

Workgroup: PCE Working Group
Internet-Draft:
draft-ietf-pce-segment-routing-policy-cp-10
Published: 21 April 2023
Intended Status: Standards Track
Expires: 23 October 2023
Authors: M. Koldychev S. Sivabalan
 Cisco Systems, Inc. Ciena Corporation
 C. Barth S. Peng
 Juniper Networks, Inc. Huawei Technologies
 H. Bidgoli
 Nokia

PCEP extension to support Segment Routing Policy Candidate Paths

Abstract

A Segment Routing (SR) Policy [[RFC9256](#)] is a non-empty set of SR Candidate Paths, that share the same <headend, color, endpoint> tuple. This document extends [[RFC8664](#)] to fully support the SR Policy construct. SR Policy is modeled in PCEP as an Association of one or more SR Candidate Paths. PCEP extensions are defined to signal additional attributes of an SR Policy, which are not covered by [[RFC8664](#)]. The mechanism is applicable to all data planes of SR (MPLS, SRv6, etc.).

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 23 October 2023.

Copyright Notice

Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

- [1. Introduction](#)
- [2. Terminology](#)
- [3. Overview](#)
 - [3.1. SR Policy Identifiers](#)
 - [3.2. SR Policy Candidate Path Identifiers](#)
 - [3.3. SR Policy Candidate Path Attributes](#)
 - [3.4. Multiple Optimization Objectives and Constraints](#)
- [4. SR Policy Association](#)
 - [4.1. Association Parameters](#)
 - [4.2. Association Information](#)
 - [4.2.1. SR Policy Name TLV](#)
 - [4.2.2. SR Policy Candidate Path Identifiers TLV](#)
 - [4.2.3. SR Policy Candidate Path Name TLV](#)
 - [4.2.4. SR Policy Candidate Path Preference TLV](#)
- [5. Generic Mechanisms](#)
 - [5.1. Computation Priority TLV](#)
 - [5.2. Explicit Null Label Policy \(ENLP\) TLV](#)
 - [5.3. Invalidation TLV](#)
 - [5.4. Specified-BSID-only](#)
- [6. IANA Considerations](#)
 - [6.1. Association Type](#)
 - [6.2. PCEP TLV Type Indicators](#)
 - [6.3. PCEP Errors](#)
 - [6.4. TE-PATH-BINDING TLV Flag field](#)
 - [6.5. SR Policy Candidate Path Protocol Origin field](#)
- [7. Implementation Status](#)
 - [7.1. Cisco](#)
 - [7.2. Juniper](#)
- [8. Security Considerations](#)
- [9. Acknowledgement](#)
- [10. References](#)
 - [10.1. Normative References](#)

[10.2. Informative References](#)
[Appendix A. Contributors](#)
[Authors' Addresses](#)

1. Introduction

PCEP Extensions for Segment Routing [[RFC8664](#)] specifies extensions that allow PCEP to work with basic SR-TE paths.

PCEP Extensions for Establishing Relationships Between Sets of LSPs [[RFC8697](#)] introduces a generic mechanism to create a grouping of LSPs, called an Association.

Segment Routing Policy for Traffic Engineering [[RFC9256](#)] introduces the SR Policy construct as a grouping of SR Candidate Paths.

This document extends [[RFC8664](#)] to fully support the SR Policy construct. SR Policy is modeled in PCEP as an Association and the SR Candidate Paths are the members of that Association. 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.

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 [[RFC9256](#)].

SRPA: SR Policy Association. PCEP ASSOCIATION that describes the SR Policy. Can refer to the PCEP object or to the group of LSPs that belong to the Association. This should be clear from the context.

Association Parameters: As described in [[RFC8697](#)], refers to the key data, that uniquely identifies the Association in the network.

Association Information: As described in [[RFC8697](#)], refers to the non-key information about the Association.

3. Overview

The SR Policy is represented by a new type of PCEP Association, called the SR Policy Association (SRPA). The SR Candidate Paths of an SR Policy are the PCEP LSPs within the same SRPA. The subject of encoding multiple Segment Lists within an SR Policy Candidate Path is described in [[I-D.ietf-pce-multipath](#)].

The SRPA carries three pieces of information: SR Policy Identifiers, SR Policy Candidate Path Identifiers, and SR Policy Candidate Path Attributes.

Additional information is also carried outside of SRPA: Computation Priority, Explicit Null Label Policy, Drop upon Invalid behavior, and Specified-BSID-only.

3.1. SR Policy Identifiers

SR Policy Identifiers uniquely identify the SR Policy within the network. SR Policy Identifiers MUST be the same for all SR Policy Candidate Paths in the same SRPA. SR Policy Identifiers MUST NOT change for a given SR Policy Candidate Path during its lifetime. SR Policy Identifiers MUST be different for different SRPAs. SR Policy Identifiers consist of:

- *Headend router where the SR Policy originates.

- *Color of SR Policy.

- *Endpoint of SR Policy.

3.2. SR Policy Candidate Path Identifiers

SR Policy Candidate Path Identifiers uniquely identify the SR Policy Candidate Path within the context of an SR Policy. SR Policy Candidate Path Identifiers MUST NOT change for a given LSP during its lifetime. SR Policy Candidate Path Identifiers MUST be different for different Candidate Paths within the same SRPA. When these rules are not satisfied, the PCE MUST send a PCErr message with Error-Type = 26 "Association Error", Error Value = TBD8 "SR Policy Candidate Path Identifiers Mismatch". SR Policy Candidate Path Identifiers consist of:

- *Protocol Origin.

- *Originator.

- *Discriminator.

3.3. SR Policy Candidate Path Attributes

SR Policy Candidate Path Attributes carry non-key information about the Candidate Path and MAY change during the lifetime of the LSP. SR Policy Candidate Path Attributes consist of:

- *Preference.

- *Optionally, the SR Policy Candidate Path name.

*Optionally, the SR Policy name.

3.4. Multiple Optimization Objectives and Constraints

In certain scenarios, it is desired for each SR Policy 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 Policy Candidate Paths. This means that multiple PCEP Tunnels are allocated for each SR Policy Candidate Path. Each PCEP Tunnel has its own optimization objective and constraints. When a single SR Policy 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 4.2.2](#).

4. SR Policy Association

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 (6) "SR Policy Association".

This Association Type is dynamic in nature, thus operator-configured Association Range MUST NOT be set for this Association type and MUST be ignored.

A PCEP speaker that supports the SRPA MUST send the ASSOC-Type-List TLV, defined in [\[RFC8697\]](#) Section 4.1, containing the value (6), corresponding to the SRPA Association Type. Otherwise the PCEP speaker MUST assume that the remote PCEP peer does not support SRPA and MUST NOT send the SRPA to that remote peer.

A given LSP MUST belong to at most one SRPA, since an SR Policy Candidate Path cannot belong to multiple SR Policies. If a PCEP speaker receives a PCEP message requesting to join more than one SRPA for the same LSP, then the PCEP speaker MUST send a PCERR message with Error-Type = 26 "Association Error", Error-Value = 7 "Cannot join the association group".

4.1. Association Parameters

As per [\[RFC9256\]](#), an SR Policy is identified through the tuple <headend, color, endpoint>. The headend is encoded as the Association Source in the ASSOCIATION object and the color and endpoint are encoded as part of Extended Association ID TLV.

The Association Parameters (see [Section 2](#)) consist of:

- *Association Type: set to 6 "SR Policy Association".
- *Association Source (IPv4/IPv6): set to the headend IP address.
- *Association ID (16-bit): set to "1".
- *Extended Association ID TLV: encodes the Color and Endpoint of the SR Policy.

The Association Source MUST be set to the headend value of the SR Policy, as defined in [\[RFC9256\]](#) Section 2.1. If the PCC receives a PCInit message with the Association Source set not to the headend IP but to some globally unique IP address that the headend owns, then the PCC SHOULD accept the PCInit message and create the SR Policy Association with the Association Source that was sent in the PCInit message.

The 16-bit Association ID field in the ASSOCIATION object MUST be set to the value of "1".

The Extended Association ID TLV MUST be included and it MUST be in the following format:

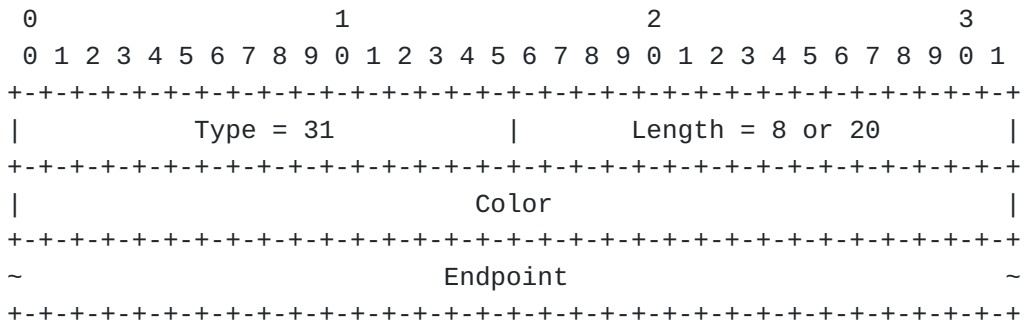


Figure 1: Extended Association ID TLV format

Type: Extended Association ID TLV, type = 31.

Length: Either 8 or 20, depending on whether IPv4 or IPv6 address is encoded in the Endpoint.

Color: SR Policy color value, non-zero as per [\[RFC9256\]](#) Section 2.1.

Endpoint: can be either IPv4 or IPv6. This value MAY be different from the one contained in the END-POINTS object, or in the LSP-IDENTIFIERS TLV.

If the PCEP speaker receives an SRPA object whose Association Parameters do not follow the above specification, then the PCEP speaker MUST send PCERR message with Error-Type = 26 "Association Error", Error-Value = TBD7 "SR Policy Identifiers Mismatch".

The purpose of choosing the Association Parameters in this way is to guarantee that there is no possibility of a race condition when multiple PCEP speakers want to create the same SR Policy at the same time. By adhering to this format, all PCEP speakers come up with the same Association Parameters independently of each other. Thus, there is no chance that different PCEP speakers will come up with different Association Parameters for the same SR Policy.

The computed destination of the SR Policy Candidate Path MAY differ from the Endpoint contained in the <headend, color, endpoint> tuple. An example use case is to terminate the SR Policy before reaching the Endpoint and have decapsulated traffic go the rest of the way to the Endpoint node using the native IGP path(s). In this example, the destination of the SR Policy Candidate Paths will be some node before the Endpoint, but the Endpoint value is still used at the head-end to steer traffic with that Endpoint IP into the SR Policy. Destination of the SR Policy Candidate Path is signaled using the END-POINTS object and/or LSP-IDENTIFIERS TLV, as per the usual PCEP procedures. When neither END-POINTS object nor LSP-IDENTIFIERS TLV is present, the PCEP speaker SHOULD extract the destination from the Endpoint field in the SRPA Extended Association ID TLV.

4.2. Association Information

The SRPA object contains the following TLVs:

*SRPOLICY-POL-NAME TLV: (optional) encodes SR Policy Name string.

*SRPOLICY-CPATH-ID TLV: (mandatory) encodes SR Policy Candidate Path Identifiers.

*SRPOLICY-CPATH-NAME TLV: (optional) encodes SR Policy Candidate Path string name.

*SRPOLICY-CPATH-PREFERENCE TLV: (optional) encodes SR Policy Candidate Path preference value.

Of these new TLVs, SRPOLICY-CPATH-ID TLV is mandatory. When a mandatory TLV is missing from the SRPA object, the PCE MUST send a PCERR message with Error-Type = 6 "Mandatory Object Missing", Error-Value = TBD6 "Missing Mandatory TLV".

Unless specifically stated otherwise, the TLVs listed in the following sub-sections are assumed to be single instance. Meaning, only one instance of the TLV SHOULD be present in the object and only

the first instance of the TLV SHOULD be interpreted and subsequent instances SHOULD be ignored.

4.2.1. SR Policy Name TLV

The SRPOLICY-POL-NAME TLV is an optional TLV for the SRPA object.

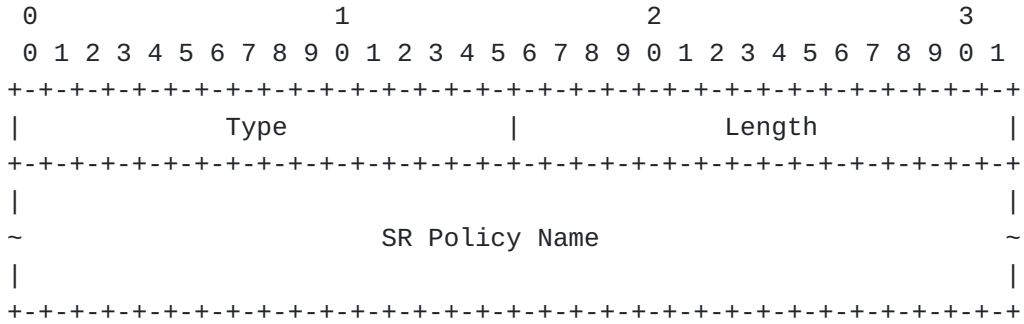


Figure 2: The SRPOLICY-POL-NAME TLV format

Type: 56 for "SRPOLICY-POL-NAME" TLV.

Length: indicates the length of the value portion 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 Name: SR Policy name, as defined in [\[RFC9256\]](#). It SHOULD be a string of printable ASCII characters, without a NULL terminator.

4.2.2. SR Policy Candidate Path Identifiers TLV

The SRPOLICY-CPATH-ID TLV is a mandatory TLV for the SRPA object.

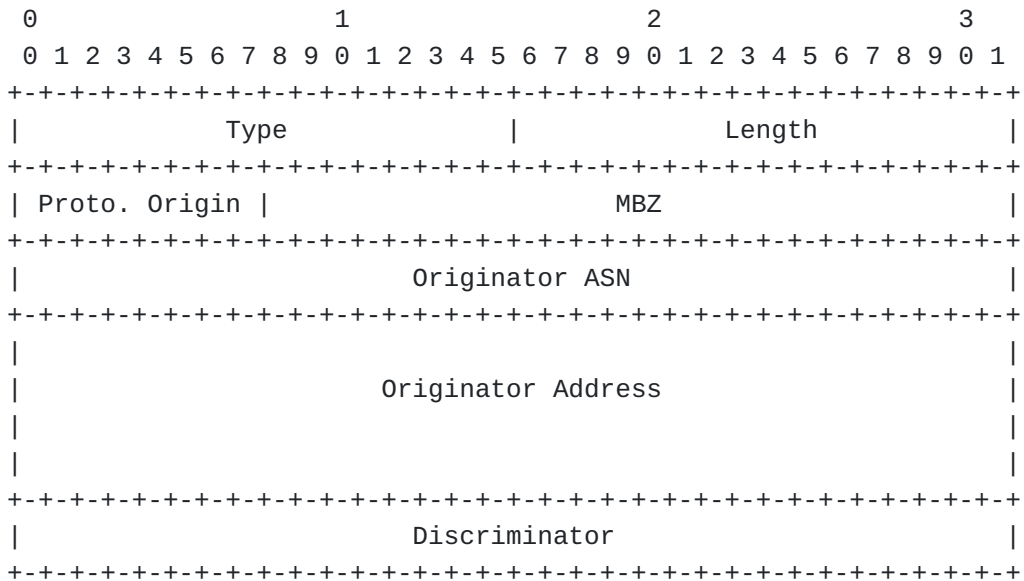


Figure 3: The SRPOLICY-CPATH-ID TLV format

Type: 57 for "SRPOLICY-CPATH-ID" TLV.

Length: 28.

Protocol Origin: 8-bit value that encodes the protocol origin, as specified in [RFC9256] Section 2.3. Note that in PCInit messages, the Protocol Origin is always set to "PCEP".

Originator ASN: Represented as 4 byte number, part of the originator identifier, as specified in [RFC9256] Section 2.4. When sending PCInit, the PCE is acting as the originator and therefore SHOULD set this to an ASN that it belongs to.

Originator Address: Represented as 128 bit value where IPv4 address are encoded in lowest 32 bits, part of the originator identifier, as specified in [RFC9256] Section 2.4. When sending PCInit, the PCE is acting as the originator and therefore SHOULD set this to an address that it owns.

Discriminator: 32-bit value that encodes the Discriminator of the Candidate Path. This is the field that mainly distinguishes different SR Candidate Paths, coming from the same originator. It is allowed to be any number in the 32-bit range.

4.2.3. SR Policy Candidate Path Name TLV

The SRPOLICY-CPATH-NAME TLV is an optional TLV for the SRPA object.

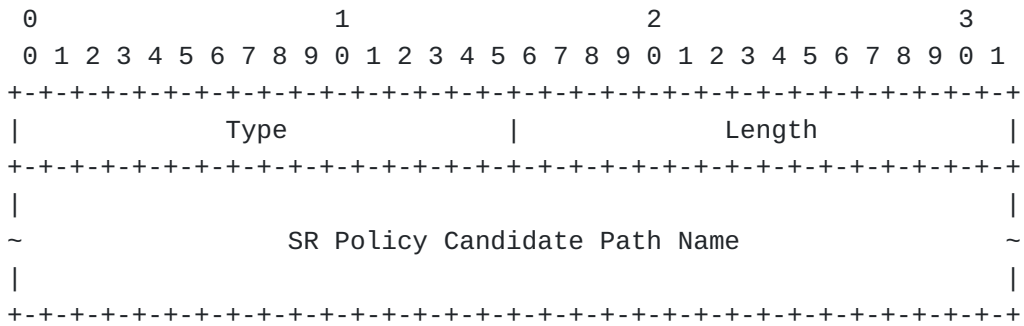


Figure 4: The SRPOLICY-CPATH-NAME TLV format

Type: 58 for "SRPOLICY-CPATH-NAME" TLV.

Length: indicates the length of the value portion 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.

Figure 6: The COMPUTATION-PRIORITY TLV format

Type: TBD1 for "COMPUTATION-PRIORITY" TLV.

Length: 4.

Priority: Numerical priority with which this LSP is to be recomputed by the PCE upon topology change.

5.2. Explicit Null Label Policy (ENLP) TLV

The ENLP TLV is an optional TLV for the LSP object. It is used to implement the "Explicit Null Label Policy", as specified in Section 2.4.5 of [[I-D.ietf-idr-segment-routing-te-policy](#)].

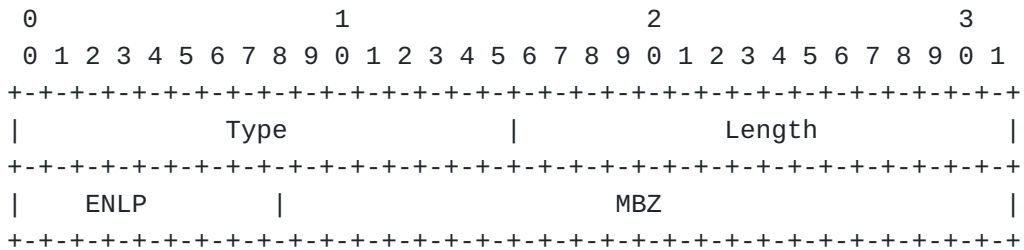


Figure 7: The Explicit Null Label Policy (ENLP) TLV format

Type: TBD2 for "ENLP" TLV.

Length: 4.

ENLP (Explicit NULL Label Policy): same values as in Section 2.4.5 of [[I-D.ietf-idr-segment-routing-te-policy](#)].

5.3. Invalidation TLV

The INVALIDATION TLV is an optional TLV for the LSP object. It is used to control traffic steering into the LSP during the time when the LSP is operationally down/invalid. In the context of SR Policy, this TLV facilitates the "Drop upon invalid" behavior, specified in Section 8.2 of [[RFC9256](#)]. Normally, if the LSP is down/invalid then it stops attracting traffic and traffic that is originally destined for that LSP is redirected somewhere else, such as via IGP or via another LSP. The "Drop upon invalid" behavior specifies that the LSP keeps attracting traffic and the traffic has to be dropped at the head-end. Such an LSP is said to be "in drop state". While in the drop state, the LSP operational state is "UP", as indicated by the O-flag in the LSP object. However the ERO object MAY be empty, if no valid path has been computed.

The INVALIDATION TLV is used in both directions between PCEP peers:

*PCE -> PCC: PCE specifies to the PCC under what conditions the LSP should enter the drop state.

*PCC -> PCE: PCC reports under what conditions the LSP will enter the drop state and the PCC also reports whether the LSP is currently in the drop state and if so, for what reason.

Reasons for entering the drop state are represented by a set of flags.

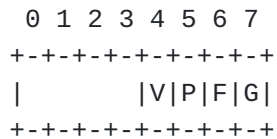


Figure 8: Invalidation Reasons Flags

*G: Generic - does not fit into any other categories below.

*F: First-hop resolution failure - head-end first hop resolution has failed.

*P: Path computation failure - no path was computed for the LSP.

*V: Verification failure - OAM/PM/BFD path verification has indicated a breakage.

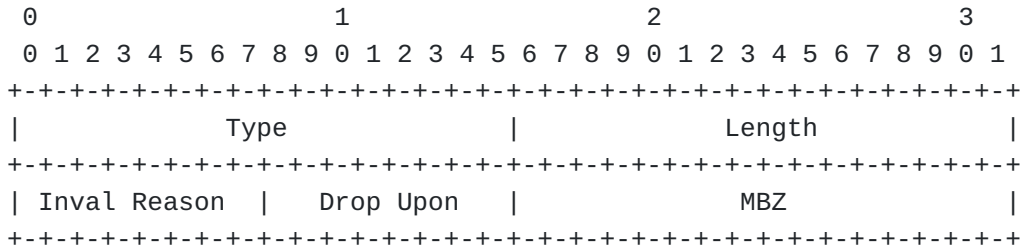


Figure 9: The INVALIDATION TLV format

Type: TBD3 for "INVALIDATION" TLV.

Length: 4.

Inval Reason: contains "Invalidation Reasons Flags" which encode the reason(s) why the LSP is currently invalidated. This field can be set to non-zero values only by the PCC, it MUST be set to 0 by the PCE and ignored by the PCC.

Drop Upon: contains "Invalidation Reasons Flags" for conditions that SHOULD cause the LSP to enter drop state. This field can be set to non-zero values by both PCC and PCE. When the G-flag is set, this indicates that the LSP is to go into Drop upon invalid state for any reason. I.e., when the PCE does not wish to distinguish any reason for LSP invalidation and just simply wants it to always go into drop state whenever the LSP is down. Note that when the G-flag is set, the values of the other flags are irrelevant.

Note that out of all the "Invalidation Reasons Flags", only the G-flag (Generic) MUST be supported. The other flags can simply be ignored if they are not supported by the PCEP speaker. For example, suppose the PCC only supports P-flag and G-flag. When this PCC receives this TLV with Drop Upon set to 0x6 (P,F), then the PCC responds with Drop Upon = 0x4 (P). When this PCC receives this TLV with Drop Upon set to 0x7 (P,F,G), then the PCC responds with Drop Upon = 0x5 (P,G).

5.4. Specified-BSID-only

Specified-BSID-only functionality is defined in Section 6.2.3 of [\[RFC9256\]](#). When specified-BSID-only is enabled for a particular binding SID, it means that the given binding SID is required to be allocated and programmed for the LSP to be operationally up. If the binding SID cannot be allocated or programmed for some reason, then the LSP must stay down.

To signal specified-BSID-only, a new bit: S (Specified-BSID-only) is allocated in the "TE-PATH-BINDING TLV Flag field" of the TE-PATH-BINDING TLV. When this bit is set for a particular BSID, it means that the BSID follows the Specified-BSID-only behavior. It is possible to have a mix of BSIDs for the same LSP: some with S=1 and some with S=0.

6. IANA Considerations

6.1. Association Type

This document defines a new association type: SR Policy Association. IANA is requested to make the following codepoint assignment in the "ASSOCIATION Type Field" subregistry [\[RFC8697\]](#) within the "Path Computation Element Protocol (PCEP) Numbers" registry:

Type	Name	Reference
6	SR Policy Association	This.I-D

6.2. PCEP TLV Type Indicators

This document defines four 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:

Value	Description	Reference
56	SRPOLICY-POL-NAME	This.I-D
57	SRPOLICY-CPATH-ID	This.I-D
58	SRPOLICY-CPATH-NAME	This.I-D
59	SRPOLICY-CPATH-PREFERENCE	This.I-D
TBD1	COMPUTATION-PRIORITY	This.I-D
TBD2	EXPLICIT-NULL-LABEL-POLICY	This.I-D
TBD3	INVALIDATION	This.I-D

6.3. PCEP Errors

This document defines one new Error-Value within the "Mandatory Object Missing" Error-Type and two 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	Meaning	Error-value	Reference
6	Mandatory Object		[RFC5440]
	Missing		
		TBD6: SR Policy	This.I-D
		Missing Mandatory TLV	
26	Association		[RFC8697]
	Error		
		TBD7: SR Policy	This.I-D
		Identifiers Mismatch	
		TBD8: SR Policy	This.I-D
		Candidate Path	
		Identifiers Mismatch	

6.4. TE-PATH-BINDING TLV Flag field

IANA is requested to allocate new bit within the "TE-PATH-BINDING TLV Flag field" sub-registry of the PCEP Numbers registry, as follows:

Bit position	Description	Reference
TBD9	S (Specified-BSID-only)	This.I-D

6.5. SR Policy Candidate Path Protocol Origin field

This document requests IANA to maintain a new registry under "Segment Routing Parameters" registry group. New values are to be assigned by "Standards Action" [RFC8126]. The new registry is called "SR Policy Protocol Origin". The registry contains the following codepoints, with initial values, to be assigned by IANA with the reference set to this document:

Value	Description
0	Reserved (not to be used)
1-9	Unassigned
10	PCEP
11-19	Unassigned
20	BGP SR Policy
21-29	Unassigned
30	Configuration (CLI, YANG model via NETCONF, etc.)
31-250	Unassigned
251 - 255	Private Use (not to be assigned by IANA)

7. Implementation Status

[Note to the RFC Editor - remove this section before publication, as well as remove the reference to RFC 7942.]

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [[RFC7942](#)]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [[RFC7942](#)], "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

7.1. Cisco

*Organization: Cisco Systems

*Implementation: IOS-XR PCC and PCE.

*Description: All features supported except Computation Priority, Explicit NULL and Invalidation Drop.

*Maturity Level: Production.

*Coverage: Full.

*Contact: mkoldych@cisco.com

7.2. Juniper

*Organization: Juniper Networks

*Implementation: Head-end and controller.

*Description: An experimental code-point is currently used.

*Maturity Level: Proof of concept.

*Coverage: Partial.

*Contact: cbarth@juniper.net

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 SRPA 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 SRPA could provide 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

Would like to thank Stephane Litkowski, Boris Khasanov, Abdul Rehman, Alex Tokar, Praveen Kumar and Tom Petch for review and suggestions.

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>>.
- [RFC8236] Hao, F., Ed., "J-PAKE: Password-Authenticated Key Exchange by Juggling", RFC 8236, DOI 10.17487/RFC8236, September 2017, <<https://www.rfc-editor.org/info/rfc8236>>.
- [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>>.
- [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>>.
- [RFC9256] Filsfils, C., Talaulikar, K., Ed., Voyer, D., Bogdanov, A., and P. Mattes, "Segment Routing Policy Architecture", RFC 9256, DOI 10.17487/RFC9256, July 2022, <<https://www.rfc-editor.org/info/rfc9256>>.
- [I-D.ietf-idr-segment-routing-te-policy] Previdi, S., Filsfils, C., Talaulikar, K., Mattes, P., Jain, D., and S. Lin, "Advertising Segment Routing Policies in BGP", Work in Progress, Internet-Draft, draft-ietf-idr-segment-routing-te-policy-20, 27 July 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-idr-segment-routing-te-policy-20>>.
- [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.ietf-pce-multipath]

Koldychev, M., Sivabalan, S., Saad, T., Beeram, V. P., Bidgoli, H., Yadav, B., Peng, S., and G. S. Mishra, "PCEP Extensions for Signaling Multipath Information", Work in Progress, Internet-Draft, draft-ietf-pce-multipath-07, 14 November 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-pce-multipath-07>>.

10.2. Informative References

[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>>.

[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]

Li, C., Negi, M. S., Sivabalan, S., Koldychev, M., Kaladharan, P., and Y. Zhu, "Path Computation Element Communication Protocol (PCEP) Extensions for Segment Routing leveraging the IPv6 dataplane", Work in Progress, Internet-Draft, draft-ietf-pce-segment-routing-ipv6-16, 6 March 2023, <<https://datatracker.ietf.org/doc/html/draft-ietf-pce-segment-routing-ipv6-16>>.

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

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

Email: ssidor@cisco.com

Authors' Addresses

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

Email: mkoldych@cisco.com

Siva Sivabalan
Ciena Corporation
385 Terry Fox Dr.
Kanata Ontario K2K 0L1
Canada

Email: ssivabal@ciena.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