PCE Extensions for Associating Working and Protection LSPs with Stateful PCE
draft-ietf-pce-stateful-path-protection-11

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 (MPLS-TE) Label Switched Paths (LSPs). Furthermore, it is also possible for an active stateful PCE to create, maintain, and delete LSPs. This document defines the PCEP extension to associate two or more LSPs to provide end-to-end path protection.

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 March 28, 2020.
1. Introduction

[RFC5440] describes Path Computation Element Communication Protocol 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 Label Switched Paths (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 affect 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. The focus is on a model where LSPs are configured on the PCC and control over them is delegated to the Stateful PCE. Furthermore, [RFC8281] specifies a mechanism to dynamically instantiate LSPs on a PCC based on the requests from a stateful PCE or a controller using stateful PCE.

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 also computed and controlled by the same PCE. [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 extension defined in this document 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 updates 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 a protection LSP can be established (signaled) before the failure (in which case the LSP is said to be in standby mode [RFC4427] or a Primary LSP [RFC4872]) or after failure of the corresponding working LSP (known as a secondary LSP [RFC4872]). Whether to establish it before or after failure is according to operator choice or policy.

[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. The mechanism 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
PPAG: Path Protection Association Group.
TLV: Type, Length, and Value.

3. PCEP Extensions

3.1. Path Protection Association Type

As per [I-D.ietf-pce-association-group], LSPs are not associated by listing the other LSPs with which they interact, but rather by making them belong to an association groups. All LSPs join an association group individually. The generic ASSOCIATION object is used to associate two or more LSPs as specified in [I-D.ietf-pce-association-group]. This document defines a new Association type called "Path Protection Association Type" of value TBD1 and a "Path Protection Association Group" (PPAG). A member LSP of a PPAG can take the role of working or protection LSP. A PPAG can have one working LSP and/or one or more protection LSPs. The source, destination, Tunnel ID (as carried in LSP-IDENTIFIERS TLV [RFC8231], with description as per [RFC3209]), and Protection Type (PT) (in Path Protection Association TLV) 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].

[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 this 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 in the ASSOCIATION Object 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 TBD2. 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:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Type = TBD2         |              Length = 4         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   PT      |               Unassigned Flags                |S|P|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 a working (0) or protection (1) LSP.

- Secondary (S): 1 bit - This bit is as defined in Section 14.1 of [RFC4872] to indicate if the LSP is a primary (0) or secondary (1) 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. Any type already defined or that could be defined in the future for use in the RSVP-TE PROTECTION object is acceptable in this TLV unless explicitly stated otherwise.
Unassigned bits are considered reserved. They MUST be set to 0 on transmission and MUST be ignored on receipt.

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

4. Operation

An LSP is associated with other LSPs with which it interacts 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 purposes. 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) messages. 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 LSPs 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 6.4 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 "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 or update an LSP to a PPAG and the Tunnel ID (as carried in LSP-IDENTIFIERS TLV [RFC8231]) or source or destination of the LSP is different from the LSP(s) in the PPAG, the PCEP speaker MUST send PCErr with Error-Type 26 (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]). If the Protection Type (PT) (in Path Protection Association TLV) is different from the LSPs in the PPAG, the PCEP speaker MUST send PCErr with Error-Type 26 (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 PCEP peer does not support the protection type set in PPAG, the PCEP peer MUST send PCErr with Error-Type 26 (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 (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 (i.e., protection type=0x08 or 0x10), there MUST be at maximum, 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 (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 (i.e., protection type=0x04), there MUST be at maximum, 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 (Association Error) [I-D.ietf-pce-association-group] and Error-Value TBD4 (Attempt to add another working LSP for Path Protection Association).

During the make-before-break (MBB) procedure, two paths will briefly coexist. The error handling related to number of LSPs allowed in a PPAG MUST NOT be applied during MBB.

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. The relationship between the Synchronization VECTor (SVEC) object and the Disjointness Association is described in section 5.3 of [I-D.ietf-pce-association-diversity].

[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 Path Protection Association TLV in PCEP as received from the PCE is used to trigger the signaling 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

[Note to RFC Editor and IANA: Sections 3.1, 3.2, and 4.5 contain "TBD1" through "TBD5" those should be replaced by the values that IANA assigns.]

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:

<table>
<thead>
<tr>
<th>Association type</th>
<th>Association Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD1</td>
<td>Path Protection</td>
<td>This document</td>
</tr>
</tbody>
</table>

6.2. Path Protection Association 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:

<table>
<thead>
<tr>
<th>TLV Type</th>
<th>TLV Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD2</td>
<td>Path Protection Association Group TLV</td>
<td>This document</td>
</tr>
</tbody>
</table>

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
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:

<table>
<thead>
<tr>
<th>Error-type</th>
<th>Error-value</th>
<th>Meaning</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>TBD3</td>
<td>Tunnel ID or End points mismatch for Path Protection Association</td>
<td>This document</td>
</tr>
<tr>
<td>TBD3</td>
<td></td>
<td>Association Error</td>
<td>[I-D.ietf-pce-association-group]</td>
</tr>
<tr>
<td>TBD4</td>
<td></td>
<td>Attempt to add another working /protection LSP for Path Protection Association</td>
<td>This document</td>
</tr>
<tr>
<td>TBD5</td>
<td></td>
<td>Protection type is not supported</td>
<td>This document</td>
</tr>
</tbody>
</table>
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 as described in [I-D.ietf-pce-association-group]. Adding a spurious protection LSP to the Path Protection Association group could give false sense of network reliability, which leads to issues when the working LSP is down and the protection LSP fails as well. Thus securing the PCEP session using Transport Layer Security (TLS) [RFC8253], as per the recommendations and best current practices in BCP 195 [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.

Thanks to Pete Resnick for the GENART review.

Thanks to Donald Eastlake for the SECDIR review.

Thanks to Barry Leiba, Benjamin Kaduk, Eric Vyncke, and Roman Danyliw for the IESG review.

10. References

10.1. Normative References


10.2. Informative References


[I-D.ietf-pce-association-group]


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