PCE Working Group   U. Palle
Internet-Draft   D. Dhody
Intended status: Standards Track   Huawei Technologies
Expires: November 14, 2017   Y. Tanaka
                                                   NTT Communications
                                                            V. Beeram
                                                     Juniper Networks
                                                         May 13, 2017

   Path Computation Element (PCE) Protocol Extensions for Stateful PCE
    usage for Point-to-Multipoint Traffic Engineering Label Switched Paths
                   draft-ietf-pce-stateful-pce-p2mp-03

Abstract

   The Path Computation Element (PCE) has been identified as an
   appropriate technology for the determination of the paths of point-
   to-multipoint (P2MP) TE LSPs. This document provides extensions
   required for Path Computation Element communication Protocol (PCEP)
   so as to enable the usage of a stateful PCE capability in supporting
   P2MP TE LSPs.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

As per [RFC4655], the Path Computation Element (PCE) is an entity
that is capable of computing a network path or route based on a
network graph, and applying computational constraints. A Path
Computation Client (PCC) may make requests to a PCE for paths to be
computed.

[RFC4857] describes how to set up point-to-multipoint (P2MP) Traffic
Engineering Label Switched Paths (TE LSPs) for use in Multiprotocol
Label Switching (MPLS) and Generalized MPLS (GMPLS) networks. The
PCE has been identified as a suitable application for the computation
of paths for P2MP TE LSPs ([RFC5671]).

The PCEP is designed as a communication protocol between PCCs and
PCEs for point-to-point (P2P) path computations and is defined in
[RFC5440]. The extensions of PCEP to request path computation for
P2MP TE LSPs are described in [I-D.ietf-pce-rfc6006bis].

Stateful PCEs are shown to be helpful in many application scenarios,
in both MPLS and GMPLS networks, as illustrated in [RFC8051]. These
scenarios apply equally to P2P and P2MP TE LSPs.
[I-D.ietf-pce-stateful-pce] provides the fundamental extensions
needed for stateful PCE to support general functionality for P2P TE

LSP. [I-D.ietf-pce-pce-initiated-lsp] provides the an extensions
needed for stateful PCE-initiated P2P TE LSP. Complementarily, this
document focuses on the extensions that are necessary in order for
the deployment of stateful PCEs to support P2MP TE LSPs. This
document describes the setup, maintenance and teardown of PCE-
initiated P2MP LSPs under the stateful PCE model.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in [RFC2119].

2. Terminology

Terminology used in this document is same as terminology used in
[I-D.ietf-pce-stateful-pce], [I-D.ietf-pce-pce-initiated-lsp], and
[I-D.ietf-pce-rfc6006bis].

3. Supporting P2MP TE LSP for Stateful PCE

3.1. Motivation

[RFC8051] presents several use cases, demonstrating scenarios that
benefit from the deployment of a stateful PCE including optimization,
recovery, etc which are equally applicable to P2MP TE LSPs.
[I-D.ietf-pce-stateful-pce] defines the extensions to PCEP for P2P TE
LSPs. Complementarily, this document focuses on the extensions that
are necessary in order for the deployment of stateful PCEs to support
P2MP TE LSPs.

In addition to that, the stateful nature of a PCE simplifies the
information conveyed in PCEP messages since it is possible to refer
to the LSPs via PLSP-ID ([I-D.ietf-pce-stateful-pce]). For P2MP this
is an added advantage, where the size of message is much larger.
Incase of stateless PCE, a modification of P2MP tree requires
encoding of all leaves along with the paths in PCReq message, but
using a stateful PCE with P2MP capability, the PCEP message can be
used to convey only the modifications (the other information can be
retrieved from the P2MP LSP identifier in the LSP database (LSPDB)).

In environments where the P2MP TE LSP placement needs to change in
response to application demands, it is useful to support dynamic
creation and tear down of P2MP TE LSPs. The ability for a PCE to
trigger the creation of P2MP TE LSPs on demand can be seamlessly
integrated into a controller-based network architecture, where
intelligence in the controller can determine when and where to set up
paths. Section 3 of [I-D.ietf-pce-pce-initiated-lsp] further

describes the motivation behind the PCE-Initiation capability, which
are equally applicable for P2MP TE LSPs.

3.2. Objectives

The objectives for the protocol extensions to support P2MP TE LSP for
stateful PCE are same as the objectives described in section 3.2 of
[I-D.ietf-pce-stateful-pce].

4. Functions to Support P2MP TE LSPs for Stateful PCEs

[I-D.ietf-pce-stateful-pce] specifies new functions to support a
stateful PCE. It also specifies that a function can be initiated
either from a PCC towards a PCE (C-E) or from a PCE towards a PCC
(E-C).

This document extends these functions to support P2MP TE LSPs.

Capability Advertisement (E-C,C-E): both the PCC and the PCE must
   announce during PCEP session establishment that they support PCEP
   Stateful PCE extensions for P2MP using mechanisms defined in
   Section 5.2.

LSP State Synchronization (C-E): after the session between the PCC
   and a stateful PCE with P2MP capability is initialized, the PCE
   must learn the state of a PCC's P2MP TE LSPs before it can perform
   path computations or update LSP attributes in a PCC.

LSP Update Request (E-C): a stateful PCE with P2MP capability
   requests modification of attributes on a PCC's P2MP TE LSP.

LSP State Report (C-E): a PCC sends an LSP state report to a PCE
   whenever the state of a P2MP TE LSP changes.

LSP Control Delegation (C-E,E-C): a PCC grants to a PCE the right to
   update LSP attributes on one or more P2MP TE LSPs; the PCE becomes
   the authoritative source of the LSP's attributes as long as the
   delegation is in effect (See Section 5.7 of
   [I-D.ietf-pce-stateful-pce]); the PCC may withdraw the delegation
   or the PCE may give up the delegation at any time.

PCE-initiated LSP instantiation (E-C): a PCE sends an LSP Initiate
   Message to a PCC to instantiate or delete a P2MP TE LSP.

5. Architectural Overview of Protocol Extensions

5.1. Extension of PCEP Messages

   New PCEP messages are defined in [I-D.ietf-pce-stateful-pce] to
   support stateful PCE for P2P TE LSPs. In this document these
   messages are extended to support P2MP TE LSPs.

   Path Computation State Report (PCRpt): Each P2MP TE LSP State Report
      in a PCRpt message can contain actual P2MP TE LSP path attributes,
      LSP status, etc. An LSP State Report carried on a PCRpt message
      is also used in delegation or revocation of control of a P2MP TE
      LSP to/from a PCE. The extension of PCRpt message is described in
      Section 6.1.

   Path Computation Update Request (PCUpd): Each P2MP TE LSP Update
      Request in a PCUpd message MUST contain all LSP parameters that a
      PCE wishes to set for a given P2MP TE LSP. An LSP Update Request
      carried on a PCUpd message is also used to return LSP delegations
      if at any point PCE no longer desires control of a P2MP TE LSP.
      The PCUpd message is described in Section 6.2.

   A new PCEP message is defined in [I-D.ietf-pce-pce-initiated-lsp] to
   support stateful PCE instantiation of P2P TE LSPs. In this document
   this message is extended to support P2MP TE LSPs.

   Path Computation LSP Initiate Message (PCInitiate): is a PCEP
      message sent by a PCE to a PCC to trigger P2MP TE LSP
      instantiation or deletion. The PCInitiate message is described in
      Section 6.5.

   The path computation request (PCReq) and path computation reply
   (PCRep) messages are also extended to support stateful PCE for P2P TE
   LSP in [I-D.ietf-pce-stateful-pce]. In this document these messages
   are extended to support P2MP TE LSPs as well.

5.2. Capability Advertisement

   During PCEP Initialization Phase, as per Section 7.1.1 of
   [I-D.ietf-pce-stateful-pce], PCEP speakers advertises Stateful
   capability via Stateful PCE Capability TLV in open message. Two new
   flags are defined for the STATEFUL-PCE-CAPABILITY TLV defined in
   [I-D.ietf-pce-stateful-pce] and updated in
   [I-D.ietf-pce-pce-initiated-lsp] and
   [I-D.ietf-pce-stateful-sync-optimizations].

   Three new bits N (P2MP-CAPABILITY), M (P2MP-LSP-UPDATE-CAPABILITY),
   and P (P2MP-LSP-INSTANTIATION-CAPABILITY) are added in this document:

N (P2MP-CAPABILITY bit - TBD4): if set to 1 by a PCC, the N Flag
   indicates that the PCC is willing to send P2MP LSP State Reports
   whenever P2MP LSP parameters or operational status changes.; if
   set to 1 by a PCE, the N Flag indicates that the PCE is interested
   in receiving LSP State Reports whenever LSP parameters or
   operational status changes. The P2MP-CAPABILITY Flag must be
   advertised by both a PCC and a PCE for PCRpt messages P2MP
   extension to be allowed on a PCEP session.

M (P2MP-LSP-UPDATE-CAPABILITY bit - TBD5): if set to 1 by a PCC, the
   M Flag indicates that the PCC allows modification of P2MP LSP
   parameters; if set to 1 by a PCE, the M Flag indicates that the
   PCE is capable of updating P2MP LSP parameters. The P2MP-LSP-
   UPDATE-CAPABILITY Flag must be advertised by both a PCC and a PCE
   for PCUpd messages P2MP extension to be allowed on a PCEP session.

P (P2MP-LSP-INSTANTIATION-CAPABILITY bit - TBD6): If set to 1 by a
   PCC, the P Flag indicates that the PCC allows instantiation of an
   P2MP LSP by a PCE. If set to 1 by a PCE, the P flag indicates
   that the PCE supports P2MP LSP instantiation. The P2MP-LSP-
   INSTANTIATION-CAPABILITY flag must be set by both PCC and PCE in
   order to support PCE-initiated P2MP LSP instantiation.

A PCEP speaker should continue to advertise the basic P2MP capability
via mechanisms as described in [I-D.ietf-pce-rfc6006bis].

5.3. IGP Extensions for Stateful PCE P2MP Capabilities Advertisement

When PCCs are LSRs participating in the IGP (OSPF or IS-IS), and PCEs
are either LSRs or servers also participating in the IGP, an
effective mechanism for PCE discovery within an IGP routing domain
consists of utilizing IGP advertisements. Extensions for the
advertisement of PCE Discovery Information are defined for OSPF and
for IS-IS in [RFC5088] and [RFC5089] respectively.

The PCE-CAP-FLAGS sub-TLV, defined in [RFC5089], is an optional sub-
TLV used to advertise PCE capabilities. It MAY be present within the
PCED sub-TLV carried by OSPF or IS-IS. [RFC5088] and [RFC5089]
provide the description and processing rules for this sub-TLV when
carried within OSPF and IS-IS, respectively.

The format of the PCE-CAP-FLAGS sub-TLV is included below for easy
reference:

Type: 5

Length: Multiple of 4.

Value: This contains an array of units of 32 bit flags with the most
significant bit as 0. Each bit represents one PCE capability.

PCE capability bits are defined in [RFC5088]. This document defines
new capability bits for the stateful PCE with P2MP as follows:

        Bit   Capability
        TBD1   Active Stateful PCE with P2MP
        TBD2   Passive Stateful PCE with P2MP
        TBD3   PCE-Initiation with P2MP

Note that while active, passive or initiation stateful PCE with P2MP
capabilities may be advertised during discovery, PCEP Speakers that
wish to use stateful PCEP MUST advertise stateful PCEP capabilities
during PCEP session setup, as specified in the current document. A
PCC MAY initiate stateful PCEP P2MP capability advertisement at PCEP
session setup even if it did not receive any IGP PCE capability
advertisements.

5.4. State Synchronization

State Synchronization operations described in Section 5.6 of
[I-D.ietf-pce-stateful-pce] are applicable for P2MP TE LSPs as well.
The optimizations described in
[I-D.ietf-pce-stateful-sync-optimizations] can also be applied for
P2MP.

5.5. LSP Delegation

LSP delegation operations described in Section 5.7 of
[I-D.ietf-pce-stateful-pce] are applicable for P2MP TE LSPs as well.

5.6. LSP Operations

5.6.1. Passive Stateful PCE

LSP operations for passive stateful PCE described in Section 5.8.1 of
[I-D.ietf-pce-stateful-pce] are applicable for P2MP TE LSPs as well.

The Path Computation Request and Response message format for P2MP TE
LSPs is described in Section 3.4 and Section 3.5 of
[I-D.ietf-pce-rfc6006bis] respectively.

The Request and Response message for P2MP TE LSPs are extended to
support encoding of LSP object, so that it is possible to refer to a
LSP with a unique identifier and simplify the PCEP message exchange.
For example, incase of modification of one leaf in a P2MP tree, there
should be no need to carry the full P2MP tree in PCReq message.

The extension for the Request and Response message for passive
stateful operations on P2MP TE LSPs are described in Section 6.3 and
Section 6.4. The extension for the Path Computation LSP State Report
(PCRpt) message is described in Section 6.1.

5.6.2. Active Stateful PCE

LSP operations for active stateful PCE described in Section 5.8.2 of
[I-D.ietf-pce-stateful-pce] are applicable for P2MP TE LSPs as well.

The extension for the Path Computation LSP Update (PCUpd) message for
active stateful operations on P2MP TE LSPs are described in
Section 6.2.

5.6.3. PCE-Initiated LSP

As per section 5.1 of [I-D.ietf-pce-pce-initiated-lsp], the PCE sends
a Path Computation LSP Initiate Request (PCInitiate) message to the
PCC to suggest instantiation or deletion of a P2P TE LSP. This
document extends the PCInitiate message to support P2MP TE LSP (see
details in Section 6.5).

P2MP TE LSP suggested instantiation and deletion operations are same
as P2P LSP as described in section 5.3 and 5.4 of
[I-D.ietf-pce-pce-initiated-lsp].

5.6.3.1. P2MP TE LSP Instantiation

The Instantiation operation of P2MP TE LSP is same as defined in
section 5.3 of [I-D.ietf-pce-pce-initiated-lsp] including handling of
PLSP-ID, SYMBOLIC-PATH-NAME TLV etc. Rules of processing and error
codes remains unchanged. The N bit MUST be set in LSP object in
PCInitiate message by PCE to specify the instantiation is for P2MP TE
LSP.

Though N bit is set in the LSP object, P2MP-LSP-IDENTIFIER TLV MUST
NOT be included in the LSP object in PCIntiitate message as it SHOULD
be generated by PCC and carried in PCRpt message.

5.6.3.2. P2MP TE LSP Deletion

The deletion operation of P2MP TE LSP is same as defined in section
5.4 of [I-D.ietf-pce-pce-initiated-lsp] by sending an LSP Initiate
Message with an LSP object carrying the PLSP-ID of the LSP to be
removed and an SRP object with the R flag set (LSP-REMOVE as per
section 5.2 of [I-D.ietf-pce-pce-initiated-lsp]). Rules of
processing and error codes remains unchanged.

5.6.3.3. Adding and Pruning Leaves for the P2MP TE LSP

Adding of new leaves and Pruning of old Leaves for the PCE initiated
P2MP TE LSP MUST be carried in PCUpd message and SHOULD refer
Section 6.2 for P2MP TE LSP extensions. As defined in
[I-D.ietf-pce-rfc6006bis], leaf type = 1 for adding of new leaves,
leaf type = 2 for pruning of old leaves of P2MP END-POINTS Object are
used in PCUpd message.

PCC MAY use the Incremental State Update mechanims as described in
[RFC4875] to signal adding and pruning of leaves.

5.6.3.4. P2MP TE LSP Delegation and Cleanup

P2MP TE LSP delegation and cleanup operations are same as defined in
section 6 of [I-D.ietf-pce-pce-initiated-lsp]. Rules of processing
and error codes remains unchanged.

6. PCEP Message Extensions

6.1. The PCRpt Message

As per Section 6.1 of [I-D.ietf-pce-stateful-pce], PCRpt message is
used to report the current state of a P2P TE LSP. This document
extends the PCRpt message in reporting the status of P2MP TE LSP.

The format of PCRpt message is as follows:

```
<PCRpt Message> ::= <Common Header>
                      <state-report-list>
Where:

<state-report-list> ::= <state-report>
                          [<state-report-list>]

<state-report> ::= [<SRP>]
                     <LSP>
                     <end-point-intended-path-pair-list>
                     [<actual-attribute-list>
                     <end-point-actual-path-pair-list>]
                     <intended-attribute-list>

Where:

<end-point-intended-path-pair-list>::=
                     [<END-POINTS>]
                     [<S2LS>]
                     <intended-path>
                     [<end-point-intended-path-pair-list>]

<end-point-actual-path-pair-list>::=
                     [<END-POINTS>]
                     <actual-path>
                     [<end-point-actual-path-pair-list>]

<intended-path> ::= (<ERO>|<SERO>)
            [<intended-path>]

<actual-path> ::= (<RRO>|<SRRO>)
            [<actual-path>]
```

<intended-attribute-list> is defined in [RFC5440] and
extended by PCEP extensions.
<actual-attribute-list> consists of the actual computed and
signaled values of the <BANDWIDTH> and <metric-lists>
objects defined in [RFC5440].

The P2MP END-POINTS object defined in [I-D.ietf-pce-rfc6006bis] is
mandatory for specifying address of P2MP leaves grouped based on leaf
types.

o New leaves to add (leaf type = 1)

o Old leaves to remove (leaf type = 2)

   o Old leaves whose path can be modified/reoptimized (leaf type = 3)

   o Old leaves whose path must be left unchanged (leaf type = 4)

   When reporting the status of a P2MP TE LSP, the destinations are
   grouped in END-POINTS object based on the operational status (O field
   in S2LS object) and leaf type (in END-POINTS). This way the leaves
   that share the same operational status are grouped together. For
   reporting the status of delegated P2MP TE LSP, leaf-type = 3, where
   as for non-delegated P2MP TE LSP, leaf-type = 4 is used.

   For delegated P2MP TE LSP configuration changes are reported via
   PCRpt message. For example, adding of new leaves END-POINTS (leaf-
   type = 1) is used where as removing of old leaves (leaf-type = 2) is
   used.

   Note that we preserve compatibility with the
   [I-D.ietf-pce-stateful-pce] definition of <state-report>. At least
   one instance of <END-POINTS> MUST be present in this message for P2MP
   LSP.

   During state synchronization, the PCRpt message must report the
   status of the full P2MP TE LSP.

   The S2LS object MUST be carried in PCRpt message along with END-
   POINTS object when N bit is set in LSP object for P2MP TE LSP. If
   the S2LS object is missing, the receiving PCE MUST send a PCErr
   message with Error-type=6 (Mandatory Object missing) and Error-
   value=TBD11 (S2LS object missing). If the END-POINTS object is
   missing, the receiving PCE MUST send a PCErr message with Error-
   type=6 (Mandatory Object missing) and Error-value=3 (END-POINTS
   object missing) (defined in [RFC5440].

6.2. The PCUpd Message

   As per Section 6.2 of [I-D.ietf-pce-stateful-pce], PCUpd message is
   used to update P2P TE LSP attributes. This document extends the
   PCUpd message in updating the attributes of P2MP TE LSP.

   The format of a PCUpd message is as follows:

```
    <PCUpd Message> ::= <Common Header>
                        <update-request-list>


    Where:

    <update-request-list> ::= <update-request>
                              [<update-request-list>]


    <update-request> ::= <SRP>
                         <LSP>
                         <end-point-path-pair-list>
                         <attribute-list>


    Where:

    <end-point-path-pair-list>::=
                    [<END-POINTS>]
                    <intended-path>
                    [<end-point-path-pair-list>]

    <intended-path> ::= (<ERO>|<SERO>)
              [<intended-path>]


    <attribute-list> is defined in [RFC5440] and
    extended by PCEP extensions.
```

Note that we preserve compatibility with the
[I-D.ietf-pce-stateful-pce] definition of <update-request>.

The PCC MAY use the make-before-break or sub-group-based procedures
described in [RFC4875] based on a local policy decision.

The END-POINTS object MUST be carried in PCUpd message when N bit is
set in LSP object for P2MP TE LSP. If the END-POINTS object is
missing, the receiving PCC MUST send a PCErr message with Error-
type=6 (Mandatory Object missing) and Error-value=3 (END-POINTS
object missing) (defined in [RFC5440].

6.3. The PCReq Message

As per Section 3.4 of [I-D.ietf-pce-rfc6006bis], PCReq message is
used for a P2MP path computation request. This document extends the
PCReq message such that a PCC MAY include the LSP object in the PCReq
message if the stateful PCE P2MP capability has been negotiated on a
PCEP session between the PCC and a PCE.

The format of PCReq message is as follows:

```
 <PCReq Message>::= <Common Header>
                      [<svec-list>]
                      <request-list>
```

where:

```
<svec-list>::= <SVEC>
               [<OF>]
               [<metric-list>]
               [<svec-list>]
```

```
<request-list>::=<request>[<request-list>]
```

```
<request>::= <RP>
             <end-point-rro-pair-list>
             [<LSP>]
             [<OF>]
             [<LSPA>]
             [<BANDWIDTH>]
             [<metric-list>]
             [<IRO>|<BNC>]
             [<LOAD-BALANCING>]
```

```
<end-point-rro-pair-list>::= <END-POINTS>
                             [<RRO-List>[<BANDWIDTH>]]
                             [<end-point-rro-pair-list>]
```

```
<RRO-List>::=(<RRO>|<SRRO>)[<RRO-List>]
<metric-list>::=<METRIC>[<metric-list>]
```

6.4. The PCRep Message

As per Section 3.5 of [I-D.ietf-pce-rfc6006bis], PCRep message is
used for a P2MP path computation reply. This document extends the
PCRep message such that a PCE MAY include the LSP object in the PCRep
message if the stateful PCE P2MP capability has been negotiated on a
PCEP session between the PCC and a PCE.

The format of PCRep message is as follows:

```
<PCRep Message>::= <Common Header>
                   <response-list>
```

where:

```
<response-list>::=<response>[<response-list>]
```

```
<response>::=<RP>
             [<end-point-path-pair-list>]
             [<LSP>]
             [<NO-PATH>]
             [<UNREACH-DESTINATION>]
             [<attribute-list>]
```

```
<end-point-path-pair-list>::= [<END-POINTS>]
                              <path>
                              [<end-point-path-pair-list>]
```

```
<path> ::= (<ERO>|<SERO>) [<path>]
```

```
<attribute-list>::=[<OF>]
                   [<LSPA>]
                   [<BANDWIDTH>]
                   [<metric-list>]
                   [<IRO>]
```

6.5. The PCInitiate message

As defined in section 5.1 of [I-D.ietf-pce-pce-initiated-lsp], PCE
sends a PCInitiate message to a PCC to recommend instantiation of a
P2P TE LSP, this document extends the format of PCInitiate message
for the creation of P2MP TE LSPs but the creation and deletion
operations of P2MP TE LSP are same to the P2P TE LSP.

The format of PCInitiate message is as follows:

```
<PCInitiate Message> ::= <Common Header>
                         <PCE-initiated-lsp-list>
Where:

<PCE-initiated-lsp-list> ::= <PCE-initiated-lsp-request>
                             [<PCE-initiated-lsp-list>]

<PCE-initiated-lsp-request> ::=
(<PCE-initiated-lsp-instantiation>|<PCE-initiated-lsp-deletion>)

<PCE-initiated-lsp-instantiation> ::= <SRP>
                                      <LSP>
                                      <end-point-path-pair-list>
                                      [<attribute-list>]

<PCE-initiated-lsp-deletion> ::= <SRP>
                                 <LSP>


Where:

<end-point-path-pair-list>::=
                  [<END-POINTS>]
                  <intended-path>
                  [<end-point-path-pair-list>]

<intended-path> ::= (<ERO>|<SERO>)
         [<intended-path>]

<attribute-list> is defined in [RFC5440] and extended
by PCEP extensions.
```

The PCInitiate message with an LSP object with N bit (P2MP) set is
used to convey operation on a P2MP TE LSP. The SRP object is used to
correlate between initiation requests sent by the PCE and the error
reports and state reports sent by the PCC as described in
[I-D.ietf-pce-stateful-pce].

The END-POINTS object MUST be carried in PCInitiate message when N
bit is set in LSP object for P2MP TE LSP. If the END-POINTS object
is missing, the receiving PCC MUST send a PCErr message with Error-
type=6 (Mandatory Object missing) and Error-value=3 (END-POINTS
object missing) (defined in [RFC5440].

6.6. Example

6.6.1. P2MP TE LSP Update Request

LSP Update Request message is sent by an active stateful PCE to
update the P2MP TE LSP parameters or attributes. An example of a
PCUpd message for P2MP TE LSP is described below:

             Common Header
             SRP
             LSP with P2MP flag set
             END-POINTS for leaf type 3
               ERO list

In this example, a stateful PCE request updation of path taken by
some of the leaves in a P2MP tree. The update request uses the END-
POINT type 3 (modified/reoptimized). The ERO list represents the
S2LS path after modification. The update message does not need to
encode the full P2MP tree in this case.

6.6.2. P2MP TE LSP Report

LSP State Report message is sent by a PCC to report or delegate the
P2MP TE LSP. An example of a PCRpt message for a delegated P2MP TE
LSP is described below to add new leaves to an existing P2MP TE LSP:

             Common Header
             LSP with P2MP flag set
             END-POINTS for leaf type 1
               S2LS (O=DOWN)
               ERO list (empty)

An example of a PCRpt message for P2MP TE LSP is described below to
prune leaves from an existing P2MP TE LSP:

             Common Header
             LSP with P2MP flag set
             END-POINTS for leaf type 2
               S2LS (O=UP)
               ERO list

An example of a PCRpt message for a delegated P2MP TE LSP is
described below to report status of leaves in an existing P2MP TE
LSP:

```
              Common Header
              LSP with P2MP flag set
              END-POINTS for leaf type 3
                S2LS (O=UP)
                ERO list
              END-POINTS for leaf type 3
                S2LS (O=DOWN)
                ERO list
```

An example of a PCRpt message for a non-delegated P2MP TE LSP is
described below to report status of leaves:


```
              Common Header
              LSP with P2MP flag set
              END-POINTS for leaf type 4
                S2LS (O=ACTIVE)
                ERO list
              END-POINTS for leaf type 4
                S2LS (O=DOWN)
                ERO list
```

7. PCEP Object Extensions

The PCEP TLV defined in this document is compliant with the PCEP TLV
format defined in [RFC5440].

7.1. Extension of LSP Object

LSP Object is defined in Section 7.3 of [I-D.ietf-pce-stateful-pce].
It specifies PLSP-ID to uniquely identify an LSP that is constant for
the life time of a PCEP session. Similarly for P2MP tunnel, PLSP-ID
identify a P2MP TE LSP uniquely. This document adds the following
flags to the LSP Object:

N (P2MP bit - TBD7): If the bit is set to 1, it specifies the
   message is for P2MP TE LSP which MUST be set in PCRpt or PCUpd
   message for a P2MP TE LSP.

F (Fragmentation bit - TBD8): If the bit is set to 1, it specifies
   the message is fragmented.

If P2MP bit is set, the following P2MP-LSP-IDENTIFIER TLV MUST be
present in LSP object.

7.2. P2MP-LSP-IDENTIFIER TLV

The P2MP LSP Identifier TLV MUST be included in the LSP object in
PCRpt message for RSVP-TE signaled P2MP TE LSPs. If the TLV is
missing, the PCE will generate an error with error-type 6 (mandatory
object missing) and error-value TBD12 (P2MP-LSP-IDENTIFIER TLV
missing) and close the PCEP session.

The P2MP LSP Identifier TLV MAY be included in the LSP object in
PCUpd message for RSVP-TE signaled P2MP TE LSPs. The special value
of all zeros for this TLV is used to refer to all paths pertaining to
a particular PLSP-ID.

There are two P2MP LSP Identifier TLVs, one for IPv4 and one for
IPv6.

The format of the IPV4-P2MP-LSP-IDENTIFIER TLV is shown in the
following figure:

```
 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Type=TBD9           |           Length=16           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                   IPv4 Tunnel Sender Address                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           LSP ID              |           Tunnel ID           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Extended Tunnel ID                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           P2MP ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

             Figure 6: IPV4-P2MP-LSP-IDENTIFIER TLV format

The type (16-bit) of the TLV is TBD9 to be assigned by IANA. The
length (16-bit) has a fixed value of 16 octets. The value contains
the following fields:

IPv4 Tunnel Sender Address: contains the sender node's IPv4 address,
   as defined in [RFC3209], Section 4.6.2.1 for the LSP_TUNNEL_IPv4
   Sender Template Object.

LSP ID: contains the 16-bit 'LSP ID' identifier defined in
   [RFC3209], Section 4.6.2.1 for the LSP_TUNNEL_IPv4 Sender Template
   Object.

Tunnel ID: contains the 16-bit 'Tunnel ID' identifier defined in
    [RFC3209], Section 4.6.1.1 for the LSP_TUNNEL_IPv4 Session Object.

Extended Tunnel ID: contains the 32-bit 'Extended Tunnel ID'
    identifier defined in [RFC3209], Section 4.6.1.1 for the
    LSP_TUNNEL_IPv4 Session Object.

P2MP ID: contains the 32-bit 'P2MP ID' identifier defined in
    Section 19.1.1 of [RFC4875] for the P2MP LSP Tunnel IPv4 SESSION
    Object.

The format of the IPV6-P2MP-LSP-IDENTIFIER TLV is shown in the
following figure:

```
 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Type=TBD10           |           Length=40           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                  IPv6 tunnel sender address                   |
+                        (16 octets)                            +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            LSP ID             |           Tunnel ID           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                      Extended Tunnel ID                       |
+                        (16 octets)                            +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           P2MP ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
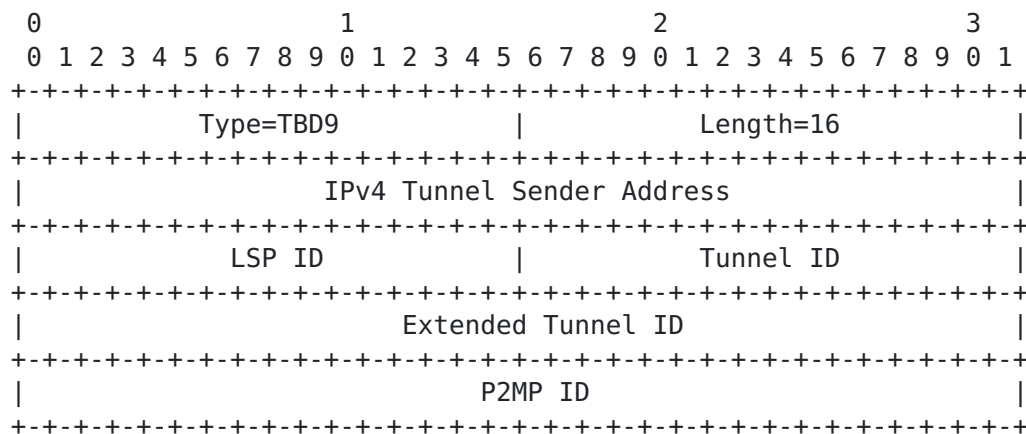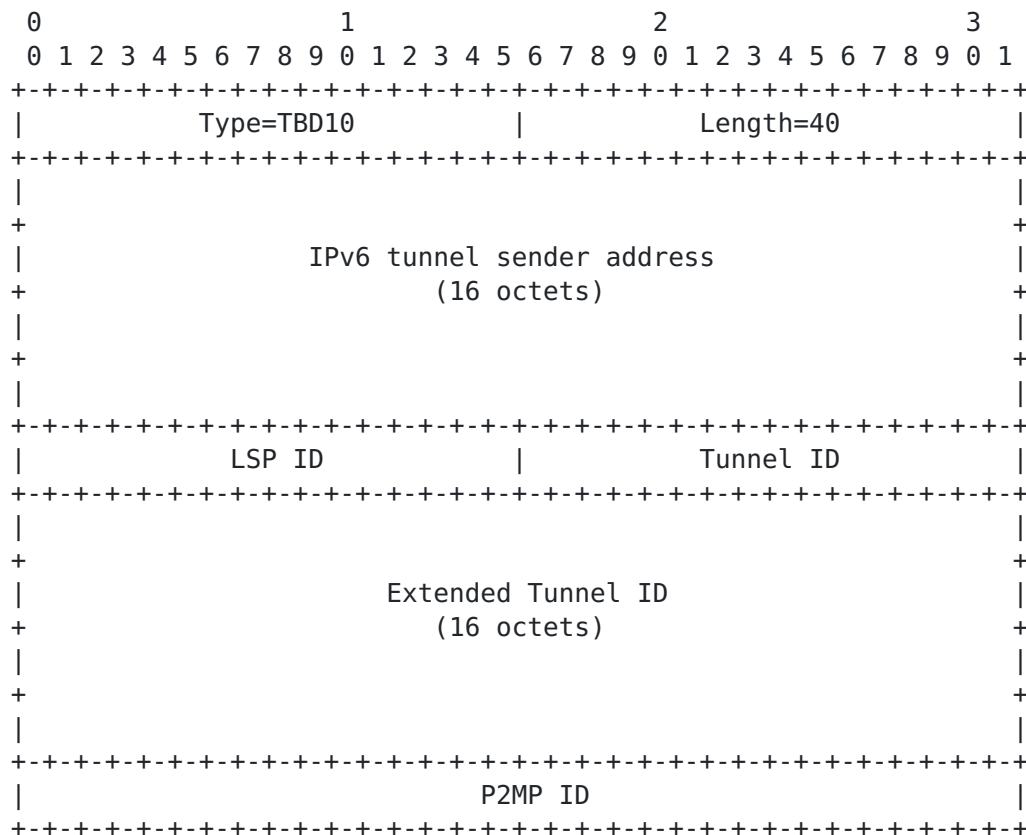
Figure 7: IPV6-P2MP-LSP-IDENTIFIER TLV format

The type of the TLV is TBD10 to be assigned by IANA. The length
(16-bit) has a fixed length of 40 octets. The value contains the
following fields:

   IPv6 Tunnel Sender Address: contains the sender node's IPv6 address,
      as defined in [RFC3209], Section 4.6.2.2 for the LSP_TUNNEL_IPv6
      Sender Template Object.

   LSP ID: contains the 16-bit 'LSP ID' identifier defined in
      [RFC3209], Section 4.6.2.2 for the LSP_TUNNEL_IPv6 Sender Template
      Object.

   Tunnel ID: contains the 16-bit 'Tunnel ID' identifier defined in
      [RFC3209], Section 4.6.1.2 for the LSP_TUNNEL_IPv6 Session Object.

   Extended Tunnel ID: contains the 128-bit 'Extended Tunnel ID'
      identifier defined in [RFC3209], Section 4.6.1.2 for the
      LSP_TUNNEL_IPv6 Session Object.

   P2MP ID: As defined above in IPV4-P2MP-LSP-IDENTIFIERS TLV.

   Tunnel ID remains constant over the life time of a tunnel.

7.3. S2LS Object

   The S2LS (Source-to-Leaves) Object is used to report RSVP-TE state of
   one or more destinations (leaves) encoded within the END-POINTS
   object for a P2MP TE LSP. It MUST be carried in PCRpt message along
   with END-POINTS object when N bit is set in LSP object.

   S2LS Object-Class is TBD19.

   S2LS Object-Types is 1.

   The format of the S2LS object is shown in the following figure:


```
 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 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Flags                           |  O|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
//                     Optional TLVs                          //
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
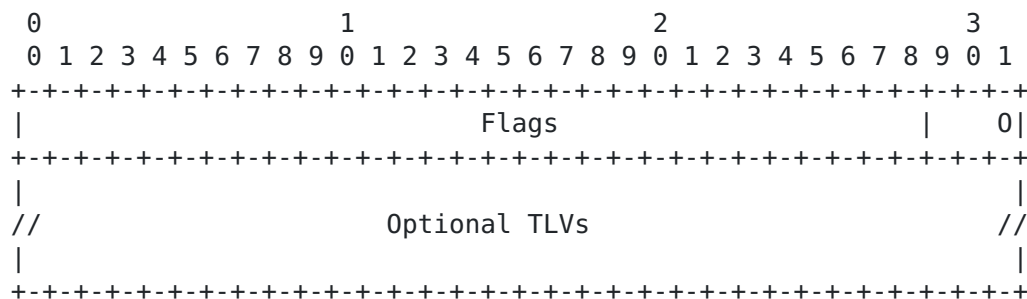

                     Figure 8: S2LS object format

   Flags(32 bits):

O(Operational - 3 bits) the O Field represents the operational
   status of the group of destinations. The values are as per
   Operational field in LSP object defined in Section 7.3 of
   [I-D.ietf-pce-stateful-pce].

When N bit is set in LSP object then the O field in LSP object
represents the operational status of the full P2MP TE LSP and the O
field in S2LS object represents the operational status of a group of
destinations encoded within the END-POINTS object.

Future documents MAY define optional TLVs that MAY be included in the
S2LS Object.

8. Message Fragmentation

The total PCEP message length, including the common header, is 16
bytes. In certain scenarios the P2MP report and update request may
not fit into a single PCEP message (e.g. initial report or update).
The F-bit is used in the LSP object to signal that the initial
report, update, or initiate message was too large to fit into a
single message and will be fragmented into multiple messages. In
order to identify the single report or update each message will use
the same PLSP-ID. In order to identify that a series of PCInitiate
messages represents a single Initiate, each message will use the same
PLSP-ID (in this case 0) and SRP-ID-number.

Fragmentation procedure described below for report or update message
is similar to [I-D.ietf-pce-rfc6006bis] which describes request and
response message fragmentation.

8.1. Report Fragmentation Procedure

If the initial report is too large to fit into a single report
message, the PCC will split the report over multiple messages. Each
message sent to the PCE, except the last one, will have the F-bit set
in the LSP object to signify that the report has been fragmented into
multiple messages. In order to identify that a series of report
messages represents a single report, each message will use the same
PLSP-ID.

To indicate P2MP message fragmentation errors associated with a P2MP
Report, a Error-Type (18) for "P2MP Fragmentation Error" and a new
error-value TBD13 is used if a PCE has not received the last piece of
the fragmented message, it should send an error message to the PCC to
signal that it has received an incomplete message (i.e., "Fragmented
Report failure").

8.2. Update Fragmentation Procedure

Once the PCE computes and updates a path for some or all leaves in a
P2MP TE LSP, an update message is sent to the PCC. If the update is
too large to fit into a single update message, the PCE will split the
update over multiple messages. Each update message sent by the PCE,
except the last one, will have the F-bit set in the LSP object to
signify that the update has been fragmented into multiple messages.
In order to identify that a series of update messages represents a
single update, each message will use the same PLSP-ID and SRP-ID-
number.

To indicate P2MP message fragmentation errors associated with a P2MP
Update request, a Error-Type (18) for "P2MP Fragmentation Error" and
a new error-value TBD14 is used if a PCC has not received the last
piece of the fragmented message, it should send an error message to
the PCE to signal that it has received an incomplete message (i.e.,
"Fragmented Update failure").

8.3. PCIntiate Fragmentation Procedure

Once the PCE initiates to set up the P2MP TE LSP, a PCInitiate
message is sent to the PCC. If the PCInitiate is too large to fit
into a single PCInitiate message, the PCE will split the PCInitiate
over multiple messages. Each PCInitiate message sent by the PCE,
except the last one, will have the F-bit set in the LSP object to
signify that the PCInitiate has been fragmented into multiple
messages. In order to identify that a series of PCInitiate messages
represents a single Initiate, each message will use the same PLSP-ID
(in this case 0) and SRP-ID-number.

To indicate P2MP message fragmentation errors associated with a P2MP
PCInitiate, a Error-Type (18) for "P2MP Fragmentation Error" and a
new error-value TBD15 is used if a PCC has not received the last
piece of the fragmented message, it should send an error message to
the PCE to signal that it has received an incomplete message (i.e.,
"Fragmented Instantiation failure").

9. Non-Support of P2MP TE LSPs for Stateful PCE

The PCEP protocol extensions described in this document for stateful
PCEs with P2MP capability MUST NOT be used if PCE has not advertised
its stateful capability with P2MP as per Section 5.2. If the PCEP
Speaker on the PCC supports the extensions of this draft (understands
the P2MP flag in the LSP object) but did not advertise this
capability, then upon receipt of PCUpd message from the PCE, it
SHOULD generate a PCErr with error-type 19 (Invalid Operation),
error-value TBD17 (Attempted LSP Update Request for P2MP if active

stateful PCE capability for P2MP was not advertised). If the PCEP
Speaker on the PCE supports the extensions of this draft (understands
the P2MP flag in the LSP object) but did not advertise this
capability, then upon receipt of a PCRpt message from the PCC, it
SHOULD generate a PCErr with error-type 19 (Invalid Operation),
error-value TBD16 (Attempted LSP State Report for P2MP if stateful
PCE capability for P2MP was not advertised) and it will terminate the
PCEP session.

If a Stateful PCE receives a P2MP TE LSP report message and the PCE
does not understand the P2MP flag in the LSP object, and therefore
the PCEP extensions described in this document, then the Stateful PCE
would act as per [I-D.ietf-pce-stateful-pce].

The PCEP protocol extensions described in this document for PCC or
PCE with instantiation capability for P2MP TE LSPs MUST NOT be used
if PCC or PCE has not advertised its stateful capability with
Instantiation and P2MP capability as per Section 5.2. If the PCEP
Speaker on the PCC supports the extensions of this draft (understands
the P (P2MP-LSP-INSTANTIATION-CAPABILITY) flag in the LSP object) but
did not advertise this capability, then upon receipt of PCInitiate
message from the PCE, it SHOULD generate a PCErr with error-type 19
(Invalid Operation), error-value TBD18 (Attempted LSP Instantiation
Request for P2MP if stateful PCE instantiation capability for P2MP
was not advertised).

10. Manageability Considerations

All manageability requirements and considerations listed in
[RFC5440], [I-D.ietf-pce-rfc6006bis], [I-D.ietf-pce-stateful-pce],
and [I-D.ietf-pce-pce-initiated-lsp] apply to PCEP protocol
extensions defined in this document. In addition, requirements and
considerations listed in this section apply.

10.1. Control of Function and Policy

A PCE or PCC implementation MUST allow configuring the stateful PCEP
capability, the LSP Update capability, and the LSP Initiation
capability for P2MP LSPs.

10.2. Information and Data Models

The PCEP YANG module [I-D.ietf-pce-pcep-yang] SHOULD be extended to
include advertised P2MP stateful capabilities, P2MP synchronization
status, and delegation status of P2MP LSP etc. The statistics module
should also count P2MP LSP related data.

10.3. Liveness Detection and Monitoring

Mechanisms defined in this document do not imply any new liveness
detection and monitoring requirements in addition to those already
listed in [RFC5440].

10.4. Verify Correct Operations

Mechanisms defined in this document do not imply any new operation
verification requirements in addition to those already listed in
[RFC5440], [I-D.ietf-pce-rfc6006bis], [I-D.ietf-pce-stateful-pce],
and [I-D.ietf-pce-pce-initiated-lsp].

10.5. Requirements On Other Protocols

Mechanisms defined in this document do not imply any new requirements
on other protocols.

10.6. Impact On Network Operations

Mechanisms defined in this document do not have any impact on network
operations in addition to those already listed in [RFC5440],
[I-D.ietf-pce-rfc6006bis], [I-D.ietf-pce-stateful-pce], and
[I-D.ietf-pce-pce-initiated-lsp].

Stateful PCE feature for P2MP LSP would help with network operations.

11. IANA Considerations

This document requests IANA actions to allocate code points for the
protocol elements defined in this document.

11.1. PCE Capabilities in IGP Advertisements

IANA is requested to allocate new bits in the OSPF Parameters "PCE
Capability Flags" registry, as follows:

```
              Bit       Meaning              Reference
              TBD1      Active Stateful      [This I-D]
                        PCE with P2MP
              TBD2      Passive Stateful     [This I-D]
                        PCE with P2MP
              TBD3      Stateful PCE         [This I-D]
                        Initiation with P2MP
```

11.2. STATEFUL-PCE-CAPABILITY TLV

   The STATEFUL-PCE-CAPABILITY TLV is defined in
   [I-D.ietf-pce-stateful-pce] and a registry is requested to be
   created to manage the flags in the TLV. IANA is requested to make
   the following allocations in the aforementioned registry.

       Bit   Description   Reference

       TBD4   P2MP-CAPABILITY   [This I-D]
       TBD5   P2MP-LSP-UPDATE-   [This I-D]
               CAPABILITY
       TBD6   P2MP-LSP-   [This I-D]
               INSTANTIATION-
               CAPABILITY

11.3. LSP Object

   The LSP object is defined in [I-D.ietf-pce-stateful-pce] and a
   registry is created to manage the Flags field of the LSP object.

   IANA is requested to make the following allocations in the
   aforementioned registry.

       Bit   Description   Reference

       TBD7   P2MP   [This I-D]
       TBD8   Fragmentation   [This I-D]

11.4. PCEP-Error Object

   IANA is requested to allocate new error values within the "PCEP-ERROR
   Object Error Types and Values" sub-registry of the PCEP Numbers
   registry, as follows:

```
        Error-Type  Meaning
           6        Mandatory Object missing [RFC5440]
                       Error-value=TBD11: S2LS object missing
                       Error-value=TBD12: P2MP-LSP-IDENTIFIER TLV missing
          18        P2MP Fragmentation Error [I-D.ietf-pce-rfc6006bis]
                       Error-value= TBD13. Fragmented Report
                            failure
                       Error-value= TBD14. Fragmented Update
                            failure
                       Error-value= TBD15. Fragmented Instantiation
                            failure
          19        Invalid Operation [I-D.ietf-pce-stateful-pce]
                       Error-value= TBD16. Attempted LSP State Report
                            for P2MP if stateful PCE capability
                            for P2MP was not advertised
                       Error-value= TBD17. Attempted LSP Update Request
                            for P2MP if active stateful PCE capability
                            for P2MP was not advertised
                       Error-value= TBD18. Attempted LSP Instantiation
                            Request for P2MP if stateful PCE
                            instantiation capability for P2MP was not
                            advertised
```

   Referece for all new Error-Value above is [This I-D].

11.5. PCEP TLV Type Indicators

   IANA is requested to make the assignment of a new value for the
   existing "PCEP TLV Type Indicators" registry as follows:

```
        Value     Meaning                          Reference
          TBD9    P2MP-IPV4-LSP-IDENTIFIERS        [This I-D]
          TBD10   P2MP-IPV6-LSP-IDENTIFIERS        [This I-D]
```

11.6. PCEP object

   IANA is requested to allocate new object-class values and object
   types within the "PCEP Objects" sub-registry of the PCEP Numbers
   registry, as follows.

```
   Object-Class Value  Name                                Reference

          TBD19        S2LS                               [This.I-D]
                       Object-Type
                       1
```

11.7. S2LS object

   This document requests that a new sub-registry, named "S2LS Object
   Flag Field", is created within the "Path Computation Element Protocol
   (PCEP) Numbers" registry to manage the Flag field of the S2LS
   object.New values are to be assigned by Standards Action [RFC5226].
   Each bit should be tracked with the following qualities:

   o Bit number (counting from bit 0 as the most significant bit)

   o Capability description

   o Defining RFC

   The following values are defined in this document:

```
                  Bit     Description          Reference

                  29-31   Operational (3-bit)  [This.I-D]
```

12. Security Considerations

   The stateful operations on P2MP TE LSP are more CPU-intensive and
   also utilize more bandwidth on wire. In the event of an unauthorized
   stateful P2MP operations, or a denial of service attack, the
   subsequent PCEP operations may be disruptive to the network.
   Consequently, it is important that implementations conform to the
   relevant security requirements of [RFC5440],
   [I-D.ietf-pce-rfc6006bis] and [I-D.ietf-pce-stateful-pce], and
   [I-D.ietf-pce-pce-initiated-lsp]. Further [I-D.ietf-pce-pceps]
   discusses an enhanced approach to provide secure transport for PCEP
   via Transport Layer Security (TLS).

13. Acknowledgments

Thanks to Quintin Zhao, Avantika and Venugopal Reddy for his comments.

14. References

14.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119,
           DOI 10.17487/RFC2119, March 1997,
           <http://www.rfc-editor.org/info/rfc2119>.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V.,
           and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP
           Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001,
           <http://www.rfc-editor.org/info/rfc3209>.

[RFC5088] Le Roux, JL., Ed., Vasseur, JP., Ed., Ikejiri, Y., and R.
           Zhang, "OSPF Protocol Extensions for Path Computation
           Element (PCE) Discovery", RFC 5088, DOI 10.17487/RFC5088,
           January 2008, <http://www.rfc-editor.org/info/rfc5088>.

[RFC5089] Le Roux, JL., Ed., Vasseur, JP., Ed., Ikejiri, Y., and R.
           Zhang, "IS-IS Protocol Extensions for Path Computation
           Element (PCE) Discovery", RFC 5089, DOI 10.17487/RFC5089,
           January 2008, <http://www.rfc-editor.org/info/rfc5089>.

[RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation
           Element (PCE) Communication Protocol (PCEP)", RFC 5440,
           DOI 10.17487/RFC5440, March 2009,
           <http://www.rfc-editor.org/info/rfc5440>.

[I-D.ietf-pce-stateful-pce]
           Crabbe, E., Minei, I., Medved, J., and R. Varga, "PCEP
           Extensions for Stateful PCE", draft-ietf-pce-stateful-
           pce-18 (work in progress), December 2016.

[I-D.ietf-pce-stateful-sync-optimizations]
           Crabbe, E., Minei, I., Medved, J., Varga, R., Zhang, X.,
           and D. Dhody, "Optimizations of Label Switched Path State
           Synchronization Procedures for a Stateful PCE", draft-
           ietf-pce-stateful-sync-optimizations-10 (work in
           progress), March 2017.

[I-D.ietf-pce-pce-initiated-lsp]
          Crabbe, E., Minei, I., Sivabalan, S., and R. Varga, "PCEP
          Extensions for PCE-initiated LSP Setup in a Stateful PCE
          Model", draft-ietf-pce-pce-initiated-lsp-09 (work in
          progress), March 2017.

[I-D.ietf-pce-rfc6006bis]
          Zhao, Q., Dhody, D., Palleti, R., and D. King, "Extensions
          to the Path Computation Element Communication Protocol
          (PCEP) for Point-to-Multipoint Traffic Engineering Label
          Switched Paths", draft-ietf-pce-rfc6006bis-02 (work in
          progress), April 2017.

14.2. Informative References

[RFC4655] Farrel, A., Vasseur, J., and J. Ash, "A Path Computation
          Element (PCE)-Based Architecture", RFC 4655,
          DOI 10.17487/RFC4655, August 2006,
          <http://www.rfc-editor.org/info/rfc4655>.

[RFC4857] Fogelstroem, E., Jonsson, A., and C. Perkins, "Mobile IPv4
          Regional Registration", RFC 4857, DOI 10.17487/RFC4857,
          June 2007, <http://www.rfc-editor.org/info/rfc4857>.

[RFC4875] Aggarwal, R., Ed., Papadimitriou, D., Ed., and S.
          Yasukawa, Ed., "Extensions to Resource Reservation
          Protocol - Traffic Engineering (RSVP-TE) for Point-to-
          Multipoint TE Label Switched Paths (LSPs)", RFC 4875,
          DOI 10.17487/RFC4875, May 2007,
          <http://www.rfc-editor.org/info/rfc4875>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an
          IANA Considerations Section in RFCs", BCP 26, RFC 5226,
          DOI 10.17487/RFC5226, May 2008,
          <http://www.rfc-editor.org/info/rfc5226>.

[RFC5671] Yasukawa, S. and A. Farrel, Ed., "Applicability of the
          Path Computation Element (PCE) to Point-to-Multipoint
          (P2MP) MPLS and GMPLS Traffic Engineering (TE)", RFC 5671,
          DOI 10.17487/RFC5671, October 2009,
          <http://www.rfc-editor.org/info/rfc5671>.

[RFC8051] Zhang, X., Ed. and I. Minei, Ed., "Applicability of a
          Stateful Path Computation Element (PCE)", RFC 8051,
          DOI 10.17487/RFC8051, January 2017,
          <http://www.rfc-editor.org/info/rfc8051>.

   [I-D.ietf-pce-pceps]
              Lopez, D., Dios, O., Wu, Q., and D. Dhody, "Secure
              Transport for PCEP", draft-ietf-pce-pceps-12 (work in
              progress), April 2017.

   [I-D.ietf-pce-pcep-yang]
              Dhody, D., Hardwick, J., Beeram, V., and j.
              jefftant@gmail.com, "A YANG Data Model for Path
              Computation Element Communications Protocol (PCEP)",
              draft-ietf-pce-pcep-yang-02 (work in progress), March
              2017.

Appendix A. Contributor Addresses

    Yuji Kamite
    NTT Communications Corporation
    Granpark Tower
    3-4-1 Shibaura, Minato-ku
    Tokyo 108-8118
    Japan

    EMail: y.kamite@ntt.com

Authors' Addresses

    Udayasree Palle
    Huawei Technologies
    Divyashree Techno Park, Whitefield
    Bangalore, Karnataka 560066
    India

    EMail: udayasreereddy@gmail.com

    Dhruv Dhody
    Huawei Technologies
    Divyashree Techno Park, Whitefield
    Bangalore, Karnataka 560066
    India

    EMail: dhruv.ietf@gmail.com

    Yosuke Tanaka
    NTT Communications Corporation
    Granpark Tower
    3-4-1 Shibaura, Minato-ku
    Tokyo 108-8118
    Japan

    EMail: yosuke.tanaka@ntt.com

    Vishnu Pavan Beeram
    Juniper Networks

    EMail: vbeeram@juniper.net