PCE Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 1, 2020

H. Ananthakrishnan
Netflix
S. Sivabalan
Cisco
C. Barth
Juniper Networks
I. Minei
Google, Inc
M. Negi
Huawei Technologies

July 31, 2019

PCEP Extensions for Associating Working and Protection LSPs with Stateful PCE
draft-ietf-pce-stateful-path-protection-08

Abstract

An active stateful Path Computation Element (PCE) is capable of computing as well as controlling via Path Computation Element Communication Protocol (PCEP) Multiprotocol Label Switching Traffic Engineering Label Switched Paths (MPLS LSP). Furthermore, it is also possible for an active stateful PCE to create, maintain, and delete LSPs. This document describes PCEP extension to associate two or more LSPs to provide end-to-end path protection.

Table of Contents

1. Introduction

[RFC5440] describes PCEP for communication between a Path Computation Client (PCC) and a PCE or between a pair of PCEs as per [RFC4655]. A PCE computes paths for MPLS-TE LSPs based on various constraints and optimization criteria.

Stateful PCE [RFC8231] specifies a set of extensions to PCEP to enable stateful control of paths such as MPLS TE LSPs between and across PCEP sessions in compliance with [RFC4657]. It includes mechanisms to effect LSP state synchronization between PCCs and PCEs, delegation of control of LSPs to PCEs, and PCE control of timing and sequence of path computations within and across PCEP sessions and focuses on a model where LSPs are configured on the PCC and control over them is delegated to the PCE. Furthermore, a mechanism to dynamically instantiate LSPs on a PCC based on the requests from a stateful PCE or a controller using stateful PCE, is specified in [RFC8281].

Path protection [RFC4427] refers to a paradigm in which the working LSP is protected by one or more protection LSP(s). When the working LSP fails, protection LSP(s) is/are activated. When the working LSPs are computed and controlled by the PCE, there is benefit in a mode of operation where protection LSPs are as well. [RFC8051] describes applicability of path protection in PCE deployments.

This document specifies a stateful PCEP extension to associate two or more LSPs for the purpose of setting up path protection. The proposed extension covers the following scenarios:

- A PCC initiates a protection LSP and retains the control of the LSP. The PCC computes the path itself or makes a request for path computation to a PCE. After the path setup, it reports the information and state of the path to the PCE. This includes the association group identifying the working and protection LSPs. This is the passive stateful mode [RFC8051].

- A PCC initiates a protection LSP and delegates the control of the LSP to a stateful PCE. During delegation the association group identifying the working and protection LSPs is included. The PCE computes the path for the protection LSP and update the PCC with the information about the path as long as it controls the LSP. This is the active stateful mode [RFC8051].

- A protection LSP could be initiated by a stateful PCE, which retains the control of the LSP. The PCE is responsible for computing the path of the LSP and updating to the PCC with the

information about the path. This is the PCE-Initiated mode [RFC8281].

Note that protection LSP can be established (signaled) prior to the failure (in which case the LSP is said to be in standby mode [RFC4427] or a Primary LSP [RFC4872]) or post failure of the corresponding working LSP according to the operator choice/policy (known as secondary LSP [RFC4872]).

[I-D.ietf-pce-association-group] introduces a generic mechanism to create a grouping of LSPs which can then be used to define associations between a set of LSPs that is equally applicable to stateful PCE (active and passive modes) and stateless PCE.

This document specifies a PCEP extension to associate one working LSP with one or more protection LSPs using the generic association mechanism.

This document describes a PCEP extension to associate protection LSPs by creating Path Protection Association Group (PPAG) and encoding this association in PCEP messages for stateful PCEP sessions.

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 terminologies are used in this document:

ERO: Explicit Route Object.

LSP: Label Switched Path.

PCC: Path Computation Client.

PCE: Path Computation Element

PCEP: Path Computation Element Communication Protocol.

PPAG: Path Protection Association Group.

TLV: Type, Length, and Value.

3. PCEP Extensions

3.1. Path Protection Association Type

LSPs are not associated by listing the other LSPs with which they interact, but rather by making them belong to an association group referred to as "Path Protection Association Group" (PPAG) in this document. All LSPs join a PPAG individually. PPAG is based on the generic Association object used to associate two or more LSPs specified in [I-D.ietf-pce-association-group]. A member of a PPAG can take the role of working or protection LSP. This document defines a new Association type called "Path Protection Association Type" of value TBD1. A PPAG can have one working LSP and/or one or more protection LSPs. The source, destination and Tunnel ID (as carried in LSP-IDENTIFIERS TLV [RFC8231], with description as per [RFC3209]) of all LSPs within a PPAG MUST be the same. As per [RFC3209], TE tunnel is used to associate a set of LSPs during reroute or to spread a traffic trunk over multiple paths.

The format of the Association object used for PPAG is specified in [I-D.ietf-pce-association-group].

This document defines a new Association type, the "Path Protection Association Type", value will be assigned by IANA (TBD1).

[I-D.ietf-pce-association-group] specifies the mechanism for the capability advertisement of the Association types supported by a PCEP speaker by defining a ASSOC-Type-List TLV to be carried within an OPEN object. This capability exchange for the Association type described in this document (i.e. Path Protection Association Type) MAY be done before using the policy association, i.e., the PCEP speaker MAY include the Path Protection Association Type (TBD1) in the ASSOC-Type-List TLV before using the PPAG in the PCEP messages.

This Association type is dynamic in nature and created by the PCC or PCE for the LSPs belonging to the same TE tunnel (as described in [RFC3209]) originating at the same head node and terminating at the same destination. These associations are conveyed via PCEP messages to the PCEP peer. As per [I-D.ietf-pce-association-group], the association source is set to the local PCEP speaker address that created the association, unless local policy dictates otherwise. Operator-configured Association Range MUST NOT be set for this Association type and MUST be ignored.

3.2. Path Protection Association TLV

The Path Protection Association TLV is an optional TLV for use with the Path Protection Association Type. The Path Protection Association TLV MUST NOT be present more than once. If it appears more than once, only the first occurrence is processed and any others MUST be ignored.

The Path Protection Association TLV follows the PCEP TLV format of [RFC5440].

The type (16 bits) of the TLV is to be assigned by IANA. The length field (16 bit) has a fixed value of 4.

The value comprises of a single field, the Path Protection Association Flags (32 bits), where each bit represents a flag option.

The format of the Path Protection Association TLV (Figure 1) is as follows:

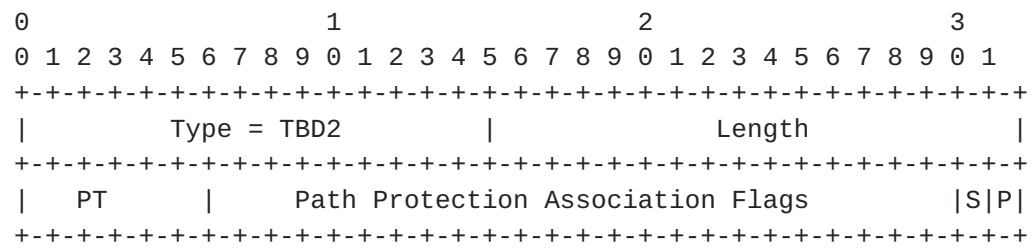

Figure 1: Path Protection Association TLV format

Path Protection Association Flags (32 bits) - The following flags are currently defined -

Protecting (P): 1 bit - This bit is as defined in Section 14.1 of [RFC4872] to indicate if the LSP is working or protection LSP.

Secondary (S): 1 bit - This bit is as defined in Section 14.1 of [RFC4872] to indicate if the LSP is primary or secondary LSP. The S flag is ignored if the P flag is not set.

Protection Type (PT): 6 bits - This field is as defined in Section 14.1 of [RFC4872] to indicate the LSP protection type in use.

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

If the TLV is missing, it is considered that the LSP is the working LSP (i.e. as if P bit is unset).

4. Operation

An LSP is associated with other LSPs with which they interact by adding them to a common association group via the ASSOCIATION object. All procedures and error-handling for the ASSOCIATION object is as per [I-D.ietf-pce-association-group].

4.1. State Synchronization

During state synchronization, a PCC reports all the existing LSP states as described in [RFC8231]. The association group membership pertaining to an LSP is also reported as per [I-D.ietf-pce-association-group]. This includes PPAGs.

4.2. PCC-Initiated LSPs

A PCC can associate a set of LSPs under its control for path protection purpose. Similarly, the PCC can remove one or more LSPs under its control from the corresponding PPAG. In both cases, the PCC reports the change in association to PCE(s) via Path Computation Report (PCRpt) message. A PCC can also delegate the working and protection LSPs to an active stateful PCE, where the PCE would control the LSPs. The stateful PCE could update the paths and attributes of the LSPs in the association group via Path Computation Update (PCUpd) message. A PCE could also update the association to the PCC via PCUpd message. These procedures are described in [I-D.ietf-pce-association-group].

It is expected that both working and protection LSP are delegated together (and to the same PCE) to avoid any race conditions. Refer to [I-D.litkowski-pce-state-sync] for the problem description.

4.3. PCE-Initiated LSPs

A PCE can create/update working and protection LSPs independently. As specified in [I-D.ietf-pce-association-group], Association Groups can be created by both the PCE and the PCC. Further, a PCE can remove a protection LSP from a PPAG as specified in [I-D.ietf-pce-association-group]. The PCE uses PCUpd or Path Computation Initiate (PCInitiate) messages to communicate the association information to the PCC.

4.4. Session Termination

As per [I-D.ietf-pce-association-group] the association information is cleared along with the LSP state information. When a PCEP session is terminated, after expiry of State Timeout Interval at the PCC, the LSP state associated with that PCEP session is reverted to operator-defined default parameters or behaviors as per [RFC8231]. The same procedure is also followed for the association information. On session termination at the PCE, when the LSP state reported by PCC is cleared, the association information is also cleared as per [I-D.ietf-pce-association-group]. Where there are no LSPs in a association group, the association is considered to be deleted.

4.5. Error Handling

As per the processing rules specified in section 5.4 of [I-D.ietf-pce-association-group], if a PCEP speaker does not support this Path Protection Association Type, it would return a PCErr message with Error-Type 26 (Early allocation by IANA) "Association Error" and Error-Value 1 "Association type is not supported".

All LSPs (working or protection) within a PPAG MUST belong to the same TE Tunnel (as described in [RFC3209]) and have the same source and destination. If a PCEP speaker attempts to add an LSP to a PPAG and the Tunnel ID (as carried in LSP-IDENTIFIERS TLV [RFC8231], with description as per [RFC3209]) or source or destination of the LSP is different from the LSP(s) in the PPAG, the PCC MUST send PCErr with Error-Type 26 (Early allocation by IANA) (Association Error) [I-D.ietf-pce-association-group] and Error-Value TBD3 (Tunnel ID or End points mismatch for Path Protection Association). In case of Path Protection, LSP-IDENTIFIERS TLV SHOULD be included for all LSPs (including Segment Routing (SR) [I-D.ietf-pce-segment-routing]).

When the PCEP peer does not support the protection type set in PPAG, the PCEP peer MUST send PCErr with Error-Type 26 (Early allocation by IANA) (Association Error) [I-D.ietf-pce-association-group] and Error-Value TBD5 (Protection type is not supported).

A given LSP MAY belong to more than one PPAG. If there is a conflict between any of the two PPAGs, the PCEP peer MUST send PCErr with Error-Type 26 (Early allocation by IANA) (Association Error) [I-D.ietf-pce-association-group] and Error-Value 6 (Association information mismatch) as per [I-D.ietf-pce-association-group].

When the protection type is set to 1+1 or 1:N with N=1, there MUST be only one working LSP and one protection LSP within a PPAG. If a PCEP speaker attempts to add another working/protection LSP, the PCEP peer MUST send PCErr with Error-Type 26 (Early allocation by IANA)

(Association Error) [I-D.ietf-pce-association-group] and Error-Value TBD4 (Attempt to add another working/protection LSP for Path Protection Association). When the protection type is set to 1:N with N>1, there MUST be only one working LSP and number of protection LSPs MUST NOT be more than N within a PPAG. If a PCEP speaker attempts to add another working/protection LSP, the PCEP peer MUST send PCErr with Error-Type 26 (Early allocation by IANA) (Association Error) [I-D.ietf-pce-association-group] and Error-Value TBD4 (Attempt to add another working/protection LSP for Path Protection Association).

All processing as per [I-D.ietf-pce-association-group] continues to apply.

5. Other Considerations

The working and protection LSPs are typically resource disjoint (e.g., node, SRLG disjoint). This ensures that a single failure will not affect both the working and protection LSPs. The disjoint requirement for a group of LSPs is handled via another Association type called "Disjointness Association", as described in [I-D.ietf-pce-association-diversity]. The diversity requirements for the protection LSP are also handled by including both ASSOCIATION objects identifying both the protection association group and the disjoint association group for the group of LSPs.

[RFC4872] introduces the concept and mechanisms to support the association of one LSP to another LSP across different RSVP - Traffic Engineering (RSVP-TE) sessions using ASSOCIATION and PROTECTION object. The information in the PPAG TLV in PCEP as received from the PCE, is used to trigger the signalling of working LSP and protection LSP, with the Path Protection Association Flags mapped to the corresponding fields in the PROTECTION Object in RSVP-TE.

6. IANA Considerations

6.1. Association Type

This document defines a new Association type, originally defined in [I-D.ietf-pce-association-group], for path protection. IANA is requested to make the assignment of a new value for the sub-registry "ASSOCIATION Type Field" (request to be created in [I-D.ietf-pce-association-group]), as follows:

Association type Value	Association Name	Reference
TBD1	Path Protection Association	This document

6.2. PPAG TLV

This document defines a new TLV for carrying additional information of LSPs within a path protection association group. IANA is requested to make the assignment of a new value for the existing "PCEP TLV Type Indicators" registry as follows:

TLV Type Value	TLV Name	Reference
TBD2	Path Protection Association Group TLV	This document

This document requests that a new sub-registry, named "Path protection Association Group TLV Flag Field", is created within the "Path Computation Element Protocol (PCEP) Numbers" registry to manage the Flag field in the Path Protection Association Group TLV. New values are to be assigned by Standards Action [RFC8126]. Each bit should be tracked with the following qualities:

- Bit number (count from 0 as the most significant bit)
- Name flag
- Reference

Bit Number	Name	Reference
31	P - PROTECTION-LSP	This document
30	S - SECONDARY-LSP	This document
0-5	Protection Type Flags	This document

Table 1: PPAG TLV

6.3. PCEP Errors

This document defines new Error-Values related to path protection association for Error-type 26 "Association Error" defined in [I-D.ietf-pce-association-group]. IANA is requested to allocate new error values within the "PCEP-ERROR Object Error Types and Values" sub-registry of the PCEP Numbers registry, as follows:

Error-value	Meaning	Reference
TBD3	Tunnel ID or End points mismatch for Path Protection Association	This document
TBD4	Attempt to add another working/protection LSP for Path Protection Association	This document
TBD5	Protection type is not supported	This document

7. Security Considerations

The security considerations described in [RFC8231], [RFC8281], and [RFC5440] apply to the extensions described in this document as well. Additional considerations related to associations where a malicious PCEP speaker could be spoofed and could be used as an attack vector by creating associations is described in [I-D.ietf-pce-association-group]. Thus securing the PCEP session using Transport Layer Security (TLS) [RFC8253], as per the recommendations and best current practices in [RFC7525], is RECOMMENDED.

8. Manageability Considerations

8.1. Control of Function and Policy

Mechanisms defined in this document do not imply any control or policy requirements in addition to those already listed in [RFC5440], [RFC8231], and [RFC8281].

8.2. Information and Data Models

[RFC7420] describes the PCEP MIB, there are no new MIB Objects for this document.

The PCEP YANG module [I-D.ietf-pce-pcep-yang] supports associations.

8.3. 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], [RFC8231], and [RFC8281].

8.4. Verify Correct Operations

Mechanisms defined in this document do not imply any new operation verification requirements in addition to those already listed in [RFC5440], [RFC8231], and [RFC8281].

8.5. Requirements On Other Protocols

Mechanisms defined in this document do not imply any new requirements on other protocols.

8.6. 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], [RFC8231], and [RFC8281].

9. Acknowledgments

We would like to thank Jeff Tantsura, Xian Zhang and Greg Mirsky for their contributions to this document.

Thanks to Ines Robles for the RTGDIR review.

10. References

10.1. 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>.

[RFC4872] Lang, J., Ed., Rekhter, Y., Ed., and D. Papadimitriou, Ed., "RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery", RFC 4872, DOI 10.17487/RFC4872, May 2007, <https://www.rfc-editor.org/info/rfc4872>.

[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>.

[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>.

[I-D.ietf-pce-association-group] Minei, I., Crabbe, E., Sivabalan, S., Ananthakrishnan, H., Dhody, D., and Y. Tanaka, "Path Computation Element Communication Protocol (PCEP) Extensions for Establishing Relationships Between Sets of Label Switched Paths (LSPs)", draft-ietf-pce-association-group-10 (work in progress), August 2019.

10.2. Informative References

[RFC4427] Mannie, E., Ed. and D. Papadimitriou, Ed., "Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4427, DOI 10.17487/RFC4427, March 2006, <https://www.rfc-editor.org/info/rfc4427>.

[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>.

[RFC4657] Ash, J., Ed. and J. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol Generic Requirements", RFC 4657, DOI 10.17487/RFC4657, September 2006, <https://www.rfc-editor.org/info/rfc4657>.

[RFC7420] Koushik, A., Stephan, E., Zhao, Q., King, D., and J. Hardwick, "Path Computation Element Communication Protocol (PCEP) Management Information Base (MIB) Module", RFC 7420, DOI 10.17487/RFC7420, December 2014, <https://www.rfc-editor.org/info/rfc7420>.

[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>.

[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>.

[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>.

[I-D.ietf-pce-pcep-yang] Dhody, D., Hardwick, J., Beeram, V., and J. Tantsura, "A YANG Data Model for Path Computation Element Communications Protocol (PCEP)", draft-ietf-pce-pcep-yang-12 (work in progress), July 2019.

[I-D.ietf-pce-association-diversity] Litkowski, S., Sivabalan, S., Barth, C., and M. Negi, "Path Computation Element Communication Protocol (PCEP) Extension for LSP Diversity Constraint Signaling", draft-ietf-pce-association-diversity-08 (work in progress), July 2019.

[I-D.ietf-pce-segment-routing]
Sivabalan, S., Filsfils, C., Tantsura, J., Henderickx, W., and J. Hardwick, "PCEP Extensions for Segment Routing", draft-ietf-pce-segment-routing-16 (work in progress), March 2019.

[I-D.litkowski-pce-state-sync]
Litkowski, S., Sivabalan, S., Li, C., and H. Zheng, "Inter Stateful Path Computation Element (PCE) Communication Procedures.", draft-litkowski-pce-state-sync-06 (work in progress), July 2019.

Appendix A. Contributor Addresses

Dhruv Dhody
Huawei Technologies
Divyashree Techno Park, Whitefield
Bangalore, Karnataka 560066
India

EMail: dhruv.ietf@gmail.com

Raveendra Torvi
Juniper Networks
1194 N Mathilda Ave,
Sunnyvale, CA, 94086
USA

EMail: rtorvi@juniper.net

Edward Crabbe
Individual Contributor

EMail: edward.crabbe@gmail.com

Authors' Addresses

Hariharan Ananthakrishnan
Netflix
USA

Email: hari@netflix.com

Siva Sivabalan
Cisco
2000 Innovation Drive
Kananta, Ontaria K2K 3E8
Canada

Email: msiva@cisco.com

Colby Barth
Juniper Networks
1194 N Mathilda Ave,
Sunnyvale, CA, 94086
USA

Email: cbarth@juniper.net

Ina Minei
Google, Inc
1600 Amphitheatre Parkway
Mountain View, CA, 94043
USA

Email: inaminei@google.com

Mahendra Singh Negi
Huawei Technologies
Divyashree Techno Park, Whitefield
Bangalore, Karnataka 560066
India

Email: mahend.ietf@gmail.com