PCE Working Group
Internet-Draft
Intended status: Standards Track
Expires: 3 September 2026

S. Sidor
Z. Ali
Cisco Systems, Inc.
C. Li
Huawei Technologies
M. Koldychev
Ciena Corporation
A. Stone
Nokia

2 March 2026

LSP State Reporting Extensions in Path Computation Element Communication Protocol (PCEP)
draft-sidor-pce-lsp-state-reporting-extensions-06

Abstract

The Path Computation Element Communication Protocol (PCEP) is defined in multiple RFCs for enabling communication between Path Computation Elements (PCEs) and Path Computation Clients (PCCs).

Although PCEP defines various Label Switched Path (LSP) identifiers, attributes, and constraints, there are operational attributes available on the PCC that can enhance path computation and improve the debugging experience, which are not currently supported in PCEP.

This document defines extensions to PCEP to include:

* Support for explicit or dynamic path types
* Mechanisms to mark LSPs as eligible for use as transit LSPs

Table of Contents

1. Introduction

A Stateful Path Computation Element (PCE) maintains comprehensive information on the current network state, including computed Label Switched Paths (LSPs), reserved network resources, and the pending path computation requests. This information is critical for computing paths for traffic-engineering LSPs and any associated or dependent LSPs.

This document introduces the ability to encode information regarding whether a path included in an Explicit Route Object (ERO) was specified explicitly or was the result of dynamic path computation executed by a PCE or PCC. Such information can aid debuggability and can be used by other PCEs in the network to avoid triggering unnecessary path computations for LSPs where it is not intended (e.g., PCE-initiated LSPs with an explicit path).

Additionally, this document specifies a set of extensions to PCEP to enhance the accuracy of path computations by considering LSP transit eligibility, for example, as described in the case of LSP stitching in [I-D.ietf-pce-stateful-interdomain].

The Explicit Path mechanism described in this document is applicable to all path setup types. The Transit Eligible mechanism described in this document is applicable to LSPs that have an associated Binding Label/SID as defined in [RFC9604].

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

The following terms are used in this document:

* Binding Label/SID: A Binding Segment Identifier (SID) or Binding Label associated with an SR Policy or SR-TE LSP, as defined in [RFC9604].
* CP: Candidate Path, one of the candidate paths of an SR Policy.
* ERO: Explicit Route Object.
* LSP: Label Switched Path.
* PCC: Path Computation Client.
* PCE: Path Computation Element.
* PCEP: Path Computation Element Protocol.

* SL: Segment List, a sequence of segments describing a path through the network.
* Transit LSP: An LSP whose Binding Label/SID is used as a segment (hop) in the path computed for another LSP. By referring to the Binding Label/SID of the Transit LSP as a single segment, the head-end of the outer LSP can steer traffic along the inner LSP's path without having to encode all of its individual hops. This technique is used, for example, in inter-domain LSP stitching as described in [I-D.ietf-pce-stateful-interdomain].

3. Protocol Extensions

3.1. STATEFUL-PCE-CAPABILITY TLV

New flags are defined for the STATEFUL-PCE-CAPABILITY TLV, originally defined in Section 5.4 of [RFC8231].

* T (TRANSIT-ELIGIBLE-CAPABILITY): If set, indicates that the PCEP peer supports the advertisement of the Transit Eligible flag in the LSP-EXTENDED-FLAG as described in Section 4.2.
* X (EXPLICIT-PATH-CAPABILITY): If set, indicates that the PCEP peer supports the advertisement of the Explicit flag in the LSP-EXTENDED-FLAG.

3.2. LSP-EXTENDED-FLAG TLV

New flags are introduced in the LSP-EXTENDED-FLAG TLV, which was initially defined in Section 3.1 of [RFC9357].

* X (Explicit): If set, indicates that the path encoded in the ERO is explicitly specified and not dynamically computed by the PCEP peer.
* T (Transit Eligible): If set, indicates that the Binding Label/SID [RFC9604] of the LSP can be used in paths computed for other LSPs.

4. Operation

4.1. Explicit or Dynamic Path

The X flag in the LSP-EXTENDED-FLAG TLV MUST NOT be set unless the EXPLICIT-PATH-CAPABILITY is supported by both PCEP peers.

If a PCEP peer receives the X flag set in the LSP-EXTENDED-FLAG TLV without having negotiated EXPLICIT-PATH-CAPABILITY, it MUST send a PCErr message with Error-Type 10 and Error-Value TBA5 (see Section 8.3) and MUST ignore the flag.

If the EXPLICIT-PATH-CAPABILITY is not advertised, the PCE implementation MAY use a local policy to determine the type of path.

For instance, if an operator requests the creation of a PCE-initiated Candidate Path with an explicit path, then such a path will be encoded in the ERO object of the PCInitiate message sent to the PCC. If the delegation of such LSP is transferred to another PCE, the new PCE will not know whether the path of the LSP was computed dynamically or explicitly specified by the operator.

Even if a similar problem does not exist for LSPs originated on the PCC, information about the type of path may be valuable for other purposes, such as debuggability.

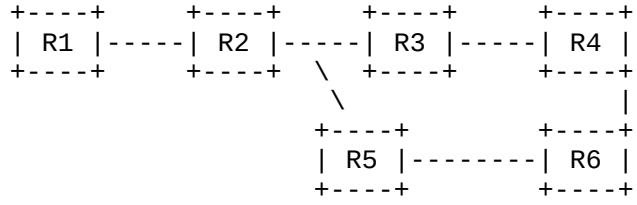
For PCC-initiated LSPs, the X flag value is initially set by the PCC in the PCRpt message, and the PCE MUST set the flag value in PCUpd messages for such LSPs based on the last reported state.

For PCE-initiated LSPs, the X flag value is initially set by the PCE in the PCInitiate message but MAY be modified in subsequent PCUpd messages. The PCC MUST set the flag value in PCRpt messages for such LSPs based on the value received from the last PCInitiate or PCUpd message.

It is important to note that the Explicit/Dynamic path type is a path-level property indicating the origin of the path decision (operator-defined vs. algorithmically computed), while strict and loose subobjects are hop-level properties defined per ERO subobject in [RFC5440] that describe how precisely each individual hop must be followed. Both explicitly specified and dynamically computed paths can contain a mix of strict and loose subobjects:

* For an Explicitly Specified Path (X flag set): An operator might define a path that explicitly specifies certain hops (strict) but allows the forwarding plane to select the exact route for other segments (loose). For example, "go strictly through Router A, then loosely to Network B, then strictly through Router C."
* For a Dynamically Computed Path (X flag not set): A PCE, when computing a path, might generate an ERO that includes strict hops (e.g., to satisfy specific constraints like avoiding certain links) and loose hops (e.g., where flexibility is allowed to optimize for metrics like shortest path).

The following example illustrates the distinction. Consider the topology below:



An operator wishes to create an LSP from R1 to R4 and explicitly requires that traffic passes through R2 (e.g., for policy reasons). The operator does not prescribe the exact route beyond R2. The resulting ERO would contain R2 as a strict subobject followed by R4 as a loose subobject. Because the overall path was defined by the operator, the X flag is set (Explicit Path), even though one of the hops is loose. The forwarding plane may choose either R2->R3->R4 or R2->R5->R6->R4 to reach R4.

By contrast, consider a PCE that computes a path R1->R2->R3->R4 using all strict subobjects to satisfy a specific bandwidth constraint. Because the path was computed algorithmically by the PCE, the X flag is not set (Dynamic Path), even though every hop is strict.

This distinction is operationally significant: a downstream PCE that receives delegation for an LSP can use the X flag to determine whether it should attempt to recompute the path. For a PCE-initiated LSP with X flag set, the PCE SHOULD NOT recompute the path unless explicitly instructed to do so, as the explicit path reflects operator intent.

For LSPs with multiple Segment Lists (SLs) per Candidate Path (CP), the path type (explicit or dynamic) is advertised only once per Candidate Path. Therefore, it is not possible to mix dynamic and explicit Segment Lists within a single Candidate Path.

4.2. LSP Transit Eligibility

The T flag in the LSP-EXTENDED-FLAG TLV MUST NOT be set unless the TRANSIT-ELIGIBLE-CAPABILITY is supported by both PCEP peers.

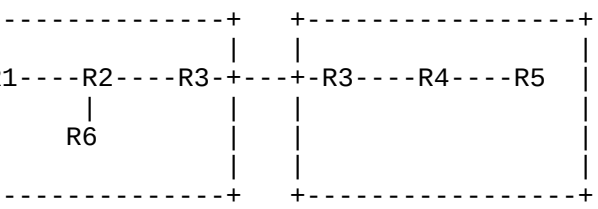
If a PCEP peer receives the T flag set in the LSP-EXTENDED-FLAG TLV without having negotiated TRANSIT-ELIGIBLE-CAPABILITY, it MUST send a PCErr message with Error-Type 10 and Error-Value TBA6 (see Section 8.3) and MUST ignore the flag.

If the TRANSIT-ELIGIBLE-CAPABILITY is not advertised, the PCE implementation MAY use a local policy to determine the value of the Transit Eligible flag.

For PCC-initiated LSPs, the T flag value is initially set by the PCC in the PCRpt message. The PCE MUST set the flag value in PCUpd messages for these LSPs based on the last reported state.

For PCE-initiated LSPs, the T flag value is initially set by the PCE in the PCInitiate message but MAY be modified in subsequent PCUpd messages. The PCC MUST set the flag value in PCRpt messages for these LSPs based on the value received from the latest PCInitiate or PCUpd message.

The following example illustrates the use of the T flag. Consider an inter-domain topology where a PCE is responsible for computing an end-to-end LSP across two domains:



LSP_B: R1 -> R3 (Binding SID: BS1, T flag set)
LSP_C: R3 -> R5 (Binding SID: BS2, T flag set)

LSP_B is an intra-domain LSP within Domain 1, traversing R1->R2->R3, with a Binding SID BS1 assigned to it. LSP_C is an intra-domain LSP within Domain 2, traversing R3->R4->R5, with a Binding SID BS2 assigned to it. Both LSP_B and LSP_C have the T flag set in their LSP-EXTENDED-FLAG TLV, indicating to the PCE that their respective Binding SIDs may be used as segments in paths computed for other LSPs.

When an operator requests an end-to-end LSP_A from R1 to R5, the PCE can leverage the T flag information to construct the path. Instead of computing a full explicit path enumerating every hop across both domains, the PCE can use BS1 and BS2 as single-hop segments in the ERO for LSP_A. The resulting ERO for LSP_A would be: {BS1 (strict), BS2 (strict)}, stitching the two intra-domain LSPs together. Without the T flag, the PCE would have no standardized way to know which LSPs have Binding SIDs available and are eligible for use in this manner, potentially leading to suboptimal path computation or requiring out-of-band coordination.

5. Manageability Considerations

All manageability requirements and considerations listed in [RFC5440] and [RFC8231] apply to the PCEP extensions defined in this document. In addition, requirements and considerations listed in this section apply.

5.1. Control of Function and Policy

A PCE or PCC implementation MAY allow the capability of supporting PCEP extensions introduced in this document to be enabled or disabled as part of the global configuration.

5.2. Information and Data Models

An implementation SHOULD allow the operator to view the capability defined in this document. It is expected that a future version of the PCEP YANG module [RFC9826] will be extended to include the capability introduced in Section 3.1 for the PCEP peer.

5.3. Verify Correct Operations

Operation verification requirements already listed in [RFC5440] and [RFC8231] are applicable to mechanisms defined in this document.

5.4. Impact on Network Operations

The mechanisms defined in [RFC5440] and [RFC8231] also apply to the PCEP extensions defined in this document.

6. Implementation Status

[Note to the RFC Editor - remove this section before publication, as well as remove the reference to RFC 7942.]

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [RFC7942]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [RFC7942], "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

7. Security Considerations

The security considerations described in [RFC8231] and [RFC5440] are applicable to this document.

The X (Explicit) flag defined in this document reveals operator intent regarding how a path was determined -- whether it was hand-crafted by an operator or dynamically computed. In networks where this distinction is sensitive, an attacker with access to PCEP messages could use this information to infer network management policies. The security mechanisms defined in [RFC5440] (TCP-AO) and [RFC8231] (PCEPS with TLS) are sufficient to protect the confidentiality and integrity of this information.

The T (Transit Eligible) flag defined in this document indicates that the Binding Label/SID of an LSP may be used in paths computed for other LSPs (e.g., for LSP stitching). A misconfigured or malicious node setting this flag without authorization could cause traffic to be steered through unintended paths, potentially leading to policy violations or routing loops. Implementations SHOULD enforce capability negotiation as described in Section 4.2 and MAY apply local policies to restrict the use of LSPs for transit, regardless of the flag value.

These extensions do not introduce any new authentication or encryption requirements beyond those already specified in [RFC5440] and [RFC8231].

8. IANA Considerations

8.1. STATEFUL-PCE-CAPABILITY TLV Flag

IANA maintains a registry, named "STATEFUL-PCE-CAPABILITY TLV Flag Field", within the "Path Computation Element Protocol (PCEP) Numbers" registry group to manage the Flags field of the STATEFUL-PCE-CAPABILITY TLV. The registration policy for this registry is Standards Action [RFC8126]. IANA is requested to make the following assignments:

Bit	Description	Reference
TBA1	T (TRANSIT-ELIGIBLE-CAPABILITY)	This document
TBA2	X (EXPLICIT-PATH-CAPABILITY)	This document

Table 1

8.2. LSP-EXTENDED-FLAG TLV Flags

IANA maintains a registry, named "LSP-EXTENDED-FLAG TLV Flag Field", within the "Path Computation Element Protocol (PCEP) Numbers" registry group to manage the Flags field of the LSP-EXTENDED-FLAG TLV. The registration policy for this registry is Standards Action [RFC8126]. IANA is requested to make the following assignments:

Bit	Description	Reference
TBA3	X (Explicit)	This document
TBA4	T (Transit Eligible)	This document

Table 2

8.3. PCEP Error Object Error Types and Values

IANA maintains a registry, named "PCEP-ERROR Object Error Types and Values", within the "Path Computation Element Protocol (PCEP) Numbers" registry group. The registration policy for this registry is IETF Review [RFC8126]. IANA is requested to make the following assignments under Error-Type 10 "Reception of an invalid object" [RFC5440]:

Error-Type	Error-Value	Description	Reference
10	TBA5	X flag set in LSP-EXTENDED-FLAG TLV without EXPLICIT-PATH-CAPABILITY negotiated	This document
10	TBA6	T flag set in LSP-EXTENDED-FLAG TLV without TRANSIT-ELIGIBLE-CAPABILITY negotiated	This document

Table 3

9. References

9.1. 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>.

[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>.

[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>.

[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>.

[RFC9357] Xiong, Q., "Label Switched Path (LSP) Object Flag Extension for Stateful PCE", RFC 9357, DOI 10.17487/RFC9357, February 2023, <https://www.rfc-editor.org/info/rfc9357>.

[RFC9604] Sivabalan, S., Filsfils, C., Tantsura, J., Previdi, S., and C. Li, Ed., "Carrying Binding Label/SID in PCE-Based Networks", RFC 9604, DOI 10.17487/RFC9604, August 2024, <https://www.rfc-editor.org/info/rfc9604>.

9.2. Informative References

[I-D.ietf-pce-stateful-interdomain] Dugeon, O., Meuric, J., Lee, Y., and D. Ceccarelli, "PCEP Extension for Stateful Inter-Domain Tunnels", Work in Progress, Internet-Draft, draft-ietf-pce-stateful-interdomain-07, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pce-stateful-interdomain-07>.

[RFC7942] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205, RFC 7942, DOI 10.17487/RFC7942, July 2016, <https://www.rfc-editor.org/info/rfc7942>.

[RFC9826] Dhody, D., Ed., Beeram, V., Hardwick, J., and J. Tantsura, "A YANG Data Model for the Path Computation Element Communication Protocol (PCEP)", RFC 9826, DOI 10.17487/RFC9826, September 2025, <https://www.rfc-editor.org/info/rfc9826>.

Appendix A. Acknowledgements

The authors would like to thank Rajesh Melarcode Venkateswaran for their contributions to this document.

Authors' Addresses

Samuel Sidor
Cisco Systems, Inc.
Eurovea Central 3
Pribinova 10
811 09 Bratislava
Slovakia
Email: ssidor@cisco.com

Zafar Ali
Cisco Systems, Inc.
Email: zali@cisco.com

Cheng Li
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing
100095
China
Email: c.l@huawei.com

Mike Koldychev
Ciena Corporation
385 Terry Fox Dr.
Kanata Ontario K2K 0L1
Canada
Email: mkoldych@proton.me

Andrew Stone
Nokia
Email: andrew.stone@nokia.com