MEP-ID does not match, the event is logged and processing ceases.

b. if the target MEP-ID does not match, MEP-D sends a response with error code 1.

MEP-D then examines the message, and:

c. if the message is malformed, it sends a response with error code 2 back to MEP-A.

d. if message authentication fails, it MAY send a response with error code 4 back to MEP-A.

e. if any of the TLVs is not known, it sends a response with error code 3 back to MEP-A. It may also include the unknown TLVs.

f. if the MPLS-TP LSP is already locked, it sends a response with error code 5 back to MEP-A.

g. if the MPLS-TP LSP is not already locked and cannot be locked, it sends a response with error code 7 back to A.

h. if the MPLS-TP LSP is successfully locked, it sends a response with error code 0 (Success) back to MEP-A.

The response is sent using an MPLS LSP Ping echo reply with a response TLV or an in-Band Lock response message. An authentication TLV MAY be included.

6.4. Unlocking an LSP

1. MEP-A sends an MPLS Echo request message with the unLock TLV or an in-Band unLock request Message. Optionally, an authentication TLV MAY be included.

2. Upon receiving the unLock request message, D uses the received label stack and target FEC/source MEP-ID to identify the LSP. If no

label binding exists or there is no associated LSP back to the originator, the event is logged. Processing ceases. Otherwise the message is delivered to the target MEP.

a. if the source MEP-ID does not match, the event is logged and processing ceases.

b. if the target MEP-ID does not match, MEP-D sends a response with error code 1.

MEP-D then examines the message, and:

c. if the message is malformed, it sends a response with error code 2 back to MEP-A.

d. if message authentication fails, it MAY send a response with error code 4 back to MEP-A.

e. if any of the TLVs is not known, it sends a response with error code 3 back to MEP-A. It may also include the unknown TLVs.

f. if the MPLS-TP LSP is already unlocked, it sends a response with error code 6 back to MEP-A.

g. if the LSP is locked and cannot be unlocked, it sends a response with error code 8 back to MEP-A.

h. if the LSP is successfully unlocked, it sends a response with error code 0 (Success) back to MEP-A.

The response is sent using an MPLS LSP Ping echo reply with a response TLV or an in-Band unlock response message. An authentication TLV MAY be included.

6.5. Setting an LSP into Loopback mode

1. MEP-A sends an MPLS LSP Ping Echo request message with the loopback TLV or an in-Band Loopback request message. Optionally, an authentication TLV MAY be included.

2. Upon intercepting the MPLS Loopback message via TTL expiration, C uses the received label stack and target FEC/source MEP-ID to identify the LSP.

If no label binding exists or there is no associated LSP back to the originator, the event is logged. Processing ceases.

Otherwise the message is delivered to the target MIP/MEP - in this case MIP-C.

a. if the source MEP-ID does not match, the event is logged and processing ceases.

b. if the target MIP-ID does not match, MIP-C sends a response with error code 1.

MIP-C then examines the message, and:

c. if the message is malformed, it sends a response with error code 2 back to MEP-A.

d. if the message authentication fails, it sends a response with error code 4 back to MEP-A.

e. if any of the TLV is not known, C sends a response with error code 3 back to MEP-A. It may also include the unknown TLVs.

f. if the MPLS-TP LSP is already in the requested loopback mode, it sends a response with error code 9 back to MEP-A.

g. if the MPLS-TP LSP is not already in the requested loopback mode and that loopback mode cannot be set, it sends a response with error code 11 back to MEP-A.

h. if the MPLS-TP LSP is successfully programmed into the requested loopback mode, it sends a response with error code 0 (Success) back to MEP-A.

The response is sent using an MPLS LSP Ping echo reply with a response TLV or an in-Band Loopback response message. An authentication TLV MAY be included.

6.6. Removing an LSP from Loopback mode

1. MEP-A sends a MPLS LSP Ping Echo request message with the Loopback removal TLV or an in-Band Loopback removal request message. Optionally, an authentication TLV MAY be included.

2. Upon intercepting the MPLS Loopback removal message via TTL expiration, C uses the received label stack and the target FEC/source MEP-ID to identify the LSP.

If no label binding exists or there is no associated LSP back to the originator, the event is logged. Processing ceases.

Otherwise the message is delivered to the target MIP/MEP - in this case MIP-C.

a. if the source MEP-ID does not match, the event is logged and processing ceases.

b. if the target MIP-ID does not match, MIP-C sends a response with error code 1 back to MEP-A.

MIP-C then examines the message, and:

c. if the message is malformed, it sends a response with error code 2 back to MEP-A.

d. if the message authentication fails, it sends a response with error code 4 back to MEP-A.

e. if any of the TLV is not known, C sends a response with error code 3 back to MEP-A. It may also include the unknown TLVs.

f. if the MPLS-TP is not in loopback mode, it sends a response with error code 10 back to MEP-A.

g. if the MPLS-TP LSP loopback cannot be removed, it sends a response with error code 12 back to MEP-A.

h. if the MPLS-TP is successfully changed from loopback mode to normal mode of operation, it sends a reply with error code 0 (Success) back to MEP-A.

The response is sent using an MPLS LSP Ping echo reply with a response TLV or an in-Band Loopback removal response message. An authentication TLV MAY be included.

7. Security Considerations

The security considerations for the authentication TLV need further study.

8. IANA Considerations

TBD

9. References

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

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

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

[5] N. Bahadur, et. al., "MPLS on-demand Connectivity Verification, Route Tracing and Adjacency Verification", draft-nitinb-mpls-tp-on-demand-cv-00, work in progress, June 2010

[6] Bocci, M., Vigoureux, M., and S. Bryant, "MPLS Generic Associated Channel", RFC 5586, June 2009.

[7] Bocci, M. and G. Swallow, "MPLS-TP Identifiers", draft-ietf-mpls-tp-identifiers-01 (work in progress), June 2010.

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

9.2. Informative References

[9] Nabil Bitar, et. al, "Requirements for Multi-Segment Pseudowire Emulation Edge-to-Edge (PWE3) ", RFC5254, October 2008.

Author's Addresses

Sami Boutros
Cisco Systems, Inc.
Email: sboutros@cisco.com

Siva Sivabalan
Cisco Systems, Inc.
Email: msiva@cisco.com

Rahul Aggarwal
Juniper Networks.
EMail: rahul@juniper.net

Martin Vigoureux
Alcatel-Lucent.
Email: martin.vigoureux@alcatel-lucent.com

Xuehui Dai
ZTE Corporation.
Email: dai.xuehui@zte.com.cn

George Swallow
Cisco Systems, Inc.
Email: swallow@cisco.com

David Ward
Juniper Networks.
Email: dward@juniper.net

Stewart Bryant
Cisco Systems, Inc.
Email: stbryant@cisco.com

Carlos Pignataro
Cisco Systems, Inc.
Email: cpignata@cisco.com

Nabil Bitar
Verizon.
Email: nabil.bitar@verizon.com

Italo Busi
Alcatel-Lucent.
Email: italo.busi@alcatel-lucent.it

Lieven Levrau
Alcatel-Lucent.
Email: llevrau@alcatel-lucent.com

Laurent Ciavaglia
Alcatel-Lucent.
Email: laurent.ciavaglia@alcatel-lucent.com

Bo Wu
ZTE Corporation.
Email: wu.bo@zte.com.cn

Jian Yang
ZTE Corporation.
Email: yang_jian@zte.com.cn

Full Copyright Statement

Intellectual Property Statement

those that are translated into other languages, should not be considered to be definitive versions of these Legal Provions.

For the avoindance od doubt, each Contributor to the UETF Standards Process licenses each Contribution that he or she makes as part of the IETF Standards Process to the IETF Trust pursuant to the provisions of RFC 5378. No language to the contrary, or terms, conditions or rights that differ from or are inconsistent with the rights and licenses granted under RFC 5378, shall have any effect and shall be null and void, whether published or posted by such Contributor, or included with or in such Contribution.

Acknowledgment

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