Operating MPLS Transport Profile LSP in Loopback Mode

draft-boutros-mpls-tp-loopback-01.txt

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on June 16, 2009.

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) in loopback mode for management purpose. This extension can be used to loop either all traffic (i.e., data and control traffic) or only OAM traffic up to certain LSR on the path of the MPLS-TP LSP back to the source.

Table of Contents

1. Introduction .................................................. 2
2. Terminology ................................................... 4
3. MPLS-TP Loopback Mechanism .................................. 5
4. MPLS-OAM Loopback Message ................................... 5
   4.1. Lock Request TLV ........................................ 6
   4.2. Unlock Request TLV ....................................... 6
   4.3. Loopback Request TLV ..................................... 7
   4.4. Loopback Removal TLV .................................... 7
   4.5. Authentication TLV ....................................... 8
   4.6. Source Identifier TLV .................................. 8
   4.7. Target Identifier TLV ................................... 10
   4.8. Response TLV ........................................... 10
   4.9. Data packets ........................................... 11
   4.10. Network Management System ............................. 12
5. Operation .................................................... 12
6. Security Considerations ....................................... 15
7. IANA Considerations .......................................... 16
   TBD .......................................................... 16
8. References .................................................... 16
   8.1. Normative References .................................... 16
   8.2. Informative References .................................. 16
Author's Addresses ............................................... 17
Full Copyright Statement ........................................ 18
Intellectual Property Statement ............................... 18

1. Introduction

In traditional transport networks, circuits are provisioned on multiple switches and service providers operate the transport circuit such as T1 line in loopback mode for management purpose, e.g., to test connectivity of the circuit up to a specific switch 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. In this document, an MPLS-TP LSP means either MPLS transport LSP or MPLS Pseudowire (PW).

To describe the loopback functionality, let us assume a bi-directional MPLS-TP LSP A <--- B <--- C where A, B, and C are MPLS
capable nodes. Also, let us assume that the network operator requires B to loop the packets sent from A back to A. In this example, A and C acts as Maintenance End Points (MEPs) and B acts as a Maintenance Intermediate Point (MIP). The operator can setup the MPLS-TP LSP into loopback mode such that:

1. B loops all the packets (regardless of whether they are data or control packets) back to A. We refer to this mode "Full Loopback" (FLB).

2. B loops only the OAM packets back to A, and all other packets from A are sent towards C. We refer to this mode "OAM Loopback" (OLB).

The operator can optionally take the MPLS-TP LSP out of service before setting up the MPLS-TP LSP in loopback mode. In that case, A sends an in-band MPLS OAM message along the MPLS-TP LSP to lock the MPLS-TP LSP. The message will be intercepted by C since it is at the end of the LSP. C responds to the lock request with an ACK OAM message. If the operator does not want to take MPLS-TP LSP out of service before setting it up into loopback mode, A does not have to send lock OAM message.

In order to setup the MPLS-TP LSP in loopback mode, A sends another in-band OAM message with the correct MPLS TTL value so that the message will be intercepted by B because of the MPLS TTL expiry. The second MPLS OAM message contains a request to instruct B to operate the corresponding MPLS-TP LSP in either Full Loopback mode or OAM Loopback mode. B sends an ACK/NAK OAM message back to A to indicate whether or not it has successfully setup the MPLS-TP LSP in the required loopback mode. In the case of NAK, the OAM reply message contains an error code. Upon receiving a NAK reply to the loopback request, A sends another MPLS OAM message to unlock the MPLS-TP LSP in case it was previously locked. The unlock MPLS OAM message is intercepted by C as it is at the end of the LSP.

When the MPLS-TP LSP operates in FLB mode, all the packets (data and control) from are looped back at B. When operating the MPLS-TP LSP in OLB, B loops only the OAM packets back to A. When the loopback operation is no longer required, A sends another MPLS OAM message to remove the loopback operation mode, and the MPLS TTL is set such that this message is intercepted by B. It is expected that B sends a reply back to A to ACK/NAK the loopback mode removal request. Upon getting an ACK response to loopback mode removal request, A may send another in-band MPLS OAM message to unlock the MPLS-TP LSP, in case the MPLS-TP LSP was previously locked as mentioned above. The unlock MPLS OAM packet is intercepted by C as it is at the end of the MPLS-TP LSP.
The proposed mechanism is based on a set of new TLVs which can be transported using one of the following methods:

1. Using in-band MPLS OAM messages which are forwarded as MPLS packets (non-IP based).

2. Using LSP-Ping extensions defined in [4] where IP/UDP packets are used (IP-based). The LSP-Ping messages are sent using the codepoint defined in [3].

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. Error! Reference source not found.

2. Terminology

ACH: Associated Channel Header

FLB: Full Loopback

LSR: Label Switching Router

MEP: Maintenance End Point

MIP: Maintenance 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

OLB: OAM Loopback

TLV: Type Length Value
3. MPLS-TP Loopback Mechanism

For the in-band option, the proposed mechanism uses a new code point in the Associated Channel Header (ACH) described in [5].

The LSP-Ping option will be in compliance to specifications [3],[4], and [6].

Also, the proposed mechanism requires a set of new TLVs called Loopback Request TLV, Loopback Removal TLV, Lock Request TLV, Lock Removal TLV, Source Address TLV, Target Address TLV, Authentication Request TLV, and Response TLV. These TLVs are described below.

4. MPLS-OAM Loopback Message

In the in-band option, under MPLS label stack of the MPLS-TP LSP, the ACH with "MPLS-TP Loopback" code point indicates that the message is an MPLS OAM Loopback message. In addition, a 32-bit field is added to carry the message ID and the message length as shown below:

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 0 0 0|0 0 0 0|0 0 0 0 0 0 0 0|0xHH (MPLS-TP Loopback) |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0| Message ID |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0| Message Length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: MPLS-TP OAM Message Header

First nibble = 0001b.

The version and the reserved values are both set to 0 as specified in [1].

MPLS-TP loopback code point = 0xHH

The Message ID is set by the sender. The receiver MUST include the Message ID in the response. This way, the sender can correlate a reply with the corresponding request.
The Message Length is the total length of the message in bytes excluding the length of the MPLS-TP OAM message header.

4.1. Lock Request TLV

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           type = TBD          |    length = 0                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Lock Request TLV is used to request a MEP to take an MPLS-TP LSP out of service so that some form of maintenance can be done on the MPLS-TP. A MEP includes a Lock Request TLV in the MPLS OAM message to request the MEP on the other side of the MPLS-TP LSP to take the MPLS-TP LSP out of service.

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

4.2. Unlock Request TLV

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           type = TBD          |    length = 0                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

The receiver MEP MUST send either an ACK or a NAK response to the sender MEP using an MPLS OAM message with a Response TLV described below. 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 TLV

When a MEP wants to put an MPLS-TP in loopback mode, it sends a MPLS OAM message with Loopback Request TLV. The loopback 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 value of the flag is used to identify the loopback mode as follows:

<table>
<thead>
<tr>
<th>Flag Value</th>
<th>Loopback Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0</td>
<td>OLB</td>
</tr>
<tr>
<td>0x1</td>
<td>FLB</td>
</tr>
</tbody>
</table>

The receiver MEP or MIP MUST send either an ACK or NAK response to the sender MEP using an MPLS OAM message with a Response TLV described below. 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 TLV

When loopback mode operation of an MPLS-TP LSP is no longer required, the MEP that previously sent the MPLS OAM loopback message sends another MPLS OAM message with a Loopback Removal TLV. The receiver MEP change 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 using an MPLS OAM message with a Response TLV described below. 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.

4.5. Authentication TLV

Mechanisms similar to PPP Chap can be used to authenticate the MPLS OAM Loopback request. A variable length key can be carried in an optional authentication TLV which can be included in the MPLS OAM loopback request message. The use of authentication key is outside the scope of the document.

4.6. Source Identifier TLV

While setting up an MPLS-TP LSP in loopback mode, the sender MEP can include its ID in the Source Identifier TLV. The ID can be in IPv4, IPv6, or PW FEC (128 or 129) formats on can be any of the LSP IDs defined in [4]. The length field represents the length (in bytes) of only the source identifier. Depending on the format, type and length are interpreted as follows:

<table>
<thead>
<tr>
<th>Format</th>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP FEC TLVs defined in [4]</td>
<td>Variable</td>
<td></td>
</tr>
</tbody>
</table>
IPv4 address                        TBD              4
IPv6 address                        TBD              16
FEC 128 Pseudo Wire Identifier      TBD              4
FEC 129 Pseudo Wire Identifier      TBD              Variable

In the case of FEC 129, the source is identified by AGI, SAII, and TAI as follows:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   AGI Type    |    Length     |         AGI Value             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      AGI Value (contd.)                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   AII Type    |    Length     |        SAII Value             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     SAII Value (contd.)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   AII Type    |    Length     |        TAI Value              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     TAI Value (contd.)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

For more details on AGI, SAII, and TAI, please refer to [2].

The use of the Source Identifier TLV is outside the scope of this document.
4.7. Target Identifier TLV

While setting up an MPLS-TP LSP in loopback mode, the sender MEP can include the target ID in the Target Identifier TLV. The format exactly the same as the Source Identifier TLV described above.

The use of the Target Identifier TLV is outside the scope of this document.

4.8. Response TLV

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No error code</td>
</tr>
<tr>
<td>1</td>
<td>Success</td>
</tr>
<tr>
<td>2</td>
<td>Malformed loopback request received</td>
</tr>
<tr>
<td>3</td>
<td>One or more of the TLVs is/are unknown</td>
</tr>
<tr>
<td>4</td>
<td>Authentication failed</td>
</tr>
<tr>
<td>5</td>
<td>MPLS-TP LSP is locked</td>
</tr>
<tr>
<td>6</td>
<td>MPLS-TP LSP is not locked</td>
</tr>
</tbody>
</table>
7    Fail to lock MPLS-TP LSP
8    Fail to unlock MPLS-TP LSP
9    MPLS-TP LSP is in loopback mode
10   MPLS-TP is not in loopback mode
11   Fail to set MPLS-TP LSP in loopback mode
12   Fail to remove MPLS-TP from loopback mode
13   Fail to match target ID

Note that in the case of error code 2, the unknown TLV can also be optionally included in the response TLV.

4.9. Data packets

When an MPLS-TP LSP operates in FLB mode, data packets sent from the sender MEP will be looped back to that sender MEP. In order for the sender MEP to make ensure 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 datapackets can help calculate the Round trip delay of datapackets. The Local Time-Stamp is set by the sender, and the Remote Time-Stamp field is set by the receiver. Using these time-stamp values, sender can calculate the round trip delay as well as the breakdown of the delay in the forward path (from the sender to the receiver) and reverse path (from the receiver to the sender).
Internet-Draft  draft-boutros-mpls-tp-loopback-01.txt  December 2008

<table>
<thead>
<tr>
<th>0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS Label stack</td>
</tr>
<tr>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Label with EOS bit set</td>
</tr>
<tr>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Optional Sequence-ID</td>
</tr>
<tr>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Local Time-Stamp</td>
</tr>
<tr>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Remote Time-Stamp</td>
</tr>
</tbody>
</table>

4.10. Network Management System

An operator should be able to provision any given LSR to:

1. lock/Unlock any MPLS-TP LSP.

2. setup any MPLS-TP LSP in loopback mode (either FLB or OLB). should have the capability to Network Management System (NMS) may also be used to setup an MPLS-TP LSP in loopback mode (either FLB or OLB).

3. send MPLS OAM packets from a MEP and notify NMS when MPLS OAM response arrives.

When NMS is used to provision any of the above the functionality, the corresponding MPLS OAM message is not used.

5. Operation

Assume an MPLS-TP LSP A -- B -- C, and A wants to request B to set the MPLS-TP LSP in loopback mode. The following steps are carried out:

1. A can optionally send an MPLS-OAM loopback request message. The message can be an in-band message in the MPLS-LSP consisting of an ACH with the MPLS-TP loopback code, Lock TLV, and optional authentication TLV to C. The MPLS label stack of the LSP is added and the MPLS TTL value is set to 255. The message can also use the LSP-Ping IP/UDP option, and in this case the message contains all the above TLVs but does not contain the ACH.
2. Upon intercepting the MPLS-OAM message, C examines the message, and:
   
a. if the message is malformed, it sends a response with the error code 2 back to A.
   
b. if any of the TLV is not known, it sends a response with error code 3 back to A. It may also include the unknown TLVs.
   
c. if message authentication fails, it sends a response with the error code 4 back to A.
   
d. if the MPLS-TP is already locked, it sends a response with error code 5 back to A.
   
e. if the MPLS-TP is not already locked and cannot be locked, it sends a response with error code 7 back to A.
   
f. if the MPLS-TP is successfully locked, it sends a response an error code 1 (success) back to A.
   
   Note that MPLS TTL value is set to 255 in the response message.

3. Upon receiving the MPLS-OAM response message with error code 1, A sends an MPLS-OAM loopback request message using either the in-band or LSP-Ping option to B. The loopback request can be for either FLB or OLB mode. The message can optionally have an Authentication TLV, and Source Identifier TLV and a Target Identifier TLV. The MPLS label stack of the LSP is added and the MPLS TTL value is set to the number of hops between A and B.

4. Upon intercepting the MPLS-OAM message, B examines the message, and:
   
a. if the message is malformed, it sends a response with error code 2.
   
b. if any of the TLV is not known, B sends a response with error code 3. It may also include the unknown TLVs.
   
c. if the message authentication fails, it sends a response with error code 4.
   
d. Target ID cannot be matched, it sends a response with error code 13.
B identifies the MPLS-TP LSP, and if the request is for OLB mode, it sends a reply with error code 1 (success). If the request is for FLB mode:

a. if the MPLS-TP is already in FLB mode, it sends a response with error code 9.

b. if the MPLS-TP is successfully programmed into FLB mode, it sends a reply with error code 1 (success).

5. After receiving a positive reply from B, and if the request is for FLB mode, A can send data packets on the MPLS-TP LSP to B, and expect those packets to loopback to itself. The data packets contains sequence numbers to check for packet loss.

6. B simply loops the data packets coming over the MPLS-TP LSP back towards the source. The MPLS label stack of the LSP is added and the MPLS TTL value is set to 255.

To unlock the MPLS-TP LSP:

1. A sends an MPLS-OAM loopback request message. The message can be an in-band message in the MPLS-LSP consisting of an ACH with the MPLS-TP Loopback code, Unlock Request TLV and optionally an authentication TLV. The MPLS label stack of the LSP is added and the MPLS TTL value is set to 255. The message can also use the LSP-Ping option in which case the ACH is not used but all others TLVs are included in the message.

2. Upon intercepting the MPLS-OAM message, C examines the message, and:

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

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

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

C identifies the MPLS-TP LSP:

a. if the MPLS-TP is not locked, it sends a response with error code 6 back to A.
b. if the MPLS-TP is locked and cannot be unlocked, it sends a response with error code 8 back to A.

c. if the MPLS-TP is successfully unlocked, it sends a response with error code 1 (success) back to A.

To remove MPLS-TP LSP from FLB mode:

1. A sends an MPLS-OAM loopback request message, using either in-band or LSP-Ping option to B, consisting Loopback Removal Request TLV and optionally an authentication TLV. The MPLS label stack of the LSP is added and the MPLS TTL value is set to the number of hops between A and B.

2. Upon intercepting the MPLS-OAM message, B examines the message and:

   a. if the message is malformed, it sends a response with error code 2.

   b. if any of the TLV is not known, B sends a response with error code 3. It may also include the unknown TLVs.

   c. if the message authentication fails, it sends a response with error code 4.

   d. if the target ID is matched, it sends a response with error code 13.

B identifies the MPLS-TP LSP:

   c. if the MPLS-TP is not in loopback mode, it sends a response with error code 10.

   d. if the MPLS-TP is successfully changed from loopback mode to normal mode of operation, it sends a reply with error code 1 (success).

6. Security Considerations

The security considerations for the authentication TLV need further study.
7. IANA Considerations

    TBD

8. References

8.1. Normative References


8.2. Informative References


Author’s Addresses

Sami Boutros  
Cisco Systems, Inc.  
3750 Cisco Way  
San Jose, California 95134  
USA  
Email: sboutros@cisco.com

Siva Sivabalan  
Cisco Systems, Inc.  
2000 Innovation Drive  
Kanata, Ontario, K2K 3E8  
Canada  
Email: msiva@cisco.com

George Swallow  
Cisco Systems, Inc.  
300 Beaver Brook Road  
Boxborough, MAASSACHUSETTS 01719  
United States  
Email: swallow@cisco.com

David Ward  
Cisco Systems, Inc.  
3750 Cisco Way  
San Jose, California 95134  
USA  
Email: wardd@cisco.com

Rahul Aggarwal  
Juniper Networks  
1194 N.Mathilda Ave  
Sunnyvale, CA 94089  
USA  
EMail: rahul@juniper.net

Nabil Bitar  
Verizon  
40 Sylvan Road Waltham, MA 02145  
USA  
e-mail: nabil.bitar@verizon.com
of IETF Documents. The definitive version of these Legal Provisions is that published by, or under the auspices of, the IETF. Versions of these Legal Provisions that are published by third parties, including those that are translated into other languages, should not be considered to be definitive versions of these Legal Provisions.

For the avoidance of doubt, each Contributor to the IETF 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.