PCE Working Group
Internet-Draft
Intended status: Standards Track
Expires: 7 September 2026

S. Sidor
Cisco Systems, Inc.
P. Maheshwari
Airtel India
A. Stone
Nokia
L. Jalil
Verizon
S. Peng
Huawei Technologies
6 March 2026

Path Computation Element Communication Protocol (PCEP) extensions for Circuit Style Policies
draft-ietf-pce-circuit-style-pcep-extensions-15

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 can consist of one or a set of candidate paths, where each candidate path is represented by a segment list or a set of segment lists, which are essentially instructions that define a source-routed path.

This document specifies 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 modification and the option to request a strict hop-by-hop path, being also applicable for generic SR policy use cases where controlling path modification or deterministic and persistent path requirements are applicable.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction 3
1.1. Requirements Language 4
2. Terminology 4
3. PCEP Extensions 5
3.1. New Flags in STATEFUL-PCE-CAPABILITY TLV 5
3.2. New Flag in the LSP-EXTENDED-FLAG TLV 6
3.3. PATH-MODIFICATION TLV 6
4. Operation 7
4.1. Strict Path Enforcement 7
4.2. Path Modification Control 8
5. Operational Considerations 9
5.1. Control of Function and Policy 9
5.2. Information and Data Models 10
5.3. Liveness Detection and Monitoring 10
5.4. Verify Correct Operations 10
5.5. Requirements On Other Protocols 10
5.6. Impact On Network Operations 10
6. Implementation Status 10
6.1. Cisco 11
7. Security Considerations 11
8. IANA Considerations 12
8.1. STATEFUL-PCE-CAPABILITY 12
8.2. LSP-EXTENDED-FLAG TLV 12
8.3. PATH-MODIFICATION TLV 12
8.4. PATH-MODIFICATION TLV Flag Field 13

8.5. PCEP-Error Object 13
9. References 14
9.1. Normative References 14
9.2. Informative References 15
Contributors 16
Acknowledgements 17
Authors' Addresses 17

1. Introduction

Segment Routing (SR) [RFC8402] leverages source routing, 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.

[RFC9256] introduces the concept of Segment Routing Policy (SR Policy), which is one or a set of candidate paths that can be used to steer traffic through a network. Each candidate path is represented by a segment list or a set of segment lists, and the path can be dynamically adjusted based on network conditions and requirements.

In connection-oriented transport services, such as those described 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 [I-D.ietf-spring-cs-sr-policy]. These extensions allow for the request of strict hop-by-hop paths from the PCE, the encoding of information to disable path modification 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 term defined in [RFC3031]:

* Label Switched Path (LSP)

Note: The base PCEP specification [RFC4655] originally defined the use of the PCE architecture for MPLS and GMPLS networks with LSPs instantiated using the RSVP-TE signaling protocol. Over time, support for additional path setup types such as SRv6 has been introduced [RFC9603]. The term "LSP" is used extensively in PCEP specifications, and in the context of this document, refers to a Candidate Path within an SR Policy, which may be an SRv6 path (still represented using the LSP object as specified in [RFC8231]).

This document uses the following terms defined in [RFC5440]:

* Explicit Route Object (ERO)

* LSP Attributes (LSPA)

* Path Computation Client (PCC)

* Path Computation Element (PCE)

* Path Computation Element Protocol (PCEP)

* PCEP Peer

* PCEP speaker

This document uses the following terms defined in [RFC8402]:

* Segment Routing (SR)

* Segment Identifier (SID)

This document uses the following term defined in [RFC9256]:

* SR Policy

This document defines the following terms:

* Circuit Style (CS) SR Policy: An SR Policy designed to satisfy requirements for connection-oriented transport services. CS SR Policies are characterized by path persistency (where the path should remain stable unless explicitly changed or becomes invalid) and may require strict hop-by-hop path construction. Further details on CS SR Policies are described in [I-D.ietf-spring-cs-sr-policy].

* Path Modification: Refers to the PCE instructing the PCC, via a PCUpd message, to use a path whose set of traversed network hops differs from the current path. A PCUpd message that changes only the attributes or re-encodes the same hop sequence (e.g., alternative SID representation) is not considered a path modification.

3. PCEP Extensions

This section specifies the PCEP extensions that enable a PCC and PCE to support CS SR policies. These extensions build on the base PCEP [RFC5440] and the Stateful PCE extensions [RFC8231]. The mechanisms defined here allow a PCC or PCE to:

* Indicate the requirement for strict hop-by-hop paths,

* Signal path persistency by disabling path modification for specific paths, and

* Identify and control behavior specific to CS SR policies.

Unless explicitly stated, the procedures of existing PCEP messages and objects remain unchanged. The following subsections describe the specific object formats, TLVs, and flag definitions introduced to realize this functionality.

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. Details on the IANA registry are listed in Section 8.1. 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 O bit (Strict-Path) in LSP-EXTENDED-FLAG TLV. See Section 4.1 for details.

* PATH-MODIFICATION-CAPABILITY - 1 bit (Bit Position 19) - If set to 1, it indicates support for PATH-MODIFICATION 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 the new O bit (Strict-Path) in the LSP-EXTENDED-FLAG TLV. Details on the IANA registry are listed in Section 8.2.

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-MODIFICATION TLV

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

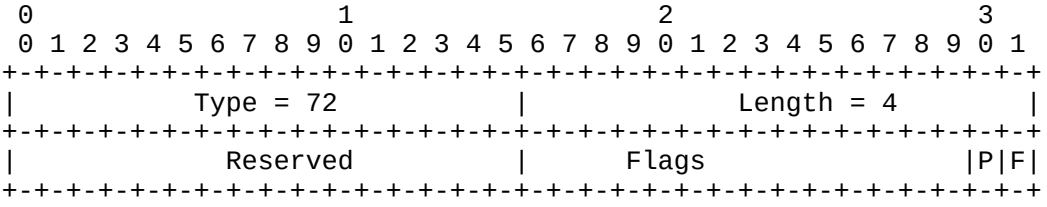

Figure 1: PATH-MODIFICATION TLV Format

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 modify the path even if the current path does not satisfy path computation constraints. If this flag is cleared, then the PCE MAY modify

the path according to local policy if the original path is invalidated. When F is set to 1, the P flag value MUST be ignored.

* F (Force): If set to 1, the PCE MUST NOT modify 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

The STRICT-PATH-CAPABILITY flag in the STATEFUL-PCE-CAPABILITY TLV MUST be set to 1 by both PCEP speakers during the PCEP session establishment to support strict hop-by-hop path enforcement. The O bit (defined in Section 3.2) MUST NOT be set to 1 if the STRICT-PATH-CAPABILITY flag was not set to 1 by both PCEP speakers. If the PCEP peer received LSP-EXTENDED-FLAG TLV with the O bit set to 1, but it does not support that capability, it MUST send PCErr with Error-Type = 2 (Capability not supported). To indicate that a path exclusively made of strict hops is required, the PCC sets the O bit to 1 in the LSP-EXTENDED-FLAG TLV in a PCRpt message sent to the PCE.

The O bit set to 0 or LSP-EXTENDED-FLAG TLV not included indicates that a non-strictly hop-by-hop path is acceptable.

For PCE-initiated LSPs, the PCE MAY set the O bit to 1 in PCInitiate or PCUpd messages. If the PCE sets the O bit to 1, the PCC MUST also set the O bit to 1 in the LSP-EXTENDED-FLAG TLV in the corresponding PCRpt messages. For PCC-initiated LSPs, if the PCC requested a strict path (by setting the O bit to 1 in the PCRpt message), the PCE MUST set the O bit to 1 in the corresponding PCUpd message. Even if the PCC did not request a strict path, the PCE MAY set the O bit to 1 in the PCUpd message if the computed path is a strict hop-by-hop path.

The flag is applicable only for stateful messages. The existing O bit in Request Parameters (RP) object can be used to indicate similar behavior in PCReq and PCRep messages as described in Section 7.4.1 of [RFC5440]. For RSVP-TE, [RFC5440] already defines the strict/loose indication for stateless PCEP; this document extends a corresponding indication to stateful messages via the LSP-EXTENDED-FLAG TLV.

If the O bit is set to 1 (either in the LSP-EXTENDED-FLAG TLV for stateful messages or in the RP object for stateless messages) for SR paths introduced in [RFC8664], the PCE MUST use only Segment Identifiers (SIDs) that explicitly specify adjacencies for packet forwarding. Adjacency SIDs SHOULD be used, but Prefix SIDs MUST NOT be used (even if there is only one adjacency).

4.2. Path Modification Control

A PCC MAY set flags in PATH-MODIFICATION TLV to control path modification behavior on the PCE side. If the PATH-MODIFICATION 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-MODIFICATION 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 LSP path MAY be modified, if the change results in a semantically equivalent path representation (e.g., a different SID list) that preserves the exact sequence of traversed network links. 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.

The PATH-MODIFICATION TLV defines the path modification behavior for an LSP. It is important to note that regardless of the flag settings described below, a PCE can always initiate an update to tear down the LSP (e.g., by sending a PCUpd message with an empty ERO) or to bring it up again with the same path it had before being torn down. The P and F flags specifically restrict the PCE’s ability to initiate a path modification:

TLV present, P=0, F=0:
The PCE MUST NOT modify the path in response to various triggers (E.g. topology updates, periodic reoptimization timers, or changes in the state of other LSPs) if the current path remains valid and meets all constraints (e.g. it is not the most optimal path, but it is still valid and satisfies all constraints including bounds). However, the PCE MAY modify the path if:

* The current path is invalidated (e.g., due to a topology change that makes it non-compliant with LSP constraints).

* An operator explicitly triggers a path modification via an implementation-specific mechanism (e.g., a Command Line Interface (CLI) or a dedicated Application Programming Interface (API) on the PCE).

P flag set (P=1) and F flag cleared (F=0):
The PCE MUST NOT modify the path due to network or optimization triggers, even if the path becomes invalidated or no longer satisfies its constraints. A path modification MAY be initiated if explicitly triggered by an operator.

F flag set (F=1):
The PCE MUST NOT modify the path for any reason, including in response to an explicit operator trigger.

A PCE includes the PATH-MODIFICATION TLV in PCInitiate and PCUpd messages to define which triggers will be disabled for an LSP. When a PCC receives and applies behavior specified by flags in the TLV, it MUST reflect the active flag values in the PATH-MODIFICATION TLV of its PCRpt messages for that LSP. By including this TLV, the PCC ensures that the LSP's path modification policy is consistently communicated to all connected PCEs.

When a PCC receives a PCUpd message with a path modification for an LSP, where such a modification is blocked by flags in the PATH-MODIFICATION TLV (e.g., the F flag is set to 1), it MUST reject the update and maintain the existing path for the LSP.The PCC MUST also send a PCErr message to the PCE with Error-Type=19 ("Invalid Operation") and Error-Value=TBD1 ("Path modification is blocked by constraint").

5. Operational 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 SHOULD allow the capability of supporting PCEP extensions introduced in this document to be enabled/disabled as part of the global configuration.

When path modification is restricted (e.g., when the P flag is set to 1 and F flag is set to 0), the PCE relies on an explicit operator trigger to modify the path if it becomes invalid. Therefore, a PCE implementation SHOULD provide a mechanism to allow an operator to explicitly trigger path modification for a specific LSP.

5.2. Information and Data Models

An implementation SHOULD allow an operator to view the PCEP peer capability defined in this document. A YANG data model specification augmenting the model defined in Sections 4.1 and 4.1.1 of [RFC9826] SHOULD include that capability for the PCEP peer.

A YANG data model specification augmenting the module defined in Section 4.2 of [RFC9826] SHOULD add a notification for blocked path modification that satisfies specified constraints if path modification is blocked using the PATH-MODIFICATION TLV.

5.3. Liveness Detection and Monitoring

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

5.4. Verify Correct Operations

A PCE implementation SHOULD allow the operator to monitor LSPs for which the PCE has determined that the current path no longer satisfies the specified constraints but path modification is blocked by the PATH-MODIFICATION TLV, for example via YANG notifications or the YANG data model described in Section 5.2.

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 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] are applicable to this document.

Note that this specification introduces the possibility to block path modification 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 can only be activated on authenticated and encrypted sessions across PCEs and PCCs belonging to the same administrative authority, using Transport Layer Security (TLS) [RFC8253][I-D.ietf-pce-pceps-tls13] as per the recommendations and best current practices in [RFC9325].

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 (<https://www.iana.org/assignments/pcep/pcep.xhtml#stateful-pce-capability-tlv-flag-field>) of the "Path Computation Element Protocol (PCEP) Numbers" registry group:

Bit	Description	Reference
18	STRICT-PATH-CAPABILITY	This document
19	PATH-MODIFICATION-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 (<https://www.iana.org/assignments/pcep/pcep.xhtml#lsp-extended-flag-tlv-flags>) 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-MODIFICATION TLV

IANA is requested to confirm the following allocation within the "PCEP TLV Type Indicators" registry (<https://www.iana.org/assignments/pcep/pcep.xhtml#pcep-tlv-type-indicators>) of the "Path Computation Element Protocol (PCEP) Numbers" registry group:

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

Table 3

8.4. PATH-MODIFICATION TLV Flag Field

IANA is requested to create a new registry named "PATH-MODIFICATION TLV Flag Field" within the "Path Computation Element Protocol (PCEP) Numbers" registry group. 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

8.5. PCEP-Error Object

IANA is requested to allocate new error types and error values within the "PCEP-ERROR Object Error Types and Values" sub-registry (<https://www.iana.org/assignments/pcep/pcep.xhtml#pcep-error-object>) of the PCEP Numbers registry for the following errors.

Error-Type	Meaning	Error-Value	Reference
19	Invalid Operation	TBD1:Path modification is blocked by constraint	This Document

Table 5

9. References

9.1. Normative References

[I-D.ietf-pce-pceps-tls13]
Dhody, D., Turner, S., and R. Housley, "Updates for PCEPS: TLS Connection Establishment Restrictions", Work in Progress, Internet-Draft, draft-ietf-pce-pceps-tls13-04, 9 January 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-pce-pceps-tls13-04>.

[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>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

[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>.

[RFC9256] Filsfils, C., Talaulikar, K., Ed., Voyer, D., Bogdanov, A., and P. Mattes, "Segment Routing Policy Architecture", RFC 9256, DOI 10.17487/RFC9256, July 2022, <https://www.rfc-editor.org/info/rfc9256>.

[RFC9325] 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>.

[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-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-16, 23 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-cs-sr-policy-16>.

[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>.

[RFC4655] Farrel, A., Vasseur, J.-P., 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>.

[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>.

[RFC9603] Li, C., Ed., Kaladharan, P., Sivabalan, S., Koldychev, M., and Y. Zhu, "Path Computation Element Communication Protocol (PCEP) Extensions for IPv6 Segment Routing", RFC 9603, DOI 10.17487/RFC9603, July 2024, <https://www.rfc-editor.org/info/rfc9603>.

[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>.

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

Acknowledgements

The authors would like to thank Dhruv Dhody for shepherding this document, Ketan Talaulikar for the AD review, and Cheng Li, Luis Contreras, Mach Chen, and Mohamed Boucadair for their review comments.

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