PCE Working Group
Internet-Draft
Intended status: Standards Track
Expires: 28 December 2025

S. Sidor
Cisco Systems, Inc.
P. Maheshwari
Airtel India
A. Stone
Nokia
L. Jalil
Verizon
S. Peng
Huawei Technologies
26 June 2025

Path Computation Element Communication Protocol (PCEP) extensions for Circuit Style Policies
draft-ietf-pce-circuit-style-pcep-extensions-09

Abstract

Segment Routing (SR) enables a node to steer packet flows along a specified path without the need for intermediate per-path states, due to the utilization of source routing. An SR Policy comprises a sequence of segments, which are essentially instructions that define a source-routed policy

This document proposes a set of extensions to the Path Computation Element Communication Protocol (PCEP) for Segment Routing Policies that are designed to satisfy requirements for connection-oriented transport services (Circuit-Style SR policies). They include the ability to control path recomputation and the option to request path with strict hops only and are also applicable for generic SR policy use cases where controlling path recomputation or distinct hop requirements are applicable.

This Internet-Draft will expire on 28 December 2025.

Table of Contents

1. Introduction

Segment Routing (SR) leverages the source routing paradigm, where the sender of a packet defines the path that the packet takes through the network. This is achieved by encoding the path information as a sequence of segments within the packet header. SR can be applied to both MPLS and IPv6 data planes, providing a flexible and scalable method for traffic engineering.

The Path Computation Element (PCE) is a network component, application, or node that is capable of computing a network path or route based on a network graph and applying computational constraints. The PCE Communication Protocol (PCEP) enables communication between a PCE and Path Computation Clients (PCCs), facilitating the computation of optimal paths for traffic flows.

[RFC8664] introduces the concept of Segment Routing Policy (SR Policy), which is a set of candidate paths that can be used to steer traffic through a network. Each candidate path is represented by a list of segments, and the path can be dynamically adjusted based on network conditions and requirements.

In connection-oriented transport services, such as those defined in [I-D.ietf-spring-cs-sr-policy], there is a need for path persistency and per-hop behavior for PCE-computed paths. This ensures that the paths remain stable and predictable, which is crucial for services that require high reliability and performance guarantees.

To support the requirements of connection-oriented transport services, this document specifies extensions to PCEP to enable the use of Circuit Style Policies. These extensions allow for the request of strict paths from the PCE, the encoding of information to disable path recomputation for specific paths, and the clarification of the usage of existing flags within PCEP messages.

The PCEP extensions described in this document are designed to be compatible with any Path Setup Type and are not limited to Circuit Style SR policies, ensuring broad applicability across different network environments and use cases.

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

This document uses the following terms defined in [RFC5440]: ERO, LSPA, PCC, PCE, PCEP, PCEP Peer, and PCEP speaker.

This document uses the following term defined in [RFC3031]: LSP.

3. Overview of Extensions to PCEP

3.1. New Flags in STATEFUL-PCE-CAPABILITY TLV

The STATEFUL-PCE-CAPABILITY TLV is an optional TLV introduced in [RFC8231] in the OPEN object for stateful PCEP peer capability advertisement. This document defines the following new flags in that TLV:

* STRICT-PATH-CAPABILITY - 1 bit (Bit Position 18) - If set to 1, it indicates support for the Strict-Path flag in LSP-EXTENDED-FLAG TLV. See Section 4.1 for details.

* PATH-RECOMPUTATION-CAPABILITY - 1 bit (Bit Position 19) - If set to 1, it indicates support for PATH-RECOMPUTATION TLV. See Section 4.2 for details.

3.2. New Flag in the LSP-EXTENDED-FLAG TLV

The LSP-EXTENDED-FLAG TLV was introduced in Section 3.1 of [RFC9357]. This document specifies new Strict-Path flag in the LSP-EXTENDED-FLAG TLV.

O (Strict-Path) - 1 bit (Bit Position 4): If set to 1, this indicates to the PCE that a path exclusively made of strict hops is required. The strict hop definition is described in Section 4.1

3.3. PATH-RECOMPUTATION TLV

This document defines new TLV for the LSPA Object for encoding information whether path recomputation is allowed for delegated LSP. The TLV is optional. If the TLV is included in LSPA object, the PCE MUST NOT recompute the path in cases specified by flags in the TLV. Only the first instance of this TLV MUST be processed, subsequent instances MUST be ignored.

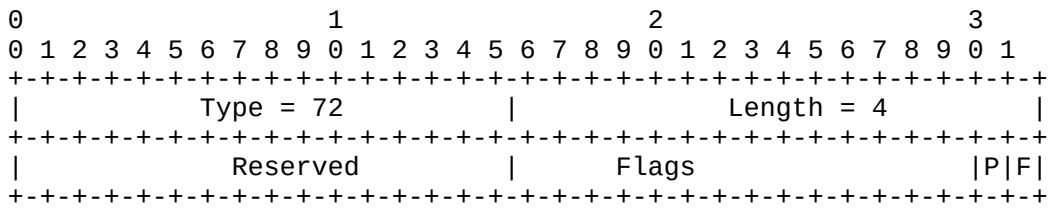

Figure 1: PATH-RECOMPUTATION TLV Format

Type (16 bits): 72.

Length (16 bits): 4.

Reserved (16 bits): This field MUST be set to zero on transmission and MUST be ignored on receipt.

Flags (16 bits): This document defines the following flag bits. The other bits MUST be set to zero by the sender and MUST be ignored by the receiver.

* P (Permanent): If set to 1, the PCE MUST NOT recompute path even if the current path does not satisfy path computation constraints. If this flag is cleared, then the PCE SHOULD recompute the path if the original path is invalidated.

* F (Force): If set to 1, the PCE MUST NOT update the path (exceptions description in Section 4.2). If the flag is cleared, the PCE MAY update the path based on an explicit request from the operator.

4. Operation

4.1. Strict Path Enforcement

PCC MAY set the O flag in LSP-EXTENDED-FLAG TLV in a PCRpt message sent to the PCE to indicate that a path exclusively made of strict hops is required. It MUST NOT be set to 1 if one or both PCEP speakers have not set the STRICT-PATH-CAPABILITY flag to 1 in the STATEFUL-PCE-CAPABILITY TLV. If the PCEP peer received LSP-EXTENDED-FLAG TLV with O flag set, but it does not support that flag, it MUST send PCErr with Error-Type = 2 (Capability not supported).

O flag cleared or LSP-EXTENDED-FLAG TLV not included indicates that a loose path is acceptable.

In PCUpd or PCInitiate messages, PCE MAY set O bit if the strict path is provided.

The flag is applicable only for stateful messages. Existing O flag in RP object MAY be used to indicate similar behavior in PCReq and PCRep messages as described in as described in Section 7.4.1 of [RFC5440].

If the O flag is set to 1 for both stateful and stateless messages for SR paths introduced in [RFC8664], the PCE MUST use only Segment Identifiers (SIDs) that explicitly specify adjacencies for packet forwarding. For example, Adjacency SIDs MAY be used, but Prefix SIDs MUST NOT be used (even if there is only one adjacency).

4.2. Path Recomputation

PCC MAY set flags in PATH-RECOMPUTATION TLV to control path computation behavior on the PCE side. If TLV is not included, then the PCE MAY use local policy to trigger path computation or LSP path update.

If a PCEP speaker does not recognize the PATH-RECOMPUTATION TLV, it MUST ignore the TLV based on Section 7.1 of [RFC5440]. If a PCEP speaker recognizes the TLV but does not support the TLV, it MUST send PCErr with Error-Type = 2 (Capability not supported).

The presence of the TLV blocks path recomputation based on various triggers like topology update, any periodic update, or changed state of other LSPs in the network. The LSP path MAY be modified if forwarded packets will still use the same path. For example, if the same path can be encoded using Adjacency, Binding, Prefix, or other SIDs, then PCE MAY switch between various representations of the same path.

If the P flag is cleared, the PCE MAY recompute if the current path is not considered valid, for example after a topology update resulting in a path not satisfying LSP’s path constraints, but it MUST NOT recompute path if the current path is not optimal.

If the P flag is set, the PCE MUST NOT recompute the path during the LSP lifetime even if the path is invalidated. The only exception is an explicit request from the operator to recompute the path.

If the F flag is cleared, the path update triggered manually by an operator or any northbound interface of PCE MAY be done. If the flag is set then PCE can update the path only to tear down LSP by sending a PCUpd message with empty ERO ERO or to bring it up again with path, which was used before LSP was torn down.

TLV MAY be included in PCInitiate and PCUpd messages to indicate, which triggers will be disabled on the PCE. PCC MUST reflect flag values in PCRpt messages to forward the requirement to other PCEs in the network.

5. Manageability Considerations

All manageability requirements and considerations listed in [RFC5440], [RFC8231] and [RFC8281] apply to PCEP protocol extensions defined in this document. In addition, the 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/disabled as part of the global configuration.

5.2. Information and Data Models

An implementation SHOULD allow an operator to view the PCEP peer capability defined in this document. Section 4.1 and 4.1.1 of [I-D.ietf-pce-pcep-yang] should be extended to include that capability for PCEP peer.

Section 4.2 of [I-D.ietf-pce-pcep-yang] module should be extended to add notification for blocked recomputation that satisfies specified constraints if recomputation is blocked using the PATH-RECOMPUTATION TLV.

5.3. Liveness Detection and Monitoring

Circuit-Style Policy draft [I-D.ietf-spring-cs-sr-policy] is already describing connectivity verification and path validity considerations for Circuit Style Policies.

5.4. Verify Correct Operations

A PCE implementation SHOULD notify the operator in case of blocked recomputation for an LSP that no longer satisfies specified constraints. It SHOULD also allow the operator to view LSPs on the PCE that does not satisfy specified constraints.

5.5. Requirements On Other Protocols

The PCEP extensions defined in this document do not imply any new requirements on other protocols. The overall concept of Circuit Style policies requires interaction with other protocols, but those requirements are already described in [I-D.ietf-spring-cs-sr-policy].

5.6. Impact On Network Operations

The mechanisms defined in [RFC5440], [RFC8231], and [RFC8281] 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".

6.1. Cisco

* Organization: Cisco Systems

* Implementation: IOS-XR PCC and PCE.

* Description: PCEP extensions supported using VENDOR-INFORMATION Object.

* Maturity Level: Production.

* Coverage: Partial.

* Contact: ssidor@cisco.com

7. Security Considerations

The security considerations described in [RFC5440], [RFC8231], [RFC8253],[RFC8281] and [RFC8664] in itself.

Note that this specification introduces the possibility to block path recomputation after various topology events. This creates an additional vulnerability if the security mechanisms of [RFC5440], [RFC8231], and [RFC8281] are not used. If there is no integrity protection on the session, then an attacker could block path updates from PCE potentially resulting in a traffic drop.

As per [RFC8231] it is RECOMMENDED that these PCEP extensions only be activated on authenticated and encrypted sessions across PCEs and PCCs using Transport Layer Security (TLS) [RFC8253], as per the recommendations and best current practices in RFC 9325 [BCP195] (unless explicitly set aside in [RFC8253]).

8. IANA Considerations

IANA maintains the "Path Computation Element Protocol (PCEP) Numbers" registry at <https://www.iana.org/assignments/pcep>.

8.1. STATEFUL-PCE-CAPABILITY

[RFC8231] defines the STATEFUL-PCE-CAPABILITY. IANA is requested to confirm the following allocations within the "STATEFUL-PCE-CAPABILITY TLV Flag Field" registry of the "Path Computation Element Protocol (PCEP) Numbers" registry group:

Bit	Description	Reference
18	STRICT-PATH-CAPABILITY	This document
19	PATH-RECOMPUTATION-CAPABILITY	This document

Table 1

8.2. LSP-EXTENDED-FLAG TLV

[RFC9357] defines the LSP-EXTENDED-FLAG TLV. IANA is requested to confirm the following allocation within the "LSP-EXTENDED-FLAG TLV Flag Field" registry of the "Path Computation Element Protocol (PCEP) Numbers" registry group:

Bit	Description	Reference
4	Strict-Path Flag (O)	This document

Table 2

8.3. PATH-RECOMPUTATION TLV

IANA is requested to confirm the following allocation within the "PCEP TLV Type Indicators" registry of the "Path Computation Element Protocol (PCEP) Numbers" registry group:

TLV Type	TLV Name	Reference
72	PATH-RECOMPUTATION TLV	This document

Table 3

8.4. PATH-RECOMPUTATION TLV Flag Field

IANA has created a new registry named "PATH-RECOMPUTATION TLV Flag Field" within the "Path Computation Element Protocol (PCEP) Numbers" registry group. New values are to be assigned by "IETF Review" [RFC8126]. Each bit should be tracked with the following qualities:

* Bit number (count from 0 as the most significant bit)
* Description
* Reference

The registry contains the following codepoints, with initial values, to be assigned by IANA with the reference set to this document:

Bit	Description	Reference
0-13	Unassigned	
14	Permanent	This document
15	Force	This document

Table 4

9. References

9.1. Normative References

[BCP195] Best Current Practice 195, <https://www.rfc-editor.org/info/bcp195>. At the time of writing, this BCP comprises the following:

Moriarty, K. and S. Farrell, "Deprecating TLS 1.0 and TLS 1.1", BCP 195, RFC 8996, DOI 10.17487/RFC8996, March 2021, <https://www.rfc-editor.org/info/rfc8996>.

Sheffer, Y., Saint-Andre, P., and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 9325, DOI 10.17487/RFC9325, November 2022, <https://www.rfc-editor.org/info/rfc9325>.

[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>.

[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>.

[RFC8664] Sivabalan, S., Filsfils, C., Tantsura, J., Henderickx, W., and J. Hardwick, "Path Computation Element Communication Protocol (PCEP) Extensions for Segment Routing", RFC 8664, DOI 10.17487/RFC8664, December 2019, <https://www.rfc-editor.org/info/rfc8664>.

[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>.

9.2. Informative References

[I-D.ietf-pce-pcep-yang] Dhody, D., Beeram, V. P., Hardwick, J., and J. Tantsura, "A YANG Data Model for Path Computation Element Communications Protocol (PCEP)", Work in Progress, Internet-Draft, draft-ietf-pce-pcep-yang-30, 26 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pce-pcep-yang-30>.

[I-D.ietf-spring-cs-sr-policy] Schmutzer, C., Ali, Z., Maheshwari, P., Rokui, R., and A. Stone, "Circuit Style Segment Routing Policy", Work in Progress, Internet-Draft, draft-ietf-spring-cs-sr-policy-10, 24 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-cs-sr-policy-10>.

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, DOI 10.17487/RFC3031, January 2001, <https://www.rfc-editor.org/info/rfc3031>.

[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>.

Contributors

Daniel Voyer
Bell Canada
Email: daniel.voyer@bell.ca

Reza Rokui
Ciena
Email: rrokui@ciena.com

Tarek Saad
Cisco Systems, Inc.
Email: tsaad.net@gmail.com

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

Ran Chen
ZTE Corporation
Email: chen.ran@zte.com.cn

Quan Xiong
ZTE Corporation
Email: xiong.quan@zte.com.cn

Dhruv Dhody
Huawei
Email: dhruv.ietf@gmail.com

Christian Schmutzer
Cisco Systems, Inc.
Email: cschmutz@cisco.com

Authors' Addresses

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

Praveen Maheshwari
Airtel India
Email: Praveen.Maheshwari@airtel.com

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

Luay Jalil
Verizon
Email: luay.jalil@verizon.com

Shuping Peng
Huawei Technologies
Email: pengshuping@huawei.com