Workgroup: Network Working Group
Internet-Draft:
draft-ietf-pce-local-protection-enforcement-09
Updates: 5440 (if approved)
Published: 8 May 2023
Intended Status: Standards Track
Expires: 9 November 2023
Authors: A. Stone M. Aissaoui S. Sidor
Nokia Nokia Cisco Systems, Inc.
S. Sivabalan
Ciena Coroporation

Local Protection Enforcement in PCEP

Abstract

This document extends the base specification to clarify usage of the local protection desired bit signalled in the Path Computation Element Protocol (PCEP). This document also introduces a new flag for signalling protection strictness in PCEP.

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/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 9 November 2023.

Table of Contents

1. Introduction

The Path Computation Element (PCE) Communication Protocol (PCEP) [RFC5440] enables the communication between a Path Computation Client (PCC) and a PCE, or between two PCEs based on the PCE architecture [RFC4655].

PCEP [RFC5440] utilizes flags, values and concepts previously defined in RSVP-TE Extensions [RFC3209] and Fast Reroute Extensions to RSVP-TE [RFC4090]. One such concept in PCEP is the 'Local Protection Desired' (L flag in the LSPA Object in [RFC5440]), which was originally defined in the SESSION-ATTRIBUTE Object in RFC3209. In RSVP, this flag signals to downstream routers that they may use a local repair mechanism. The headend router calculating the path does not know whether a downstream router will or will not protect a hop during its calculation. Therefore, a local protection desired does not require the transit router to satisfy protection in order to establish the RSVP signalled path. This flag is signalled in PCEP as an attribute of the LSP via the LSP Attributes object.

PCEP Extensions for Segment Routing ([RFC8664]) extends support in PCEP for Segment Routed paths. The path list is encoded with Segment Identifiers, each of which offer local protection. The PCE may discover the protection eligibility for a Segment Identifier (SID)

via BGP-LS [RFC9085] and take the protection into consideration as a path constraint.

It is desirable for an operator to be able to define the enforcement, or strictness of the protection requirement.

This document updates [RFC5440] by further describing the behaviour with the Local Protection Desired Flag (L flag) and extends on it with the introduction of the Enforcement Flag (E flag).

The document contains reference notes for Segment Routing, however the content described is path setup type and data plane technology agnostic.

2. 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.

3. Terminology

This document uses the following terminology:

PROTECTION MANDATORY: The Path MUST have protection eligibility on all links.

UNPROTECTED MANDATORY: The Path MUST NOT have protection eligibility on all links.

PROTECTION PREFERRED: The Path SHOULD have protection eligibility on all links but MAY contain links which do not have protection eligibility.

UNPROTECTED PREFERRED: The Path SHOULD NOT have protection eligibility on all links but MAY contain links which have protection eligibility.

PCC: Path Computation Client. Any client application requesting a path computation to be performed by a Path Computation Element.

PCE: Path Computation Element. An entity (component, application, or network node) that is capable of computing a network path or route based on a network graph and applying computational constraints.

PCEP: Path Computation Element Protocol.

LSPA: LSP Attributes Object in PCEP, defined in RFC5440

4. Motivation

4.1. Implementation differences

As defined in [RFC5440] the mechanism to signal protection enforcement in PCEP is the previously mentioned L flag defined in the LSPA Object. The name of the flag uses the term "Desired", which by definition means "strongly wished for or intended" and the use case originated from the RSVP. For RSVP signalled paths, local protection is not within control of the PCE. However, [RFC5440] does state "When set, this means that the computed path must include links protected with Fast Reroute as defined in [RFC4090]." Implementations of [RFC5440] have either interpreted the L flag as PROTECTION MANDATORY or PROTECTION PREFERRED, leading to operational differences.

4.2. SLA Enforcement

The boolean bit L flag is unable to distinguish between the different options of PROTECTION MANDATORY, UNPROTECTED MANDATORY, PROTECTION PREFERRED and UNPROTECTED PREFERRED. Selecting one of the options is typically dependent on the service level agreement the operator wishes to impose on the LSP. A network may be providing transit to multiple service agreement definitions against the same base topology network, whose behavior could vary, such as wanting local protection to be invoked on some LSPs and not wanting local protection on others. When enforcement is used, the resulting shortest path calculation is impacted.

For example, PROTECTION MANDATORY is for use cases where an operator may need the LSP to follow a path which has local protection provided along the full path, ensuring that if there is a failure anywhere along the path that traffic will be fast re-routed at the point.

For example, UNPROTECTED MANDATORY is when an operator may intentionally prefer an LSP to not be locally protected, and thus would rather local failures cause the LSP to go down. An example scenario is one where an LSP is protected with path protection via a secondary diverse LSP. Each LSP is traffic engineered to follow specific traffic engineered criteria computed by the PCE to satisfy SLA. Upon a failure, if local protection is invoked on the active LSP traffic, the traffic may temporarily traverse links which violate the TE requirements and could negatively impact the resources being traversed (e.g., insufficient bandwidth). In addition, depending on the network topological scenario, it may be not feasible for the PCE to reroute the LSP while respecting the TE requirements which include path diversity, resulting in the LSP being torn down and switched to the protected path anyways. In such scenarios its desirable for the LSP to be simply torn down immediately and not re-routed through

local protection, so that traffic may be forwarded through an already established traffic-engineered secondary path.

Both UNPROTECTED PREFERRED and PROTECTED PREFERRED options provide a relaxation of the protection constraint. These options can be used when an operator does not require protection enforcement. Regardless of the option selected, the protection status of a resource does not influence whether the link must be pruned during a path calculation. Furthermore, the selection of either option indicates a priority selection to PCE when there is an option to choose a protected or unprotected instruction associated with a resource, ensuring consistent PCE behavior across different implementations.

When used with Segment Routing, an adjacency may have both a protected SID and an unprotected SID. If the UNPROTECTED PREFERRED option is selected, PCE chooses the unprotected SID. Alternatively, if the PROTECTED PREFERRED option is selected, PCE chooses the protected SID

5. Protection Enforcement Flag (E flag)

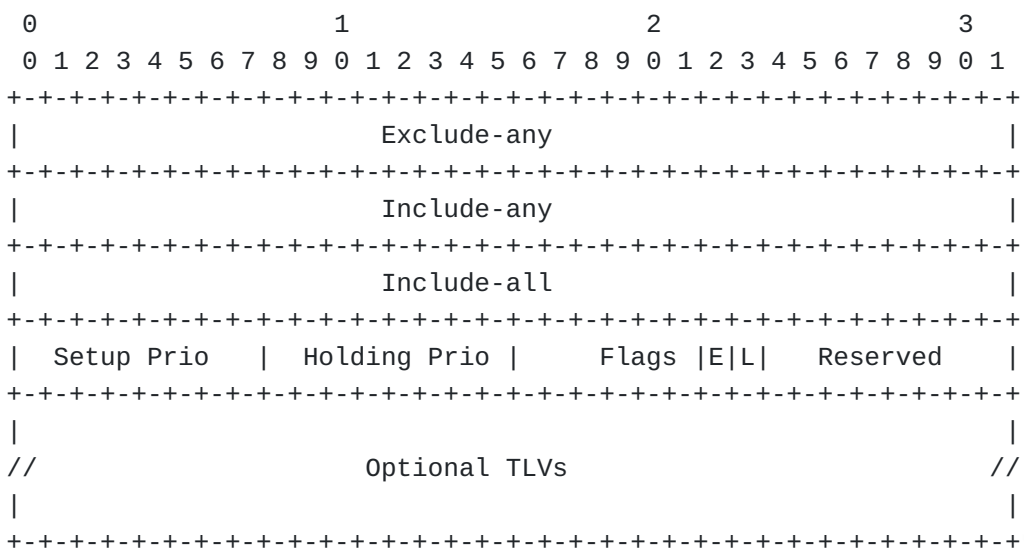
Section 7.11 in Path Computation Element Protocol [RFC5440] describes the encoding of the Local Protection Desired (L flag). A Protection Enforcement flag "E" is specified below, extending the L flag.

[RFC Editor Note: The text below assumes the E bit remains the early allocation value 6. Please adjust if this changes and remove this note before publication.]

Codespace of the Flag field (LSPA Object)

Bit	Description	Reference
7	Local Protection Desired	RFC5440
6	Local Protection Enforcement	This document

The format of the LSPA Object as defined in [RFC5440] is:



Flags (8 bits)

- L Flag: As defined in [RFC5440] and further updated by this document. When set to 1, protection is desired. When set to 0, protection is not desired. The enforcement of the protection is identified via the E flag.

- E Flag (Protection Enforcement): This flag controls the strictness in which the PCE must apply the L flag. When set to 1, the value of the L flag MUST be respected during resource selection by the PCE. When E flag is set to 0, the value of the L flag SHOULD be respected as selection criteria; however, the PCE is permitted to relax or ignore the L flag when computing a path. The statements below indicate preference when E flag is set to 0 in combination with the L flag value.

When both the L flag and E flag are set to 1, then the PCE MUST consider the protection eligibility as a PROTECTION MANDATORY constraint.

When the L flag is set to 1 and the E flag is set to 0, then the PCE MUST consider the protection eligibility as a PROTECTION PREFERRED constraint.

When both L flag and E flag are set to 0, then the PCE SHOULD consider the protection eligibility as an UNPROTECTED PREFERRED constraint but MAY consider protection eligibility as an UNPROTECTED MANDATORY constraint.

When L flag is set to 0 and E flag is set to 1, then the PCE MUST consider the protection eligibility as an UNPROTECTED MANDATORY constraint.

If a PCE is unable to infer protection status of a resource, PCE MAY use local policy to define protected status assumptions. When computing a Segment Routed path, It is RECOMMENDED that a PCE assume a Node SID is protected. It is also RECOMMENDED that a PCE assume an Adjacency SID is protected if the backup flag advertised with the Adjacency SID is set.

5.1. Backwards Compatibility

Considerations in the message passing between the PCC and the PCE for the E flag bit which are not supported by the entity are outlined in this section, with requirements for the PCE and the PCC implementing this document described at the end.

For a PCC or PCE which does not yet support this document, the E flag is ignored and set to zero in PCRpt and/or PCUpd as per [RFC5440] for PCC-initiated or as per [RFC8281] for PCE-initiated LSPs. It is important to note that [RFC8231] and [RFC8281] permit the LSP Attribute Object to be included in PCUpd messages for PCC-initiated and PCE-initiated LSPs.

For PCC-initiated LSPs, PCUpd E flag (and L flag) is an echo from the previous PCRpt however the bit value is ignored on the PCE from the previous PCRpt, therefore the E flag value set in the PCUpd is zero. A PCE which does not support this document sends PCUpd messages with the E flag set to 0 for PCC-initated LSPs even if set to 1 in the prior PCReq or PCRpt.

A PCC which does not support this document sends PCRpt messages with the E flag set to 0 for PCE-initiated LSPs even if set to 1 in the prior PCInitiate or PCUpd.

For a PCC which does support this document, it MAY set the E flag to 1 depending on local configuration. If communicating with a PCE which does not yet support this document, the PCE follows the behaviour specified in [RFC5440] and will ignore the E flag. Thus, it may compute a path which may not respect the enforcement constraint.

For PCC-initiated LSPs, the PCC SHOULD ignore the E flag value received from the PCE in a PCUpd message as it may be communicating with a PCE which does not support this document.

For PCE-initiated LSPs, the PCC MAY process the E flag value received from the PCE in a PCUpd message. The PCE SHOULD ignore the E flag value received from the PCC in a PCRpt message as it may be communicating with a PCC which does not support 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 catalogue 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. Nokia Implementation

*Organization: Nokia

*Implementation: NSP PCE and SROS PCC.

*Description: Implementation for calculation and conveying intention described in this document

*Maturity Level: Demo

*Coverage: Full

*Contact: andrew.stone@nokia.com

6.2. Cisco Implementation

*Organization: Cisco Systems, Inc.

*Implementation: IOS-XR PCE and PCC.

*Description: Implementation for calculation and conveying intention described in this document

*Maturity Level: Demo

*Coverage: Full

*Contact: ssidor@cisco.com

7. Security Considerations

This document clarifies the behaviour of an existing flag and introduces a new flag to provide further control of that existing behaviour. The introduction of this new flag and behaviour clarification does not create any new sensitive information. No additional security measure is required.

Securing the PCEP session using Transport Layer Security (TLS) [RFC8253], as per the recommendations and best current practices in [RFC7525] is RECOMMENDED.

8. IANA Considerations

[RFC Editor Note: The text below assumes the E bit remains the early allocation value 6. Please adjust if this changes and remove this note before publication.]

This document defines a new bit value in the sub-registry "LSPA Object Flag Field" in the "Path Computation Element Protocol (PCEP) Numbers" registry. IANA has made the following codepoint allocation.

Bit	Name	Reference
6	Protection Enforcement	This document

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>.

[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>.

[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>.

[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>.

[RFC4090] Pan, P., Ed., Swallow, G., Ed., and A. Atlas, Ed., "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", RFC 4090, DOI 10.17487/RFC4090, May 2005, <https://www.rfc-editor.org/info/rfc4090>.

[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>.

[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>.

[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>.

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

9.2. Informative References

[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>.

[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>.

[RFC9085] Previdi, S., Talaulikar, K., Ed., Filsfils, C., Gredler, H., and M. Chen, "Border Gateway Protocol - Link State (BGP-LS) Extensions for Segment Routing", RFC 9085, DOI 10.17487/RFC9085, August 2021, <https://www.rfc-editor.org/info/rfc9085>.

Acknowledgements

Thanks to Dhruv Dhody and Mike Koldychev for reviewing and providing very valuable feedback and discussions on this document.

Thanks to Julien Meuric for shepherding this document.

Authors' Addresses

Andrew Stone
Nokia
600 March Road
Kanata Ontario K2K 2T6
Canada

Email: andrew.stone@nokia.com

Mustapha Aissaoui
Nokia
600 March Road
Kanata Ontario K2K 2T6
Canada

Email: mustapha.aissaoui@nokia.com

Samuel Sidor
Cisco Systems, Inc.
Eurovea Central 3.
Pribinova 10
811 09 Bratislava
Slovakia

Email: ssidor@cisco.com

Siva Sivabalan

Ciena Coroporation
385 Terry Fox Drive
Kanata Ontario K2K 0L1
Canada

Email: ssivabal@ciena.com