        Stateful Path Computation Element (PCE) Protocol Extensions
     for Usage with Point-to-Multipoint TE Label Switched Paths (LSPs)

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 Label Switched Paths (LSPs). This document
   provides extensions required for the 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

   This is an Internet Standards Track document.

   This document is a product of the Internet Engineering Task Force
   (IETF). It represents the consensus of the IETF community. It has
   received public review and has been approved for publication by the
   Internet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in Section 2 of RFC 7841.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   https://www.rfc-editor.org/info/rfc8623.

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.

   [RFC4875] 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.
   [RFC5671] examines the applicability of PCE for the path computation
   for P2MP TE LSPs.

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 [RFC8306].

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. [RFC8231] provides the fundamental extensions to PCEP needed for stateful PCE to support general functionality for P2P TE LSP. [RFC8281] provides extensions to PCEP needed for stateful PCE-initiated P2P TE LSP. This document complements that work by focusing on PCEP 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", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Terminology

Terminology used in this document is the same as terminology used in [RFC8231], [RFC8281], and [RFC8306].

3. Supporting P2MP TE LSPs 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. [RFC8231] defines the extensions to PCEP needed for stateful operation of P2P TE LSPs. This document complements the previous work by focusing on 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 a PCEP-specific LSP identifier (PLSP-ID) ([RFC8231]). For P2MP, where the size of the message is much larger, this is an added advantage. When using a stateless PCE, a request to modify an existing P2MP tree requires that all the leaves are presented in the PCEP messages along with all the path information. But when using a

stateful PCE, the PCEP messages can use a PLSP-ID to represent all
information about the LSP that has previously been exchanged in PCEP
messages, and it is only necessary to encode the modifications (such
as new or removed leaf nodes). The PLSP-ID provides an index into
the LSP-DB at the PCE and identifies the LSP at the PCC.

In environments where the P2MP TE LSPs 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 [RFC8281] further describes the motivation
behind the PCE-Initiation capability, which is equally applicable to
P2MP TE LSPs.

3.2. Objectives

The objectives for the protocol extensions to support P2MP TE LSPs
for stateful PCE are the same as the objectives described in
Section 3.2 of [RFC8231].

4. Functions to Support P2MP TE LSPs for Stateful PCEs

[RFC8231] 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
   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 LSPs.

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 [RFC8231]); 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 [RFC8281].

5. Architectural Overview of Protocol Extensions

5.1. Extension of PCEP Messages

   Two new PCEP messages are defined in [RFC8231] to support stateful
   PCE for P2P TE LSPs. In this document, these messages are extended
   as follows to support P2MP TE LSPs.

   Path Computation State Report (PCRpt): Each P2MP TE LSP State Report
      in a PCRpt message contains the actual P2MP TE LSP path
      attributes, the LSP status, etc. An LSP State Report carried in 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 messages
      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 in a PCUpd message is also used to return LSP delegations
      if at any point the PCE no longer desires control of a P2MP TE
      LSP. The PCUpd message is described in Section 6.2.

   Further, a new PCEP message is defined in [RFC8281] to support
   stateful PCE instantiation of P2P TE LSPs. In this document, this
   message is extended as follows to support P2MP TE LSPs.

   Path Computation LSP Initiate Message (PCInitiate): PCInitiate is a
      PCEP message sent by a PCE to a PCC to trigger the instantiation
      or deletion of a P2MP TE LSP. 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 passive stateful PCE
   for P2P TE LSPs in [RFC8231]. In this document, these messages are
   extended to support P2MP TE LSPs as well.

5.2. Capability Advertisement

   During the PCEP initialization phase, as per Section 7.1.1 of
   [RFC8231], PCEP speakers advertise Stateful capability via the
   STATEFUL-PCE-CAPABILITY TLV in the OPEN object. Various flags are
   defined for the STATEFUL-PCE-CAPABILITY TLV defined in [RFC8231] and
   updated in [RFC8281] and [RFC8232].

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

   N (P2MP-CAPABILITY flag - 1 bit): If set to 1 by a PCC, the N Flag
      indicates that the PCC is willing to send P2MP LSP State Reports
      whenever there's a change to the parameters or operational status
      of the P2MP LSP; if set to 1 by a PCE, the N Flag indicates that
      the PCE is interested in receiving LSP State Reports whenever
      there is a parameter or operational status change to the P2MP LSP.
      The P2MP-CAPABILITY Flag MUST be advertised by both a PCC and a
      PCE for the P2MP extension (as per this document) of the PCRpt
      messages to be allowed on a PCEP session.

   M (P2MP-LSP-UPDATE-CAPABILITY flag - 1 bit): 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 the P2MP extension (as per this document) of the PCUpd
      messages to be allowed on a PCEP session.

   P (P2MP-LSP-INSTANTIATION-CAPABILITY flag - 1 bit): If set to 1 by a
      PCC, the P Flag indicates that the PCC allows instantiation of a
      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 [RFC8306].

5.3. IGP Extensions for Stateful PCE P2MP Capabilities Advertisement

   When the PCC is a Label Switching Router (LSR) participating in the
   IGP (either 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
PCE Discovery (PCED) 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 bit flags are defined in [RFC5088]. This document
defines new capability bits for the stateful PCE with P2MP as
follows:

```
            Bit                 Capability
            13                  Active Stateful PCE with P2MP
            14                  Passive Stateful PCE with P2MP
            15                  PCE-Initiation with P2MP
```

Note that, while active, passive, or initiation stateful PCE
capabilities for P2MP may be advertised during discovery, PCEP
Speakers that wish to use stateful PCEP for P2MP TE LSPs 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
   [RFC8231]) are applicable for the P2MP TE LSPs as well. The
   optimizations described in [RFC8232] can also be applied for P2MP TE
   LSPs.

5.5. LSP Delegation

   LSP delegation operations (described in Section 5.7 of [RFC8231]) 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 [RFC8231]) are applicable for P2MP TE LSPs as well.

   The PCReq and PCRep message format for P2MP TE LSPs is described in
   Sections 3.4 and 3.5 of [RFC8306], respectively.

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

   The extensions for the Request and Response message for passive
   stateful operations on P2MP TE LSPs are described in Sections 6.3 and
   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
   [RFC8231]) 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 is described in
   Section 6.2.

5.6.3. PCE-Initiated LSP

   As per Section 5.1 of [RFC8281], 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 LSPs (see details in
   Section 6.5).

   The instantiation and deletion operations for P2MP TE LSPs are the
   same as for P2P LSPs as described in Sections 5.3 and 5.4 of
   [RFC8281].

5.6.3.1. P2MP TE LSPs Instantiation

   The instantiation operation of P2MP TE LSPs is the same as the LSP
   instantiation operation defined in Section 5.3 of [RFC8281]; this
   includes the handling of the PLSP-ID, SYMBOLIC-PATH-NAME TLV, etc.
   The processing rules and use of error codes remain unchanged. The N

   (P2MP) flag (Section 7.1) MUST be set in the LSP object in the
   PCInitiate message by the PCE to specify that the instantiation is
   for P2MP TE LSPs. Like the PLSP-ID (as per [RFC8281]), the P2MP-LSP-
   IDENTIFIERS TLV SHOULD NOT be included in the LSP object in
   PCInitiate messages and MUST be ignored on receipt. These
   identifiers are generated by the PCC on receipt of the PCInitiate
   message and reported via a PCRpt message to the PCE.

5.6.3.2. P2MP TE LSPs Deletion

   The deletion operation of P2MP TE LSPs is the same as the LSP
   deletion operation defined in Section 5.4 of [RFC8281]; this entails
   sending an LSP Initiate Message with an LSP object carrying the PLSP-
   ID of the LSP to be removed as well as a Stateful PCE Request
   Parameter (SRP) object with the R flag set (LSP-REMOVE as per
   Section 5.2 of [RFC8281]). The processing rules and error codes
   remain unchanged.

5.6.3.3. Adding and Pruning Leaves for the P2MP TE LSP

   The adding of new leaves and pruning of old leaves for the PCE-
   initiated P2MP TE LSP MUST be carried in a PCUpd message as per
   Section 6.2 for P2MP TE LSP extensions. As defined in [RFC8306],
   leaf type = 1 is used for adding new leaves, and leaf type = 2 is
   used for pruning old leaves of P2MP END-POINTS Objects.

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

   Section 3.10 of [RFC8306] defines the error-handling procedures when
   adding new leaves to or removing old leaves from the existing P2MP
   tree for PCReq messages. The same error handling and error codes are
   also applicable to the stateful PCE messages as described in this
   document.

5.6.3.4. P2MP TE LSPs Delegation and Cleanup

   P2MP TE LSPs delegation and cleanup operations are the same as the
   LSP delegation and cleanup operations defined in Section 6 of
   [RFC8281]. The processing rules and error codes remain unchanged.

6. PCEP Message Extensions

   Message formats in this section, as those in [RFC8231], [RFC8281],
   and [RFC5440], are presented using Routing Backus-Naur Format (RBNF)
   as specified in [RFC5511].

6.1. The PCRpt Message

   As per Section 6.1 of [RFC8231], a 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 LSPs.

   The format of a 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>
                      <path>

   Where:
   <path> ::= <end-point-intended-path-pair-list>
              [<actual-attribute-list>
              <end-point-actual-path-pair-list>]
              [<intended-attribute-list>]

   <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>]
                      [<S2LS>]
                      <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 [RFC8306] is mandatory for
specifying the address of P2MP leaves, grouped by 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 MUST be
grouped in the END-POINTS object based on the operational status (O
field in S2LS objects) and leaf type (in END-POINTS objects). This
way, leaves of the same type that share the same operational status
can be grouped together. For reporting the status of delegated P2MP
TE LSPs, leaf type = 3 is used, whereas for nondelegated P2MP TE
LSPs, leaf type = 4 is used.

For a delegated P2MP TE LSP, configuration changes are reported via a
PCRpt message. For example, for adding new leaves, leaf type = 1 is
used in the END-POINTS object, and for removing old leaves, leaf type
= 2 is used.

Note that the compatibility with the [RFC8231] definition of <state-
report> is preserved. At least one instance of <END-POINTS> MUST be
present in this message for P2MP LSP.

Note that the ordering of <end-point-intended-path-pair-list>,
<actual-attribute-list>, <end-point-actual-path-pair-list>, and
<intended-attribute-list> is done to retain compatibility with state
reports for the P2P LSPs as per [RFC8231].

During state synchronization, the PCRpt message reports the status of
the full P2MP tree.

The S2LS object MUST be carried in a PCRpt message along with the
END-POINTS object when an N (P2MP) flag is set in an LSP object for
P2MP TE LSPs. If the S2LS object is missing, the receiving PCE MUST
send a PCEP Error (PCErr) message with Error-type=6 ("Mandatory
Object missing") and Error-value=13 ("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].

The S2LS object could be used in conjunction with the intended-path
(EXPLICIT_ROUTE object or ERO) as well as the actual-path
(RECORD_ROUTE object or RRO); for the same leaf, the state encoded in
the S2LS object associated with the actual-path MUST be used over the
intended-path.

If the E-bit (ERO-Compress bit) was set to 1 in the report, then the
path will be formed by an ERO followed by a list of
SECONDARY_EXPLICIT_ROUTE Objects (SEROs), or an RRO followed by a
list of SECONDARY_RECORD_ROUTE Objects (SRROs).

6.2. The PCUpd Message

As per Section 6.2 of [RFC8231], a PCUpd message is used to update
P2P TE LSP attributes. This document extends the PCUpd message in
updating the attributes of a 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>
                         <path>

    Where:
    <path> ::= <end-point-path-pair-list>
               <intended-attribute-list>

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

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

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

   Note that the compatibility with the [RFC8231] definition of <update-
   request> is preserved.

   The PCC SHOULD 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 a PCUpd message when the N
   flag is set in the LSP object for a 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 [RFC8306], a 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 a 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 [RFC8306], a 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 a 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 [RFC8281], a PCE sends a PCInitiate
   message to a PCC to recommend instantiation of a P2P TE LSP. This
   document extends the format of a PCInitiate message for the creation
   of P2MP TE LSPs, but the creation and deletion operations of P2MP TE
   LSPs are the same to the P2P TE LSPs.

   The format of a 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 the N flag (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
   [RFC8231].

The END-POINTS object MUST be carried in a PCInitiate message when
the N flag is set in an LSP object for a 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 LSPs Update Request

An LSP Update Request message is sent by an active stateful PCE to
update the P2MP TE LSPs parameters or attributes. An example of a
PCUpd message for P2MP TE LSPs 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 requests an update of the path taken
to some of the leaves in a P2MP tree. The update request uses the
END-POINT type 3 (modified/reoptimized). The ERO list represents the
source-to-leaves 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

The LSP State Report message is sent by a PCC to report or delegate
the P2MP TE LSP. The leaves of the P2MP TE LSP are grouped in the
END-POINTS object based on the operational status and the leaf type.
An example of a PCRpt message is described below for a delegated P2MP
TE LSP to add new leaves to an existing P2MP TE LSP:

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

An example of a PCRpt message for a 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 (remove)
          S2LS (O=UP)
          ERO list (empty)
```

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

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

In this example, the PCRpt message is in response to a PCUpd message.
The PCRpt message includes the corresponding SRP object and indicates
that some leaves are up (with the actual path) and some are down.

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

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

6.6.3. P2MP TE LSPs Initiation Request

An LSP Initiation Request message is sent by a stateful PCE to create
a P2MP TE LSP. An example of a PCInitiate message for a P2MP TE LSP
is described below:

```
        Common Header
        SRP
        LSP with P2MP flag set
        END-POINTS for leaf type 1 (add)
          ERO list
```

In this example, a stateful PCE requests the creation of a P2MP TE
LSP. The initiation request uses the END-POINT type 1 (new leaves).
The ERO list represents the source-to-leaves path. The initiate
message encodes the full P2MP tree in this case.

7. PCEP Object Extensions

   The new PCEP TLVs defined in this document are in compliance with the
   PCEP TLV format defined in [RFC5440].

7.1. LSP Object Extension

   The LSP Object is defined in Section 7.3 of [RFC8231]. It specifies
   the PLSP-ID to uniquely identify an LSP that is constant for the life
   time of a PCEP session. Similarly, for a P2MP tunnel, the PLSP-ID
   uniquely identifies a P2MP TE LSP. This document adds the following
   flags to the LSP Object:

   N (P2MP flag - 1 bit): If the N flag is set to 1, it indicates that
      the message is for a P2MP TE LSP.

   F (Fragmentation flag - 1 bit): If the F flag is unset (0), it
      indicates that the LSP is not fragmented or that it is the last
      piece of the fragmented LSP. If the F flag is set to 1, it
      indicates that the LSP is fragmented and that it is not the last
      piece of the fragmented LSP. The receiver needs to wait for
      additional fragments until it receives an LSP with the same PLSP-
      ID and with the F-bit set to 0. See Section 8 for further
      details.

   E (ERO-compression flag - 1 bit): If the E flag is set to 1, it
      indicates the route is in compressed format (that is, Secondary
      Explicit Route Object (SERO) and Secondary Record Route Object
      (SRRO) objects [RFC8306] are in use).

   The flags defined in this section (N, F, and E) are used in PCRpt,
   PCUpd, or PCInitiate messages. In the case of PCReq and PCRep
   messages, these flags have no meaning and thus MUST be ignored. The
   corresponding flags in the RP (Request Parameters) object are used as
   described in [RFC8306].

7.1.1. P2MP-LSP-IDENTIFIERS TLV

   [RFC8231] specifies the LSP-IDENTIFIERS TLVs to be included in the
   LSP object. For P2MP TE LSP, this document defines P2MP-LSP-
   IDENTIFIERS TLVs for the LSP object. There are two P2MP-LSP-
   IDENTIFIERS TLVs, one for IPv4 and one for IPv6. The P2MP-LSP-
   IDENTIFIERS TLV MUST be included in the LSP object in a PCRpt message
   for P2MP TE LSPs. If the N bit is set in the LSP object in the PCRpt
   message but the P2MP-LSP-IDENTIFIER TLV is absent, the PCE MUST
   respond with a PCErr message carrying error-type 6 ("mandatory object
   missing") and error-value 14 ("P2MP-LSP-IDENTIFIERS TLV missing") and
   close the PCEP session.

The P2MP-LSP-IDENTIFIERS TLV MAY be included in the LSP object in the
PCUpd message for P2MP TE LSPs. The special value of all zeros for
all the fields in the value portion of the TLV is used to refer to
all paths pertaining to a particular PLSP-ID. The length of the TLV
remains fixed based on the IP version.

The P2MP-LSP-IDENTIFIERS TLV SHOULD NOT be used in a PCInitiate
message (see Section 5.6.3.1) and MAY optionally be included in the
LSP object in the PCReq and the PCRep message for P2MP TE LSP.

The format of the IPV4-P2MP-LSP-IDENTIFIERS TLV is shown in Figure 1:

```
 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=32             |           Length=16           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv4 Tunnel Sender Address                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            LSP ID             |           Tunnel ID           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Extended Tunnel ID                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           P2MP ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
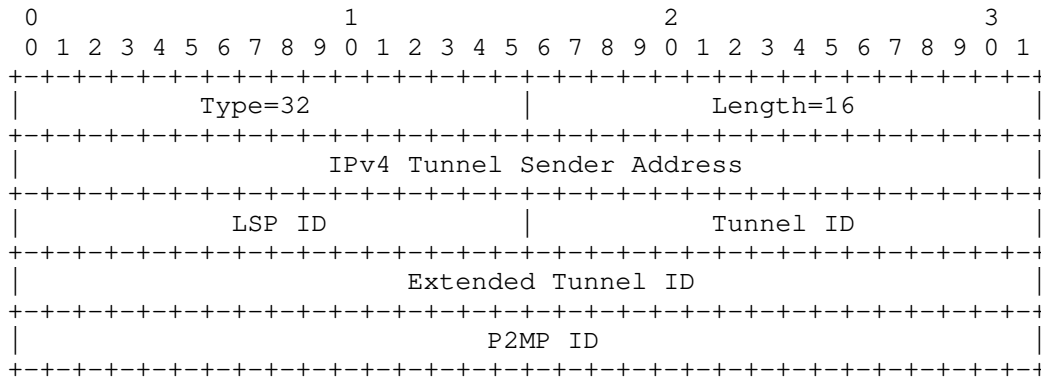
            Figure 1: IPV4-P2MP-LSP-IDENTIFIERS TLV Format

The type (16 bits) of the TLV is 32. The length (16 bits) 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]. See Section 4.6.2.1 of [RFC3209] for the
   LSP_TUNNEL_IPv4 Sender Template Object.

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

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

Extended Tunnel ID: Contains the 32-bit 'Extended Tunnel ID'
   identifier defined in [RFC3209]. See Section 4.6.1.1 of [RFC3209]
   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-IDENTIFIERS TLV is shown in Figure 2:

```
 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=33             |          Length=40            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                   IPv6 tunnel sender address                  |
+                        (16 octets)                            +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           LSP ID              |          Tunnel ID            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                      Extended Tunnel ID                       |
+                        (16 octets)                            +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           P2MP ID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
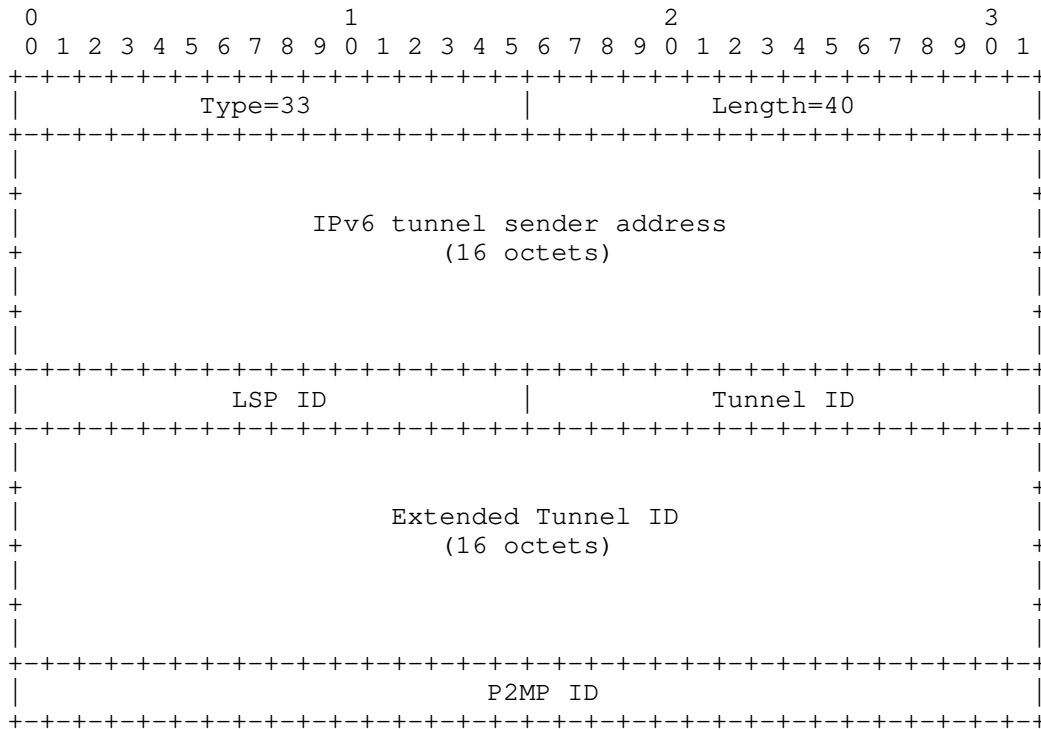
              Figure 2: IPV6-P2MP-LSP-IDENTIFIERS TLV Format

   The type (16 bits) of the TLV is 33. The length (16 bits) 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]. See Section 4.6.2.2 of [RFC3209] for the
      LSP_TUNNEL_IPv6 Sender Template Object.

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

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

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

   P2MP ID: Defined above under Figure 1.

   Tunnel ID: Remains constant over the lifetime of a tunnel.

7.2. S2LS Object

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

   S2LS Object-Class is 41.

   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 3: S2LS Object Format

   Flags (32 bits): The following flag is currently defined:

   O (Operational - 3 bits) The O field represents the operational
      status of the group of destinations. The values are as per the
      Operational field in the LSP object defined in Section 7.3 of
      [RFC8231].

   Unassigned bits are reserved for future uses. They MUST be set to 0
   on transmission and MUST be ignored on receipt.

   When the N flag is set in an LSP object, the O field in the LSP
   object represents the operational status of the full P2MP TE LSP, and
   the O field in the S2LS object represents the operational status of a
   group of destinations encoded within the END-POINTS object. If there
   is a conflict between the O field in the LSP and the S2LS object (for

example, the O field in the LSP corresponds to down whereas the O
field in the S2LS is up), the PCEP speaker MUST generate an error
with error-type 10 ("Reception of an invalid object") and error-value
22 ("Mismatch of O field in S2LS and LSP object").

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

8. Message Fragmentation

The total PCEP message length, including the common header, is
(2^16)-1 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 flag is used in the LSP object to signal that the
initial report, update, or initiate request was too large to fit into
a single PCEP 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.

The fragmentation procedure described below for report or update
messages is similar to [RFC8306], 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 flag
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.

The Error-Type value 18 ("P2MP Fragmentation Error") is used to
report any error associated with the fragmentation of a P2MP PCEP
message. A new error-value 2 indicates "Fragmented report failure"
and is used if a PCE does not receive the last part of the fragmented
message.

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 flag 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.

The Error-Type value 18 ("P2MP Fragmentation Error") is used to
report any error associated with the fragmentation of a P2MP PCEP
message. A new error-value 3 indicates "Fragmented update failure"
and is used if a PCC does not receive the last part of the fragmented
message.

8.3. PCInitiate Fragmentation Procedure

Once the PCE initiates to set up a P2MP TE LSP, a PCInitiate message
is sent to the PCC. If the initiate request is too large to fit into
a single PCInitiate message, the PCE will split the initiate request
over multiple messages. Each PCInitiate message sent by the PCE,
except the last one, will have the F flag 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.

The Error-Type value 18 ("P2MP Fragmentation Error") is used to
report any error associated with the fragmentation of a P2MP PCEP
message. A new error-value 4 indicates "Fragmented instantiation
failure" and is used if a PCC does not receive the last part of the
fragmented message.

9. Nonsupport of P2MP TE LSPs for Stateful PCE

The PCEP extensions described in this document for stateful PCEs with
P2MP capability MUST NOT be used if the PCE has not advertised its
stateful capability with P2MP as per Section 5.2. If the PCC
supports the extensions as per this document (understands the N
(P2MP-CAPABILITY) and M (P2MP-LSP-UPDATE-CAPABILITY) flags in the LSP
object) but did not advertise this capability, then upon receipt of a
PCUpd message from the PCE, it SHOULD generate a PCErr with error-
type 19 ("Invalid Operation"), error-value 12 ("Attempted LSP Update
Request for P2MP if active stateful PCE capability for P2MP was not
advertised"), and terminate the PCEP session. If the PCE supports
the extensions as per this document (understands the N (P2MP-
CAPABILITY) 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 11 ("Attempted LSP State Report for P2MP if stateful PCE
capability for P2MP was not advertised"), and it SHOULD terminate the
PCEP session.

   If a Stateful PCE receives a P2MP TE LSP report message and the PCE
   does not understand the N (P2MP-CAPABILITY) flag in the LSP object,
   and therefore the PCEP extensions described in this document, then
   the Stateful PCE would act as per Section 6.1 of [RFC8231] (and
   consider the PCRpt message as invalid).

   The PCEP extensions described in this document for PCC or PCE with
   the PCE-Initiation capability for P2MP TE LSPs MUST NOT be used if
   the PCC or PCE has not advertised its stateful capability with
   Instantiation and P2MP capability as per Section 5.2. If the PCC
   supports the extensions as per this document (understands the P
   (P2MP-LSP-INSTANTIATION-CAPABILITY) flag) but did not advertise this
   capability, then upon receipt of a PCInitiate message from the PCE,
   it SHOULD generate a PCErr with error-type 19 ("Invalid Operation"),
   error-value 13 ("Attempted LSP Instantiation Request for P2MP if
   stateful PCE instantiation capability for P2MP was not advertised"),
   and terminate the PCEP session.

10. Manageability Considerations

   All manageability requirements and considerations listed in
   [RFC5440], [RFC8306], [RFC8231], and [RFC8281] apply to PCEP
   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 configuration of 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 [PCE-PCEP-YANG] can be extended to include
   advertised P2MP stateful capabilities, P2MP synchronization status,
   and the delegation status of a P2MP LSP, etc. The statistics module
   should also count data related to P2MP LSPs.

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], [RFC8306], [RFC8231], and [RFC8281].

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],
   [RFC8306], [RFC8231], and [RFC8281].

   Stateful PCE features for P2MP LSPs would help with network
   operations.

11. IANA Considerations

   IANA has registered the code points for the protocol elements defined
   in this document.

11.1. PCE Capabilities in IGP Advertisements

   IANA has registered the new bits in the OSPF Parameters "Path
   Computation Element (PCE) Capability Flags" registry, as follows:

        Bit   Capability Description   Reference

        13   Active Stateful PCE with P2MP   RFC 8623
        14   Passive Stateful PCE with P2MP   RFC 8623
        15   Stateful PCE Initiation with P2MP RFC 8623

11.2. STATEFUL-PCE-CAPABILITY TLV

   The STATEFUL-PCE-CAPABILITY TLV is defined in [RFC8231], and the
   "STATEFUL-PCE-CAPABILITY TLV Flag Field" subregistry was created to
   manage the flags in the TLV. IANA has registered the following code
   points in the aforementioned registry.

        Bit   Description   Reference

        23   P2MP-LSP-INSTANTIATION-CAPABILITY   RFC 8623
        24   P2MP-LSP-UPDATE-CAPABILITY   RFC 8623
        25   P2MP-CAPABILITY   RFC 8623

11.3. LSP Object

   The LSP object is defined in [RFC8231], and the "LSP Object Flag
   Field" subregistry was created to manage the Flags field of the LSP
   object.

   IANA has registered the following code points in the aforementioned
   registry.

        Bit   Description   Reference

        1   ERO-compression   RFC 8623
        2   Fragmentation   RFC 8623
        3   P2MP   RFC 8623

11.4. PCEP-ERROR Object

   IANA has registered the new error values within the "PCEP-ERROR
   Object Error Types and Values" subregistry of the PCEP Numbers
   registry, as follows:

        Error-Type Meaning
           6   Mandatory Object missing [RFC5440]
                       Error-value = 13: S2LS object missing
                       Error-value = 14: P2MP-LSP-IDENTIFIERS TLV missing
          10   Reception of an invalid object [RFC5440]
                       Error-value = 22: Mismatch of O field in S2LS
                             and LSP object
          18   P2MP Fragmentation Error [RFC8306]
                       Error-value = 2: Fragmented Report failure
                       Error-value = 3: Fragmented Update failure
                       Error-value = 4: Fragmented Instantiation failure
          19   Invalid Operation [RFC8231]
                       Error-value = 11: Attempted LSP State Report
                             for P2MP if stateful PCE capability
                             for P2MP was not advertised
                       Error-value = 12: Attempted LSP Update Request
                             for P2MP if active stateful PCE capability
                             for P2MP was not advertised
                       Error-value = 13: Attempted LSP Instantiation
                             Request for P2MP if stateful PCE
                             instantiation capability for P2MP was not
                             advertised

   The reference for all new Error-values above is RFC 8623.

11.5. PCEP TLV Type Indicators

   IANA has registered the following code points in the existing "PCEP
   TLV Type Indicators" registry as follows:

        Value   Description   Reference

          32   P2MP-IPV4-LSP-IDENTIFIERS   RFC 8623
          33   P2MP-IPV6-LSP-IDENTIFIERS   RFC 8623

11.6. PCEP Object

   IANA has registered the new object-class values and object types
   within the "PCEP Objects" subregistry of the PCEP Numbers registry,
   as follows.

        Object-Class Value Name   Reference

          41   S2LS   RFC 8623
                            Object-Type
                            0: Reserved
                            1: S2LS

11.7. S2LS Object

   A new subregistry, named "S2LS Object Flag Field", has been created
   within the "Path Computation Element Protocol (PCEP) Numbers"
   registry to manage the 32-bit flag field of the S2LS object. New
   values are to be assigned by Standards Action [RFC8126]. 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

               0-28   Unassigned
               29-31   Operational (3 bits) RFC 8623

12. Security Considerations

   The stateful operations on P2MP TE LSPs are more CPU intensive and
   also utilize more bandwidth on the wire (in comparison to P2P TE
   LSPs). If a rogue PCC were able to request unauthorized stateful PCE
   operations, then it may be able to mount a DoS attack against a PCE,
   which would disrupt the network and deny service to other PCCs.
   Similarly, an attacker may flood the PCC with PCUpd messages at a
   rate that exceeds either the PCC's ability to process them or the
   network's ability to signal the changes by either spoofing messages
   or compromising the PCE itself.

   Consequently, it is important that implementations conform to the
   relevant security requirements as listed below:

   o As per [RFC8231], it is RECOMMENDED that these PCEP extensions
      only be activated on authenticated and encrypted sessions across
      PCEs and PCCs belonging to the same administrative authority,
      using Transport Layer Security (TLS) [RFC8253] as per the
      recommendations and best current practices in [RFC7525] (unless
      explicitly set aside in [RFC8253]).

   o Security considerations for path computation requests and
      responses are as per [RFC8306].

   o Security considerations for stateful operations (such as state
      report, synchronization, delegation, update, etc.) are as per
      [RFC8231].

   o Security considerations for the LSP instantiation mechanism are as
      per [RFC8231].

   o Security considerations as stated in Sections 10.1, 10.6, and 10.7
      of [RFC5440] continue to apply.

13. References

13.1. 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,
              <https://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,
              <https://www.rfc-editor.org/info/rfc3209>.

   [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,
              <https://www.rfc-editor.org/info/rfc4875>.

   [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, <https://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, <https://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,
              <https://www.rfc-editor.org/info/rfc5440>.

   [RFC5511] Farrel, A., "Routing Backus-Naur Form (RBNF): A Syntax
              Used to Form Encoding Rules in Various Routing Protocol
              Specifications", RFC 5511, DOI 10.17487/RFC5511, April
              2009, <https://www.rfc-editor.org/info/rfc5511>.

   [RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre,
              "Recommendations for Secure Use of Transport Layer
              Security (TLS) and Datagram Transport Layer Security
              (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May
              2015, <https://www.rfc-editor.org/info/rfc7525>.

   [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <https://www.rfc-editor.org/info/rfc8174>.

   [RFC8231] Crabbe, E., Minei, I., Medved, J., and R. Varga, "Path
              Computation Element Communication Protocol (PCEP)
              Extensions for Stateful PCE", RFC 8231,
              DOI 10.17487/RFC8231, September 2017,
              <https://www.rfc-editor.org/info/rfc8231>.

   [RFC8232] 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", RFC 8232,
              DOI 10.17487/RFC8232, September 2017,
              <https://www.rfc-editor.org/info/rfc8232>.

   [RFC8253] Lopez, D., Gonzalez de Dios, O., Wu, Q., and D. Dhody,
              "PCEPS: Usage of TLS to Provide a Secure Transport for the
              Path Computation Element Communication Protocol (PCEP)",
              RFC 8253, DOI 10.17487/RFC8253, October 2017,
              <https://www.rfc-editor.org/info/rfc8253>.

   [RFC8281] Crabbe, E., Minei, I., Sivabalan, S., and R. Varga, "Path
              Computation Element Communication Protocol (PCEP)
              Extensions for PCE-Initiated LSP Setup in a Stateful PCE
              Model", RFC 8281, DOI 10.17487/RFC8281, December 2017,
              <https://www.rfc-editor.org/info/rfc8281>.

   [RFC8306] Zhao, Q., Dhody, D., Ed., Palleti, R., and D. King,
              "Extensions to the Path Computation Element Communication
              Protocol (PCEP) for Point-to-Multipoint Traffic
              Engineering Label Switched Paths", RFC 8306,
              DOI 10.17487/RFC8306, November 2017,
              <https://www.rfc-editor.org/info/rfc8306>.

13.2. Informative References

   [PCE-PCEP-YANG]
              Dhody, D., Hardwick, J., Beeram, V., and J. Tantsura, "A
              YANG Data Model for Path Computation Element
              Communications Protocol (PCEP)", Work in Progress,
              draft-ietf-pce-pcep-yang-11, March 2019.

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

   [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,
              <https://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,
              <https://www.rfc-editor.org/info/rfc8051>.

   [RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for
              Writing an IANA Considerations Section in RFCs", BCP 26,
              RFC 8126, DOI 10.17487/RFC8126, June 2017,
              <https://www.rfc-editor.org/info/rfc8126>.

Contributors

   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

   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