PCE Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 4, 2020

M. Koldychev
S. Sivabalan
Cisco Systems, Inc.
C. Barth
Juniper Networks, Inc.
S. Peng
Huawei Technologies
H. Bidgoli
Nokia

June 2, 2020

PCEP extension to support Segment Routing Policy Candidate Paths
draft-barth-pce-segment-routing-policy-cp-06

Abstract

This document introduces a mechanism to specify a Segment Routing (SR) policy, as a collection of SR candidate paths. An SR policy is identified by <headend, color, end-point> tuple. An SR policy can contain one or more candidate paths where each candidate path is identified in PCEP via an PLSP-ID. This document proposes extension to PCEP to support association among candidate paths of a given SR policy. The mechanism proposed in this document is applicable to both MPLS and IPv6 data planes of SR.

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.

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 December 4, 2020.

Copyright Notice

Table of Contents

1. Introduction

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

PCEP Extensions for the Stateful PCE Model [RFC8231] describes a set of extensions to PCEP to enable active control of Multiprotocol Label Switching Traffic Engineering (MPLS-TE) and Generalized MPLS (GMPLS) tunnels. [RFC8281] describes the setup and teardown of PCE-initiated LSPs under the active stateful PCE model, without the need for local configuration on the PCC, thus allowing for dynamic centralized control of a network.

PCEP Extensions for Segment Routing [RFC8664] specifies extensions to the Path Computation Element Protocol (PCEP) that allow a stateful PCE to compute and initiate Traffic Engineering (TE) paths, as well as a PCC to request a path subject to certain constraint(s) and optimization criteria in SR networks.

PCEP Extensions for Establishing Relationships Between Sets of LSPs [RFC8697] introduces a generic mechanism to create a grouping of LSPs which can then be used to define associations between a set of LSPs and a set of attributes (such as configuration parameters or behaviors) and is equally applicable to stateful PCE (active and passive modes) and stateless PCE.

Segment Routing Policy for Traffic Engineering [I-D.ietf-spring-segment-routing-policy] details the concepts of SR Policy and approaches to steering traffic into an SR Policy.

An SR policy contains one or more candidate paths where one or more such paths can be computed via PCE. This document specifies PCEP extensions to signal additional information to map candidate paths to their SR policies. Each candidate path maps to a unique PLSP-ID in PCEP. By associating multiple candidate paths together, a PCE becomes aware of the hierarchical structure of an SR policy. Thus the PCE can take computation and control decisions about the candidate paths, with the additional knowledge that these candidate paths belong to the same SR policy. This is accomplished via the use of the existing PCEP Association object, by defining a new

association type specifically for associating SR candidate paths into a single SR policy.

[Editor's Note- Currently it is assumed that each candidate path has only one ERO (SID-List) within the scope of this document. Another document will deal with a way to allow multiple ERO/SID-Lists for a candidate path within PCEP.]

2. Terminology

The following terminologies are used in this document:

Endpoint: The IPv4 or IPv6 endpoint address of the SR policy in question, as described in [I-D.ietf-spring-segment-routing-policy].

Association parameters: As described in [RFC8697], the combination of the mandatory fields Association type, Association ID and Association Source in the ASSOCIATION object uniquely identify the association group. If the optional TLVs - Global Association Source or Extended Association ID are included, then they MUST be included in combination with mandatory fields to uniquely identify the association group.

Association information: As described in [RFC8697], the ASSOCIATION object could also include other optional TLVs based on the association types, that provides 'information' related to the association type.

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.

PCEP Tunnel: The entity identified by the PLSP-ID, as per [I-D.koldychev-pce-operational].

3. Motivation

The new Association Type (SR Policy Association) and the new TLVs for the ASSOCIATION object, defined in this document, allow a PCEP peer to exchange additional parameters of SR candidate paths and of their associated SR policy. For the SR policy, the parameters are: color

and endpoint. For the candidate path, the parameters are: protocol origin, originator, discriminator and preference. [I-D.ietf-spring-segment-routing-policy] describes the concept of SR Policy and these parameters.

The motivation for signaling these parameters is summarized in the following subsections.

3.1. Group Candidate Paths belonging to the same SR policy

Since each candidate path of an SR policy appears as a different LSP (identified via a PLSP-ID) in PCEP, it is useful to group together all the candidate paths that belong to the same SR policy. Furthermore, it is useful for the PCE to have knowledge of the SR candidate path parameters such as color, protocol origin, discriminator, and preference.

3.2. Instantiation of SR policy candidate paths

A PCE may want to instantiate one or more candidate paths on the PCC, as specified in [RFC8281]. In this scenario, the PCE needs to signal to a PCC <headend, color, end-point, originator, discriminator, preference> tuple using which the PCC can instantiate a candidate path for the SR policy identified. Current PCEP standards (as of the time of this writing) do not provide a way to signal color and preference. Although end-point can be signaled via the PCEP END-POINTS object, this object may not be suitable because the end-point to which the path is computed is not required to be the same IPv4/ IPv6 address as the actual endpoint of the SR policy. Thus, a separate way to specify SR policy's end-point is provided in this document.

3.3. Avoid computing lower preference candidate paths

When a PCE knows that a given set of candidate paths all belong to the same SR policy, then path computation MAY be done on only the highest preference candidate-path(s). Path computation for lower preference paths is not necessary if one or two higher preference paths are already computed. Since computing their paths will not affect traffic steering, it MAY be postponed until the higher preference paths become invalid, thus saving computation resources on the PCE.

3.4. Minimal signaling overhead

When an SR policy contains multiple candidate paths computed by a PCE, such candidate paths can be created, updated and deleted independently of each other. This is achieved by making each

candidate path correspond to a unique LSP (identified via PLSP-ID). For example, if an SR policy has 4 candidate paths, then if the PCE wants to update one of those candidate paths, only one set of PCUpd and PCRpt messages needs to be exchanged.

4. Procedure

4.1. Overview

As per [RFC8697], LSPs are placed into an association group. As per [I-D.koldychev-pce-operational], LSPs are contained in PCEP Tunnels and a PCEP Tunnel is contained in an Association if all of its LSPs are in that Association.

PCEP Tunnels naturally map to SR Candidate Paths and PCEP Associations naturally map to SR Policies. Definition of these mappings is the central purpose of this document.

The mapping between PCEP Associations and SR Policies is always one-to-one. However, the mapping between PCEP Tunnels and SR Candidate Paths may be either one-to-one, or many-to-one. The mapping is one-to-one when the SR Candidate Path has only a single constraint and optimization objective. The mapping is many-to-one when the SR Candidate Path has multiple constraints and optimization objectives. For more details on multiple optimization objectives and constraints, see Section 4.3.

[Editor's Note - Segment-lists within a candidate path are not represented by different PCEP Tunnels. The subject of encoding multiple segment lists within a candidate path is left to another document and is not specified in this document. It is not a good idea to have each segment-list correspond to a different Tunnel, because when the PCC wants to get a path, it must know in advance how many multipaths (i.e., segment-lists) there will be and create that many Tunnels. For example, if the PCC supports 32 multipaths, then it must delegate 32 Tunnels for every candidate path, which may not be scalable.]

A new Association Type is defined in this document, based on the generic ASSOCIATION object. Association type = TBD1 "SR Policy Association Type" for SR Policy Association Group (SRPAG). The SRPAG Association is only meant to be used for SR LSPs and with PCEP peers which advertise SR capability.

An Association object of SRPAG group contains TLVs that carry Association Information. The association information can be subdivided into three parts: Policy identifiers, Candidate path identifiers, and Candidate path attributes.

Policy Identifiers uniquely identify the SR policy to which a given LSP belongs, within the context of the head-end. Policy Identifiers MUST be the same for all candidate paths in the same SRPAG. Policy Identifiers MUST NOT change for a given LSP during its lifetime. Policy Identifiers MUST be different for different SRPAG associations. When these rules are not satisfied, the PCE MUST send a PCErr message with Error Code = 26 "Association Error", Error Type = TBD6 "Conflicting SRPAG TLV". Policy Identifiers consist of:

- Color of SR policy.
- End-point of SR policy.
- Optionally, the policy name.

Candidate Path Identifiers uniquely identify the SR candidate path within the context of an SR policy. Candidate path Identifiers MUST NOT change for a given LSP during its lifetime. Candidate path Identifiers MUST be different for different LSPs within the same SRPAG. When these rules are not satisfied, the PCE MUST send a PCErr message with Error Code = 26 "Association Error", Error Type = TBD6 "Conflicting SRPAG TLV". Candidate path Identifiers consist of:

- Protocol Origin of candidate path.
- Originator of candidate path.
- Discriminator of candidate path.
- Optionally, the candidate path name.

Candidate Path Attributes MUST NOT be used to identify the candidate path. Candidate path attributes carry additional information about the candidate path and MAY change during the lifetime of the LSP. Candidate path Attributes consist of:

- Preference of candidate path.

As per the processing rules specified in section 5.4 of [RFC8697], if a PCEP speaker does not support the SRPAG association type, it MUST return a PCErr message with Error-Type 26 (Early allocation by IANA) "Association Error" and Error-Value 1 "Association-type is not supported". Please note that the corresponding PCEP session is not reset.

4.2. Choice of Association Parameters

The Association Parameters (see Section 2) uniquely identify the Association. In this section, we describe how these are to be set.

The Association Source MUST be set to the PCC's address. This applies for both PCC-initiated and PCE-initiated candidate paths. The reasoning for this is that if different PCEs could set their own Association Source, then the candidate paths instantiated by different PCEs would by definition be in different PCEP Associations, which contradicts our requirement that the SR Policy is represented by an Association.

The Association ID MUST be chosen by the PCC when the SR policy is allocated. In PCRpt messages from the PCC, the Association ID MUST be set to the unique value that was allocated by the PCC at the time of policy creation. In PCInit messages from the PCE, the Association ID MUST be set to the reserved value 0xFFFF, which indicates that the PCE is asking the PCC to choose an ID value. The PCE MUST NOT send the Extended Association ID TLV in the PCInit messages.

If the PCC receives a PCInit message with Association Source not equal to the PCCs address, or with Association ID not equal to 0xFFFF, or with Extended Association ID TLV present, the PCC SHOULD ignore the given ASSOCIATION object.

4.3. Multiple Optimization Objectives and Constraints

In certain scenarios, it is desired for each SR Candidate Path to contain multiple sub-candidate paths, each of which has a different optimization objective and constraints. Traffic is then sent ECMP or UCMP among these sub-candidate paths.

This is represented in PCEP by a many-to-one mapping between PCEP Tunnels and SR Candidate Paths. This means that multiple PCEP Tunnels are allocated for each SR Candidate Path. Each PCEP Tunnel has its own optimization objective and constraints. When a single SR Candidate Path contains multiple PCEP Tunnels, each of these PCEP Tunnels MUST have identical values of Candidate Path Identifiers, as encoded in SRPOLICY-CPATH-ID TLV, see Section 5.3.

5. SR Policy Association Group

Two ASSOCIATION object types for IPv4 and IPv6 are defined in [RFC8697]. The ASSOCIATION object includes "Association type" indicating the type of the association group. This document adds a new Association type.

Association type = TBD1 "SR Policy Association Type" for SR Policy Association Group (SRPAG).

This Association type is dynamic in nature and created by the PCC or PCE for the candidate paths belonging to the same SR policy (as described in [I-D.ietf-spring-segment-routing-policy]). These associations are conveyed via PCEP messages to the PCEP peer. Operator-configured Association Range MUST NOT be set for this Association type and MUST be ignored.

SRPAG MUST carry additional TLVs to communicate Association Information. This document specifies five new TLVs to carry Association Information: SRPOLICY-POL-ID TLV, SRPOLICY-POL-NAME TLV, SRPOLICY-CPATH-ID TLV, SRPOLICY-CPATH-NAME TLV, SRPOLICY-CPATH-PREFERENCE TLV. These five TLVs encode the Policy Identifiers, SR Policy name, Candidate path identifiers, candidate path name, and Candidate path preference, respectively. When any of the mandatory TLVs are missing from the SRPAG association object, the PCE MUST send a PCErr message with Error Code = 26 "Association Error", Error Type = TBD7 "Missing mandatory SRPAG TLV".

A given LSP MUST belong to at most one SRPAG, since a candidate path cannot belong to multiple SR policies. If a PCEP speaker receives a PCEP message with more than one SRPAG for an LSP, then the PCEP speaker MUST send a PCErr message with Error-Type 26 "Association Error" and Error-Value TBD8 "Multiple SRPAG for one LSP". If the message is a PCRpt message, then the PCEP speaker MUST close the PCEP connection. Closing the PCEP connection is necessary because ignoring PCRpt messages may lead to inconsistent LSP DB state between the two PCEP peers.

If the PCEP speaker receives the SRPAG association when the SR capability (as per [RFC8664] or [I-D.ietf-pce-segment-routing-ipv6]) was not exchanged, the PCEP speaker MUST send a PCErr message with Error-Type 26 "Association Error" and Error-Value TBD9 "Use of SRPAG without SR capability exchange". If the Path Setup Type (PST) of the LSP in SRPAG is not set to SR or SRv6, then the PCEP speaker MUST send a PCErr message with Error-Type 26 "Association Error" and Error-Value TBD10 "non-SR LSP in SRPAG".

5.1. SR Policy Identifiers TLV

The SRPOLICY-POL-ID TLV is a mandatory TLV for the SRPAG Association. Only one SRPOLICY-POL-ID TLV can be carried and only the first occurrence is processed and any others MUST be ignored.

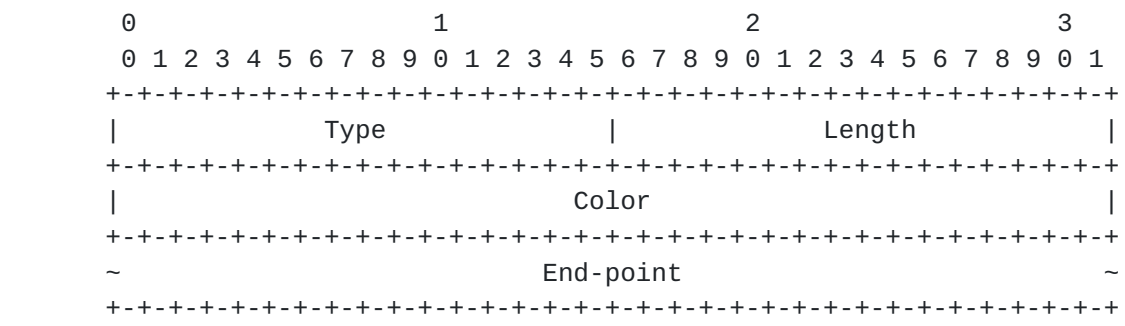

Figure 1: The SRPOLICY-POL-ID TLV format

Type: TBD2 for "SRPOLICY-POL-ID" TLV.

Length: 8 or 20, depending on length of End-point (IPv4 or IPv6)

Color: any unsigned 32-bit number.

End-point: can be either IPv4 or IPv6, depending on whether the policy endpoint has IPv4 or IPv6 address. This value may be different from the one contained in the END-POINTS object, or in the LSP IDENTIFIERS TLV of the LSP object. Endpoint is meant to strictly correspond to the endpoint of the SR policy, as it is defined in [I-D.ietf-spring-segment-routing-policy].

5.2. SR Policy Name TLV

The SRPOLICY-POL-NAME TLV is an optional TLV for the SRPAG Association. At most one SRPOLICY-POL-NAME TLV can be carried and only the first occurrence is processed and any others MUST be ignored.

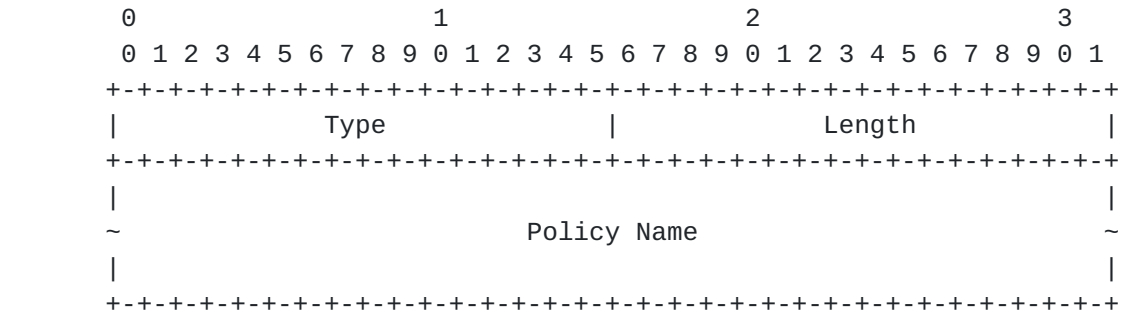

Figure 2: The SRPOLICY-POL-NAME TLV format

Type: TBD3 for "SRPOLICY-POL-NAME" TLV.

Length: indicates the total length of the TLV in octets and MUST be greater than 0. The TLV MUST be zero-padded so that the TLV is 4-octet aligned.

Policy Name: Policy name, as defined in [I-D.ietf-spring-segment-routing-policy]. It SHOULD be a string of printable ASCII characters, without a NULL terminator.

5.3. SR Policy Candidate Path Identifiers TLV

The SRPOLICY-CPATH-ID TLV is a mandatory TLV for the SRPAG Association. Only one SRPOLICY-CPATH-ID TLV can be carried and only the first occurrence is processed and any others MUST be ignored.

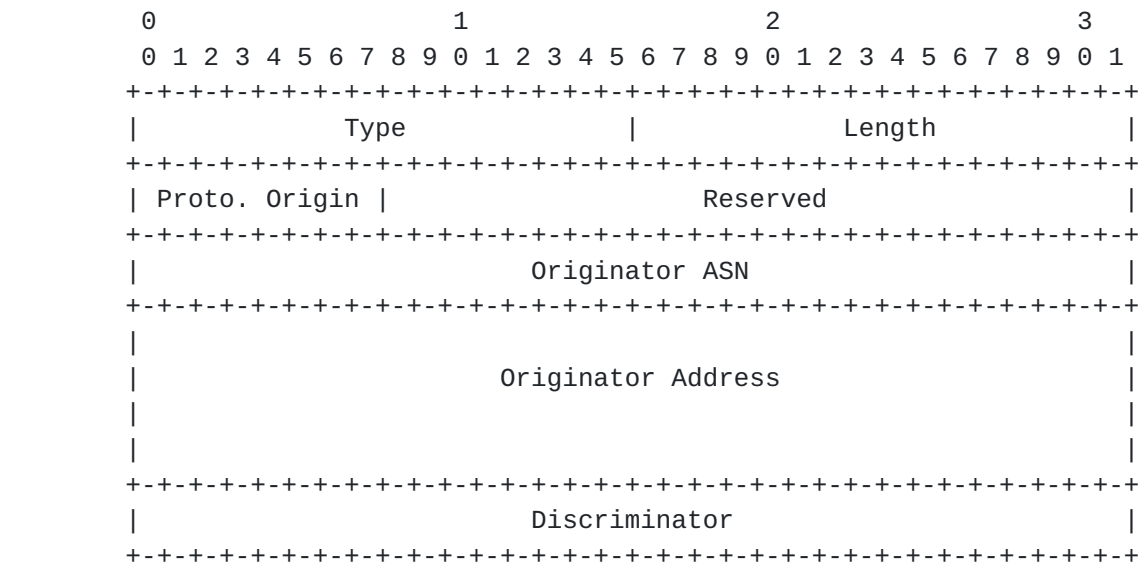

Figure 3: The SRPOLICY-CPATH-ID TLV format

Type: TBD4 for "SRPOLICY-CPATH-ID" TLV.

Length: 28.

Protocol Origin: 8-bit value that encodes the protocol origin, as specified in [I-D.ietf-spring-segment-routing-policy] Section 2.3.

Reserved: MUST be set to zero on transmission and ignored on receipt.

Originator ASN: Represented as 4 byte number, part of the originator identifier, as specified in [I-D.ietf-spring-segment-routing-policy] Section 2.4.

Originator Address: Represented as 128 bit value where IPv4 address are encoded in lowest 32 bits, part of the originator identifier, as specified in [I-D.ietf-spring-segment-routing-policy] Section 2.4.

Discriminator: 32-bit value that encodes the Discriminator of the candidate path.

5.4. SR Policy Candidate Path Name TLV

The SRPOLICY-CPATH-NAME TLV is an optional TLV for the SRPAG Association. At most one SRPOLICY-CPATH-NAME TLV can be carried and only the first occurrence is processed and any others MUST be ignored.

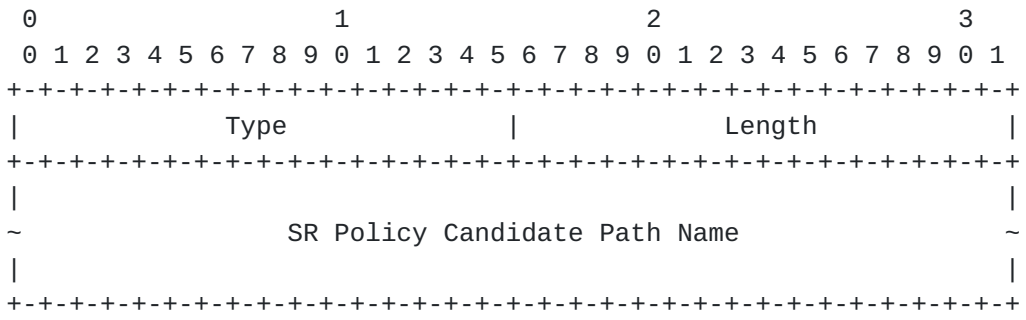

Figure 4: The SRPOLICY-CPATH-NAME TLV format

Type: TBD11 for "SRPOLICY-CPATH-NAME" TLV.

Length: indicates the total length of the TLV in octets and MUST be greater than 0. The TLV MUST be zero-padded so that the TLV is 4-octet aligned.

SR Policy Candidate Path Name: SR Policy Candidate Path Name, as defined in [I-D.ietf-spring-segment-routing-policy]. It SHOULD be a string of printable ASCII characters, without a NULL terminator.

5.5. SR Policy Candidate Path Preference TLV

The SRPOLICY-CPATH-PREFERENCE TLV is an optional TLV for the SRPAG Association. Only one SRPOLICY-CPATH-PREFERENCE TLV can be carried and only the first occurrence is processed and any others MUST be ignored.

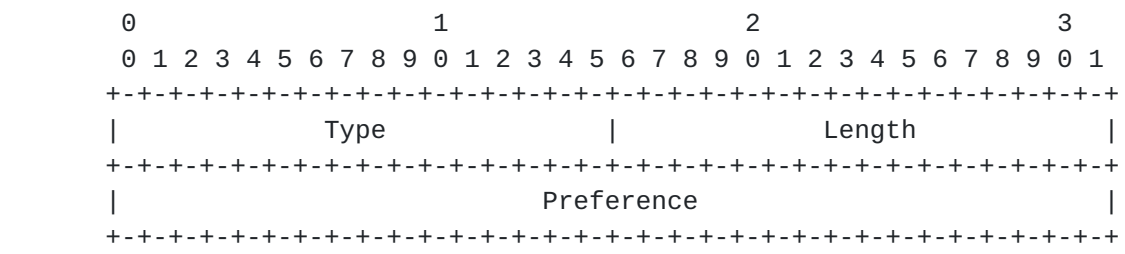

Figure 5: The SRPOLICY-CPATH-PREFERENCE TLV format

Type: TBD5 for "SRPOLICY-CPATH-PREFERENCE" TLV.

Length: 4.

Preference: Numerical preference of the candidate path, as specified in [I-D.ietf-spring-segment-routing-policy] Section 2.7.

If the TLV is missing, a default preference of 100 as specified in [I-D.ietf-spring-segment-routing-policy] is used.

6. Examples

6.1. PCC Initiated SR Policy with single candidate-path

PCReq and PCRep messages are exchanged in the following sequence:

1. PCC sends PCReq message to the PCE, encoding the SRPAG ASSOCIATION object and TLVs in the PCReq message.

2. PCE returns the path in PCRep message, and echoes back the SRPAG object that was used in the computation.

PCRpt and PCUpd messages are exchanged in the following sequence:

1. PCC sends PCRpt message to the PCE, including the LSP object and the SRPAG ASSOCIATION object.

2. PCE computes path, possibly making use of the Association Information from the SRPAG ASSOCIATION object.

3. PCE updates the SR policy candidate path's ERO using PCUpd message.

6.2. PCC Initiated SR Policy with multiple candidate-paths

PCRpt and PCUpd messages are exchanged in the following sequence:

1. For each candidate path of the SR Policy, the PCC generates a different PLSP-ID and symbolic-name and sends multiple PCRpt messages (or one message with multiple LSP objects) to the PCE. Each LSP object is followed by SRPAG ASSOCIATION object with identical Color and Endpoint values. The Association Source is set to the IP address of the PCC and the Association ID is set to a number that PCC locally chose to represent the SR Policy.

2. PCE takes into account that all the LSPs belong to the same SR policy. PCE prioritizes computation for the highest preference LSP and sends PCUpd message(s) back to the PCC.

3. If a new candidate path is added on the PCC by the operator, then a new PLSP-ID and symbolic name is generated for that candidate path and a new PCRpt is sent to the PCE.

4. If an existing candidate path is removed from the PCC by the operator, then that PLSP-ID is deleted from the PCE by sending PCRpt with the R-flag in the LSP object set.

6.3. PCE Initiated SR Policy with single candidate-path

A candidate-path is created using the following steps:

1. PCE sends PCInitiate message, containing the SRPAG Association object. The Association Source is set to the IP address of the PCC and the Association ID is set to 0xFFFF, as described in Section 4.2.

2. PCC uses the color, endpoint and preference from the SRPAG object to create a new candidate path. If no SR policy exists to hold the candidate path, then a new SR policy is created to hold the new candidate-path. The Originator of the candidate path is set to be the address of the PCE that is sending the PCInitiate message.

3. PCC sends a PCRpt message back to the PCE to report the newly created Candidate Path. The PCRpt message contains the SRPAG Association object. The Association Source is set to the IP address of the PCC and the Association ID is set to a number that PCC locally chose to represent the SR Policy.

A candidate-path is deleted using the following steps:

1. PCE sends PCInitiate message, setting the R-flag in the LSP object.

2. PCC uses the PLSP-ID from the LSP object to find the candidate path and delete it. If this is the last candidate path under the SR policy, then the containing SR policy is deleted as well.

6.4. PCE Initiated SR Policy with multiple candidate-paths

A candidate-path is created using the following steps:

1. PCE sends a separate PCInitiate message for every candidate path that it wants to create, or it sends multiple LSP objects within a single PCInitiate message. The SRPAG Association object is sent for every LSP in the PCInitiate message. The Association Source is set to the IP address of the PCC and the Association ID is set to 0xFFFF, as described in Section 4.2.

2. PCC creates multiple candidate paths under the same SR policy, identified by Color and Endpoint.

3. PCC sends a PCRpt message back to the PCE to report the newly created Candidate Path. The PCRpt message contains the SRPAG Association object. The Association Source is set to the IP address of the PCC and the Association ID is set to a number that PCC locally chose to represent the SR Policy.

A candidate path is deleted using the following steps:

1. PCE sends PCInitiate message, setting the R-flag in the LSP object.

2. PCC uses the PLSP-ID from the LSP object to find the candidate path and delete it.

7. IANA Considerations

7.1. Association Type

This document defines a new association type: SR Policy Association Group (SRPAG). IANA is requested to make the assignment of a new value for the sub-registry "ASSOCIATION Type Field" (request to be created in [RFC8697]), as follows:

Association Type Value	Association Name	Reference
TBD1	SR Policy Association	This document

7.2. PCEP Errors

This document defines five new Error-Values within the "Association Error" Error-Type. 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 Type	Error Value	Meaning	Reference
29	TBD6	Conflicting SRPAG TLV	This document
29	TBD7	Missing mandatory SRPAG TLV	This document
29	TBD8	Multiple SRPAG for one LSP	This document
29	TBD9	Use of SRPAG without SR capability exchange	This document
29	TBD10	non-SR LSP in SRPAG	This document

7.3. SRPAG TLVs

This document defines five new TLVs for carrying additional information about SR policy and SR candidate paths. 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	SRPOLICY-POL-ID	This document
TBD3	SRPOLICY-POL-NAME	This document
TBD4	SRPOLICY-CPATH-ID	This document
TBD11	SRPOLICY-CPATH-NAME	This document
TBD5	SRPOLICY-CPATH-PREFERENCE	This document

8. Security Considerations

This document defines one new type for association, which do not add any new security concerns beyond those discussed in [RFC5440], [RFC8231], [RFC8664], [I-D.ietf-pce-segment-routing-ipv6] and [RFC8697] in itself.

The information carried in the SRPAG Association object, as per this document is related to SR Policy. It often reflects information that can also be derived from the SR Database, but association provides a much easier grouping of related LSPs and messages. The SRPAG association could provides an adversary with the opportunity to eavesdrop on the relationship between the LSPs. Thus securing the PCEP session using Transport Layer Security (TLS) [RFC8253], as per the recommendations and best current practices in [RFC7525], is RECOMMENDED.

9. Acknowledgement

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>.

[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>.

[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-spring-segment-routing-policy]
Filsfils, C., Sivabalan, S., Voyer, D., Bogdanov, A., and P. Mattes, "Segment Routing Policy Architecture", draft-ietf-spring-segment-routing-policy-07 (work in progress), May 2020.

[RFC8697] 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)", RFC 8697, DOI 10.17487/RFC8697, January 2020, <https://www.rfc-editor.org/info/rfc8697>.

[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>.

[I-D.koldychev-pce-operational]
Koldychev, M., Sivabalan, S., Negi, M., Achaval, D., and H. Kotni, "PCEP Operational Clarification", draft-koldychev-pce-operational-01 (work in progress), February 2020.

10.2. Informative References

[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>.

[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>.

[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-segment-routing-ipv6]
Negi, M., Li, C., Sivabalan, S., Kaladharan, P., and Y. Zhu, "PCEP Extensions for Segment Routing leveraging the IPv6 data plane", draft-ietf-pce-segment-routing-ipv6-04 (work in progress), March 2020.

Appendix A. Contributors

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

Email: dhruv.ietf@gmail.com

Cheng Li
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing, 10095
China

Email: chengli13@huawei.com

Authors' Addresses

Mike Koldychev
Cisco Systems, Inc.
2000 Innovation Drive
Kanata, Ontario K2K 3E8
Canada

Email: mkoldych@cisco.com

Siva Sivabalan
Cisco Systems, Inc.
2000 Innovation Drive
Kanata, Ontario K2K 3E8
Canada

Email: msiva@cisco.com

Colby Barth
Juniper Networks, Inc.

Email: cbarth@juniper.net

Shuping Peng
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing 100095
China

Email: pengshuping@huawei.com

Hooman Bidgoli
Nokia

Email: hooman.bidgoli@nokia.com