PCE Working Group
Internet-Draft
Updates: 8231 (if approved)
Intended status: Standards Track
Expires: 29 August 2025

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

25 February 2025

Path Computation Element Communication Protocol (PCEP) Extensions for Segment Routing (SR) Policy Candidate Paths
draft-ietf-pce-segment-routing-policy-cp-22

Abstract

A Segment Routing (SR) ~~allows a node to steer a packet flow along any path. SR~~ Policy is an ordered list of ~~segments (i.e.,~~ instructions, ~~called "segments").~~ that represent a source-routed policy. Packet flows are steered into an SR Policy on a node where it is instantiated, called a headend node. An SR Policy is made of one or more candidate paths.

This document specifies the Path Computation Element Communication Protocol (PCEP) extension to signal candidate paths of ~~the~~ an SR Policy.

Additionally, this document updates RFC 8231 to allow stateful bring up of an SR Label Switched Path (LSP), without using the path computation request and reply messages. This document is applicable to both Segment Routing over MPLS (SR-MPLS) and Segment Routing over IPv6 (SRv6).

Commenté [MB1]: I know this is grabbed from other SR docs, but I don't think that sentence adds much here.

Commenté [MB2]: Better to use the 8402 wording here because otherwise it is not why we include the «instructions» mention.

Better would be to delete that mention 😊

Commenté [MB3]: Not clear what is meant here. Please reword

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 29 August 2025.

Table of Contents

1. Introduction 3
1.1. Requirements Language 4
2. Terminology 4
3. Overview 5
3.1. SR Policy Identifier 6
3.2. SR Policy Candidate Path Identifier 6
3.3. SR Policy Candidate Path Attributes 6
4. SR Policy Association 7
4.1. Association Parameters 7
4.2. Association Information 9
4.2.1. SR Policy Name TLV 9
4.2.2. SR Policy Candidate Path Identifier TLV 10
4.2.3. SR Policy Candidate Path Name TLV 11
4.2.4. SR Policy Candidate Path Preference TLV 12
5. Other Mechanisms 12
5.1. SR Policy Capability TLV 13
5.2. Computation Priority TLV 14
5.3. Explicit Null Label Policy (ENLP) TLV 14
5.4. Invalidation TLV 15
5.4.1. Drop-upon-invalid applies to SR Policy 17
5.5. Update to RFC 8231 17
6. IANA Considerations 18
6.1. Association Type 18
6.2. PCEP TLV Type Indicators 18
6.3. PCEP Errors 19
6.4. TE-PATH-BINDING TLV Flag field 20
6.5. SR Policy Candidate Path Protocol Origin field 21
6.6. SR Policy Invalidation Operational State 22
6.7. SR Policy Invalidation Configuration State 22
6.8. SR Policy Capability TLV Flag field 23
7. Implementation Status 23
7.1. Cisco 24
7.2. Juniper 24
8. Security Considerations 24
9. Manageability Considerations 25
9.1. Control of Function and Policy 25
9.2. Information and Data Models 25
9.3. Liveness Detection and Monitoring 25
9.4. Verify Correct Operations 25
9.5. Requirements On Other Protocols 26
9.6. Impact On Network Operations 26
10. Acknowledgement 26

11. References 26
11.1. Normative References 26
11.2. Informative References 28
Appendix A. Contributors 28
Authors' Addresses 29

1. Introduction

Segment Routing (SR) Policy Architecture [RFC9256] details the concepts of SR Policy [RFC8402] and approaches to steering traffic into an SR Policy.

Path Computation Element Protocol (PCEP) Extensions for Segment Routing [RFC8664] specifies extensions to ~~the Path Computation Element Protocol (~~PCEP~~)~~ that allow a stateful Path Computation Element (PCE) to compute and initiate Traffic Engineering (TE) paths, as well as a Path Computation Client (PCC) to request a path subject to certain constraints~~constraint(s)~~ and optimization criteria in SR networks. Although PCEP extensions introduced in [RFC8664] ~~were originally used~~are defined for creation ~~to create~~ SR-TE tunnels, these are not SR Policies and lack many important features and details.

PCEP Extensions for Establishing Relationships Between Sets of PCEP LSPs [RFC8697] introduces a generic mechanism to create a grouping of LSPs which is called an Association.

This document extends [RFC8664] to support signaling SR Policy Candidate Paths as PCEP LSPs and to signal Candidate Path membership in an SR Policy by means of the Association mechanism. ~~The~~ A PCEP Association corresponds to ~~the~~ a SR Policy and ~~the~~ a PCEP LSP corresponds to ~~the~~ a Candidate Path. The unit of signaling in PCEP is the LSP, thus all the information is carried at the Candidate Path level.

Also, ~~This~~ this document updates Section 5.8.2 of [RFC8231], making the PCReq message optional for LSPs setup~~set up~~ using Path Setup Type 1 (Segment Routing) ~~described in~~ [RFC8664] and Path Setup Type 3 (SRv6) ~~described in~~ [RFC9603], allowing a PCC to delegate such LSP by sending a Path Computation Report (PCRpt) without the preliminary Path Computation Request (PCReq) and Path Computation Reply (PCRep) messages, with the aim of reducing the PCEP message exchanges and simplifying implementation.

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

Commenté [MB4]: As this was defined first there.

Commenté [MB5]: Can we provide examples?

Commenté [MB6]: Should be introduced first

Commenté [MB7]: Which information?

Commenté [MB8]: Should this be SR-MPLS?

Commenté [MB9]: Too long and not easy to follow. Please simplify

The following ~~terminologies~~ terms are used in this document:

Endpoint: The IPv4 or IPv6 endpoint address of an SR Policy, as described in ~~[RFC9256]~~ Section 2.1 of [RFC9256].

Color: The 32-bit color of an SR Policy, as described in Section 2.1 of [RFC9256] ~~Section 2.1~~.

Protocol-Origin: The protocol that was used to create ~~the~~ a Candidate Path, as described in Section 2.3 of [RFC9256] ~~Section 2.3~~.

Originator: A ~~Device~~ device that ~~created~~ creates ~~the~~ a Candidate Path, as described in Section 2.4 of [RFC9256] ~~Section 2.4~~.

Discriminator: Distinguishes Candidate Paths created by the same device, as described in Section 2.5 of [RFC9256] ~~Section 2.5~~.

Association Parameters: As described in [RFC8697], refers to the key data~~,~~ that uniquely identifies ~~the~~ an Association.

Association Information: As described in [RFC8697], refers to the non-key information about ~~the~~ an Association.

SR Policy LSP: An LSP set up using Path Setup Type 1 (~~Segment Routing~~SR-MPLS) or Path Setup Type 3 (SRv6).

ASN: Autonomous System Number~~.~~

BSID: Binding Segment Identifier~~.~~

ENLP: Explicit Null Label Policy~~.~~

IGP: Interior Gateway Protocol~~.~~

LSP: Label Switched Path~~.~~

MPLS: Multiprotocol Label Switching~~.~~

PCC: Path Computation Client~~.~~

PCE: Path Computation Element~~.~~

PCEP: Path Computation Element Protocol~~.~~

SID: Segment Identifier~~.~~

SR: Segment Routing~~.~~

SRPA: SR Policy Association. A new association type 'SR Policy Association' is used to group candidate paths belonging to ~~the~~ an SR Policy. Depending on the discussion context, it can refer to the PCEP ASSOCIATION object of SR Policy type or to a group of LSPs that belong to the association.

Commenté [MB10]: I failed to find such wording in RFC8697

Commenté [MB11]: Should be defined first or point to RFC8408

Commenté [MB12]: Please double check.

Commenté [MB13]: I would not mix the acronym and definitions

SRPM: SR Policy Manager.

SR-TE: Segment Routing Traffic Engineering.

TE: Traffic Engineering.

TLV: Type-Length-Value.

3. Overview

The SR Policy is represented by a new type of PCEP Association, called the SR Policy Association (SRPA) (Section 7). The SR Candidate Paths of an SR Policy are the PCEP LSPs within the same SRPA. ~~The subject of encoding~~ Encoding multiple Segment Lists within an SR Policy Candidate Path is described in [I-D.ietf-pce-multipath]. These considerations are not covered here.

~~The~~ An SRPA carries three pieces of information: SR Policy Identifier, SR Policy Candidate Path Identifier, and SR Policy Candidate Path Attribute(s).

This document also specifies some additional information that is not encoded as part of an SRPA: Computation Priority, Explicit Null Label Policy, and Drop-upon-invalid behavior (Section 5).

This document does not ~~propose~~ define any extension for the use of Binding SID (BSID) with SR Policy; the ~~existing~~ behavior is documented in [RFC9604].

3.1. SR Policy Identifier

SR Policy Identifier uniquely identifies ~~the~~ an SR Policy [RFC9256] within the network. SR Policy Identifier MUST be the same for all SR Policy Candidate Paths in the same SRPA. SR Policy Identifier MUST be constant for a given SR Policy Candidate Path for the lifetime of the PCEP session. SR Policy Identifier MUST be different for different SRPAs. If the identifier is inconsistent among Candidate Paths, changes during the lifetime of the PCEP session, or is not unique across different SRPAs, the PCEP speaker MUST send a PCEP Error (PCErr) message with Error-Type = 26 "Association Error" and Error Value = 20 "SR Policy Identifier Mismatch". SR Policy Identifier ~~consist~~ consists of:

* Headend router where the SR Policy originates.
* Color of the SR Policy ([RFC9256], Section 2.1).
* Endpoint of the SR Policy ([RFC9256], Section 2.1).

3.2. SR Policy Candidate Path Identifier

SR Policy Candidate Path Identifier uniquely identifies the SR Policy Candidate Path within the context of an SR Policy. SR Policy Candidate Path Identifier MUST be constant for the lifetime of the PCEP session. SR Policy Candidate Path Identifier MUST be different

Commenté [MB14]: This is used once in the doc!

Commenté [MB15]: Used only one!

Commenté [MB16]: You may move this text to be positionned near the text about BSID to group items that are out of scope.

Commenté [MB17]: Given that this is an overview, consider a brief description/goal of these extra TLVs.

Commenté [MB18]: !! Are there additional considerations to take into account when used with the new objects on this document?

For example, the base spec says «Candidate paths of different SR Policies MUST NOT have the same BSID. » while this is not (at least I failed to find where) defined in 9604.

Commenté [MB19]: Who assigns this id? Who ensures unicity?

Commenté [MB20]: !! Do you meant «is» instead of «is not» given that you say «SR Policy Identifier MUST be different for different SRPAs.»

for distinct Candidate Paths within the same SRPA. If an identifier changes during the lifetime of the PCEP session or is not unique among distinct Candidate Paths, the PCEP speaker MUST send a PCErr message with Error-Type = 26 "Association Error" and Error Value = 21 "SR Policy Candidate Path Identifier Mismatch". SR Policy Candidate Path Identifier ~~consist~~ consists of:

* Protocol Origin ([RFC9256], Section 2.3).

* Originator ([RFC9256], Section 2.4).

* Discriminator ([RFC9256], Section 2.5).

3.3. SR Policy Candidate Path Attributes

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

* Candidate Path preference.

* Candidate Path name.

* SR Policy name.

4. SR Policy Association (SRPA)

~~As p~~Per [RFC8697], LSPs are associated with other LSPs with which they interact by adding them to a common association group. ~~As described in [RFC8697], the~~An association group is uniquely identified by the combination of the following fields in the ASSOCIATION object (Section 6.1 of [RFC8697]):

Association Type, Association ID, Association Source, and (if present) Global Association Source, or Extended Association ID~~,~~. These fields are referred to as Association Parameters (Section 4.1).

[RFC8697] specifies the ASSOCIATION Object with two Object-Types for IPv4 and IPv6 which includes the field "Association Type". This document defines a new Association type (6) "SR Policy Association" for SRPA (Section 6.1).

[RFC8697] specifies the mechanism for the capability advertisement of the Association Types supported by a PCEP speaker by defining an ASSOC-Type-List TLV to be carried within an OPEN object. This capability exchange for the SR Policy Association ~~Types~~ Type MUST be done before using the SRPA. ~~Thus~~To that aim, ~~the~~ a PCEP speaker MUST include the SRPA Type (6) in the ASSOC-Type-List TLV and MUST receive the same from the PCEP peer before using the SRPA.

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

Commenté [MB21]: !! Please double check with the previous text «SR Policy Candidate Path Identifier MUST be different for distinct Candidate Paths». Do you mean «is» instead of «is not»?

Commenté [MB22]: cite 2.7 of rfc9256

Commenté [MB23]: Is this the name defined in 2.6 of 9256?

Commenté [MB24]: Is this the same as in 2.1 of RFC9256

Commenté [MB25]: Split the long sentence.

join the association group".

4.1. Association Parameters

As Pper Section 2.1 of [RFC9256], an SR Policy is identified through the tuple <headend, color, endpoint> tuple. The headend is encoded in the 'Association Source' field in the ASSOCIATION object. The color and endpoint are encoded as part of the Extended Association ID TLV.

The Association Parameters (see Section 2) consist of:

* Association Type: Part of the base ASSOCIATION object. Set to 6 "SR Policy Association".

* Association Source (IPv4/IPv6): Part of the base ASSOCIATION object. Set to the headend value of the SR Policy, as defined in [RFC9256], Section 2.1.

* Association ID (16-bit): Part of the base ASSOCIATION object. Always set to the numeric value "1". This 16-bit field does not store meaningful data, because neither the Color nor the Endpoint can fit in it.

* Extended Association ID TLV: Mandatory TLV of the ASSOCIATION object. Encodes the Color and Endpoint of the SR Policy (Figure 1).

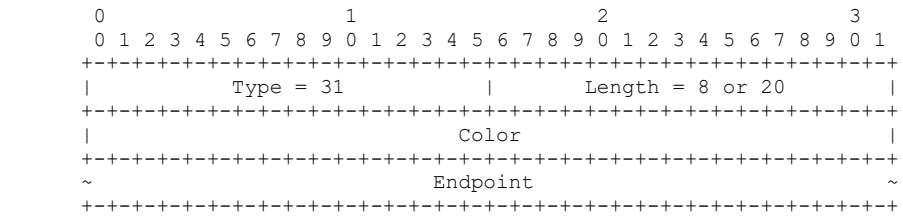


Figure 1: Extended Association ID TLV Fformat

Type: Extended Association ID TLV, type = 31 [RFC8697].

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

Color: SR Policy color value, MUST be non-zero as per Section 2.1 of [RFC9256] Section 2.1.

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

If the a PCEP speaker receives an SRPA object whose Association Parameters do not follow the above specification, then the PCEP speaker MUST send a PCErr message with Error-Type = 26 "Association

Commenté [MB26]: Please double check

Commenté [MB27]: Isn't this redundant with the bullets right after? I think so.

Commenté [MB28]: Not sure why this citation is needed.

Commenté [MB29]: No need to repeat this as that is clear in 6.1. of RFC8697

Commenté [MB30]: ??

Commenté [MB31]: As that one is optional in rfc8697, I think the wording should be clear this is for SR policy context

Commenté [MB32]: Point to 2.1 of 9256

Error", Error-Value = 20 "SR Policy Identifier Mismatch".

~~The purpose of choosing~~The encoding choice of the Association Parameters in this way is~~ meant~~ to guarantee that there is no possibility of a race condition when multiple PCEP speakers want to associate 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 based on the SR Policy ~~[RFC9256]~~ parameters [RFC9256]. ~~Thus, there is no chance that different PCEP speakers will come up with different Association Parameters for the same SR Policy.~~

The last hop of ~~the~~ a computed 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~~ be forwarded the rest of the ~~way~~ path 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~~headend to steer traffic with that Endpoint IP address into the SR Policy. The Destination of ~~the~~ a SR Policy Candidate Path is signaled using the END-POINTS object and/or LSP-IDENTIFIERS TLV, ~~as~~ per the usual PCEP ~~Procedures~~procedure. When neither the END-POINTS object nor LSP-IDENTIFIERS TLV is present, the PCEP speaker MUST extract the destination from the Endpoint field in the SRPA Extended Association ID TLV.

SR Policy with Color-Only steering is signaled with the ~~End-Point~~Endpoint value set to unspecified~~null~~, i.e., 0.0.0.0 for IPv4 or :: for IPv6 per~~, see~~ Section 8.8.1 of [RFC9256] ~~Section 8.8.1~~.

4.2. Association Information

The SRPA object may carry the following TLVs:

* SRPOLICY-POL-NAME TLV (Section 4.2.1): (optional) encodes the SR Policy Name string.

* SRPOLICY-CPATH-ID TLV (Section 4.2.2): (mandatory) encodes the SR Policy Candidate Path Identifier.

* SRPOLICY-CPATH-NAME TLV (Section 4.2.3): (optional) encodes the SR Policy Candidate Path string name.

* SRPOLICY-CPATH-PREFERENCE TLV (Section 4.2.4): (optional) encodes the SR Policy Candidate Path preference value.

~~Out of these TLVs, the SRPOLICY-CPATH-ID TLV is mandatory, all others~~

Commenté [MB33]: Assuming consistent instructions trigger the association. Otherwise, I think some elaboration is needed here.

Commenté [MB34]: Otherwise, I don't parse this.

~~are optional.~~ When a mandatory TLV is missing from ~~the~~ an SRPA object,
the PCEP speaker MUST send a PCErr message with Error-Type = 6 "Mandatory Object Missing", Error-Value = 21 "Missing SR Policy Mandatory TLV".

~~This document specifies four new TLVs to be carried in the SRPA object.~~ Only one TLV instance of each TLV type can be carried in an SRPA object, and only the first occurrence is processed. Any others MUST be silently ignored.

4.2.1. SR Policy Name TLV

The SRPOLICY-POL-NAME TLV (Figure 2) is an optional TLV for the SRPA object.

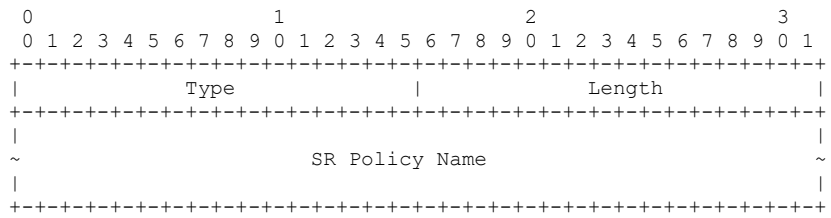


Figure 2: ~~The~~ SRPOLICY-POL-NAME TLV ~~f~~format

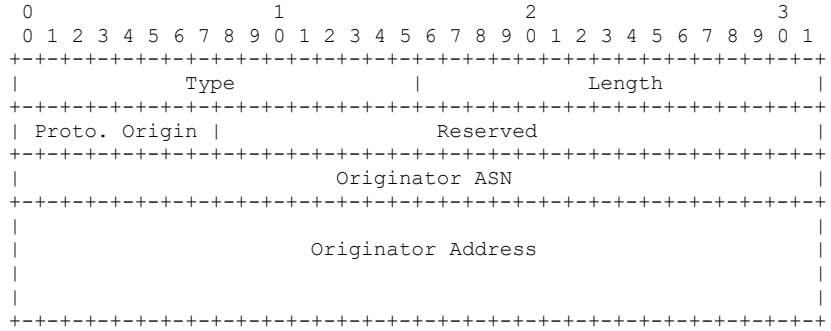
Type: 56 for "SRPOLICY-POL-NAME" TLV.

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 Section 2.1 [RFC9256]. It MUST be a string of printable ASCII characters, without a NULL terminator.

4.2.2. SR Policy Candidate Path Identifier TLV

The SRPOLICY-CPATH-ID TLV (Figure 3) is a mandatory TLV for the SRPA object.



Commenté [MB35]: Redundant with the description above.

Commenté [MB36]: Already listed in the preamble of this section

Commenté [MB37]: Should any of these be logged?

Commenté [MB38]: !! The SR policy BGP spec includes

«It is RECOMMENDED that the size of the symbolic name for the SR Policy is limited to 255 bytes. Implementations MAY choose to truncate long names to 255 bytes when signaling via BGP.¶»

I guess we should be consistent and align the various pieces, unless there are specifics to a given signaling mechanism.

This is even important given that some computed paths will be passed between the two:

«Typically, but not limited to, an SR Policy is computed by a controller or a path computation engine (PCE) and originated by a BGP speaker on its behalf.¶»

Commenté [MB39]: Should we remind that padding is not included in the Length field?

Commenté [MB40]: Please cite STD 80

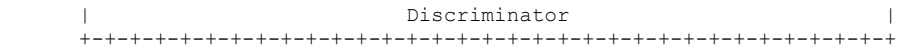


Figure 3: ~~The~~ SRPOLICY-CPATH-ID TLV F~~f~~ormat

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

Length: 28.

Protocol Origin: 8-bit value that encodes the protocol origin, as specified in Section 6.5. Note that in the PCInitiate message [RFC8281], the Protocol Origin is always set to 10 - "PCEP (In PCEP or when BGP-LS Producer is PCE)". The "SR Policy Protocol Origin" IANA registry includes a combination of values intended for use in PCEP and BGP-LS. When the registry contains two variants of values associated with the mechanism or protocol used for provisioning of the Candidate Path, for example 1 - "PCEP" and 10 - "PCEP (In PCEP or when BGP-LS Producer is PCE)", the "(In PCEP or when BGP-LS Producer is PCE)" variants MUST be used in PCEP.

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

Originator Autonomous System Number (ASN): Represented as a 4-byte number, part of the originator identifier, as specified in Section 2.4 of [RFC9256]. When sending a PCInitiate message [RFC8281], the PCE is the originator of the Candidate Path. ~~AS number~~ ASN is not a PCE concept and PCE is not required to have one for itself. If the PCE ~~has its As~~is configured with an ASN ~~number~~, then it MUST set it, otherwise the ~~AS number~~ASN ~~can be~~is set to 0.

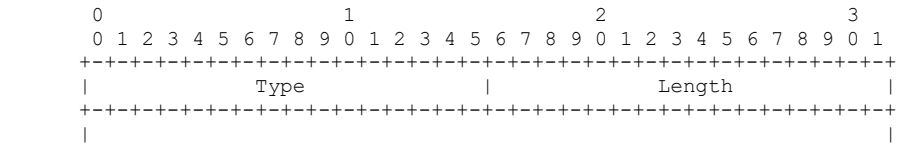
Commenté [MB41]: We may delete this.

Originator Address: Represented as a 128-bit value as specified in Section 2.4 of [RFC9256]. When sending a PCInitiate message, the PCE is acting as the originator and, therefore, MUST set this to an address that it owns.

Discriminator: 32-bit value that encodes the Discriminator of the Candidate Path, as specified in Section 2.5 of [RFC9256] ~~Section 2.5~~. 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 (Figure 4) is an optional TLV for the SRPA object.



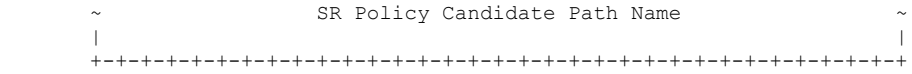


Figure 4: ~~The~~ SRPOLICY-CPATH-NAME TLV f~~f~~ormat

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.

SR Policy Candidate Path Name: SR Policy Candidate Path Name, as defined in Section 2.6 of [RFC9256]. It MUST be a string of printable ASCII characters, without a NULL terminator.

Commenté [MB42]: !! The BGP spec has the following «It is RECOMMENDED that the size of the symbolic name for the candidate path is limited to 255 bytes. Implementations MAY choose to truncate long names to 255 bytes when signaling via BGP. »

I guess we should be consistent

4.2.4. SR Policy Candidate Path Preference TLV

The SRPOLICY-CPATH-PREFERENCE TLV (Figure 5) is an optional TLV for the SRPA object. If the TLV is absent, then default Preference value is 100, ~~as~~ per Section 2.7 of [RFC9256].

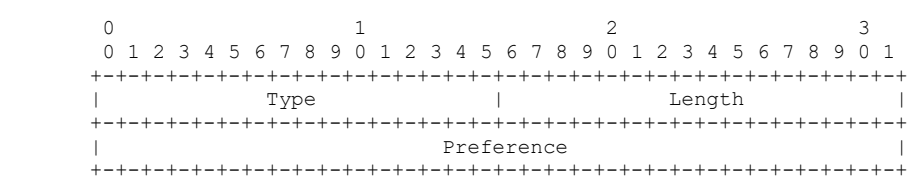


Figure 5: ~~The~~ SRPOLICY-CPATH-PREFERENCE TLV F~~f~~ormat

Type: 59 for "SRPOLICY-CPATH-PREFERENCE" TLV.

Length: 4.

Preference: Numerical preference of the Candidate Path as defined in Section 2.7 of [RFC9256].

5. Other Mechanisms

Commenté [MB43]: A more explicit title would be helpful.

BTW, the flow would be better if we first introduced the capabilities/session establishment and then SRPA signaling

This section describes mechanisms that are standardized for SR Policies in [RFC9256], but do not make use of the SRPA for signaling in PCEP. Since SRPA is not used, there needs to be a separate capability negotiation.

Commenté [MB44]: I don't parse this.

This document specifies four new TLVs to be carried in the OPEN or LSP object. Only one TLV instance of each type can be carried, and only the first occurrence is processed. Any others MUST be ignored.

5.1. SR Policy Capability TLV

The SRPOLICY-CAPABILITY TLV (Figure 6) is a TLV for the OPEN object. It is used at session establishment to learn the peer's capabilities with respect to SR Policy. Implementations that support SR Policy MUST

include SRPOLICY-CAPABILITY TLV in the OPEN object. In addition, the ASSOC-Type-List TLV containing SRPA Type (6) MUST be present in the OPEN object, as specified in Section 4.

If a PCEP speaker receives SRPA but the SRPOLICY-CAPABILITY TLV is not exchanged, then the PCEP speaker MUST send a PCErr message with Error- Type = 10 ("Reception of an invalid object") and Error-Value = TBD ("Missing SRPOLICY-CAPABILITY TLV") and MUST then close the PCEP session.

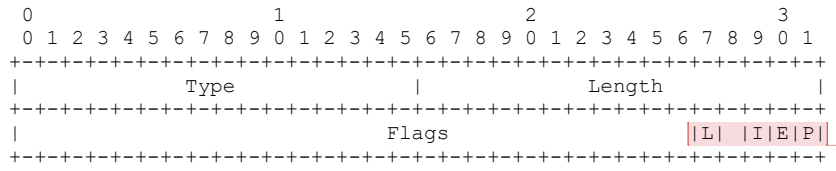


Figure 6: ~~The~~ SRPOLICY-CAPABILITY TLV ~~format~~Format

Type: 71 for "SRPOLICY-CAPABILITY TLV.

Length: 4.

P-flag (Computation Priority): If set to '1' by a PCEP speaker, the P flag indicates that the PCEP speaker supports the handling of COMPUTATION-PRIORITY TLV for the SR Policy~~, see~~ (~~Section~~ 5.2). If this flag is not set, then the receiving PCEP speaker MUST NOT send the COMPUTATION-PRIORITY TLV and MUST ignore it on receipt.

E-Flag (Explicit NULL Label Policy): If set to '1' by a PCEP speaker, the E flag indicates that the PCEP speaker supports the handling of Explicit Null Label Policy (ENLP)~~ENLP~~ TLV for the SR Policy (~~, see~~ Section 5.3). If this flag is not set, then the PCEP speaker MUST NOT send the ENLP TLV and MUST ignore it on receipt.

I-Flag (Invalidation): If set to '1' by a PCEP speaker, the I flag indicates that the PCEP speaker supports the handling of INVALIDATION TLV for the SR Policy~~, see~~ (~~Section~~ 5.4). If this flag is not set, then the PCEP speaker MUST NOT send the INVALIDATION TLV and MUST ignore it on receipt.

L-Flag (Stateless Operation): If set to '1' by a PCEP speaker, the L flag indicates that the PCEP speaker supports the stateless (PCReq/ PCRep) operations for the SR Policy~~, see~~ (~~Section~~ 5.5). If the PCE did not set this flag, then the PCC MUST NOT send PCReq messages to this PCE for the SR Policy.

Unassigned bits MUST be set to '0' on transmission and MUST be ignored on receipt.

5.2. Computation Priority TLV

Commenté [MB45]: ! Shouldn't this be conditioned by the activation to use the feature?

Commenté [MB46]: I guess we should log this.

Idem for similar constructs

Commenté [MB47]: Any reason non contiguous bits were used for these flags?

Commenté [MB48]: ! To demux which speaker we are talking about.

Please check other similar statements in the subsequent part. Thanks.

a mis en forme : Surlignage

The COMPUTATION-PRIORITY TLV (Figure 7) is an optional TLV for the LSP object.

It is used to signal the numerical computation priority, as specified in Section 2.12 of [RFC9256]. If the TLV is absent from the LSP object and the P-flag in the SRPOLICY-CAPABILITY TLV is set to 1, a default Priority value of 128 is used.

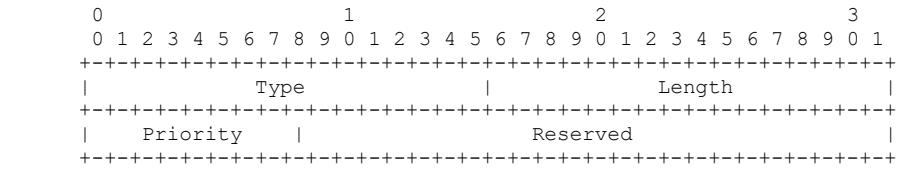


Figure 7: ~~The~~ COMPUTATION-PRIORITY TLV ~~format~~Format

Type: 68 for "COMPUTATION-PRIORITY" TLV.

Length: 4.

Priority: Numerical priority with which this LSP is to be recomputed by the PCE upon topology change. Lowest value is the highest priority. The default value of priority is 128 (if this TLV is absent), see Section 2.12 of [RFC9256].

Commenté [MB49]: Already stated right before the figure

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

5.3. Explicit Null Label Policy (ENLP) TLV

To steer an unlabeled IP packet into an SR policy, it is necessary to create a label stack for that packet, and push one or more labels onto that stack. The Explicit NULL Label Policy (ENLP) TLV is an optional TLV for the LSP object used to indicate whether an Explicit NULL Label [RFC3032] must be pushed on an unlabeled IP packet before any other labels. The contents of this TLV are used by the SRPM as described in ~~section~~ Section 4.1 of [RFC9256]. If an ENLP TLV is not present, the decision of whether to push an Explicit NULL label on a given packet is a matter of local configuration. Note that Explicit Null is currently only defined for SR MPLS and not for SRv6. Therefore, ~~Therefore~~ the PCEP speaker MUST ignore the presence of this TLV for SRv6 Policies.

Commenté [MB50]: ! Does it make sense for SRv6?

I would align the description with draft-ietf-idr-segment-routing-te-policy

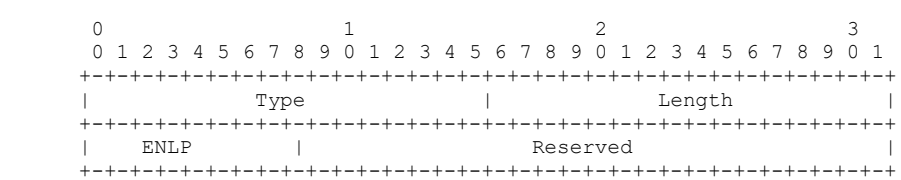


Figure 8: The Explicit Null Label Policy (ENLP) TLV format

Type: 69 for "ENLP" TLV.

Length: 4.

ENLP (Explicit NULL Label Policy): Indicates whether Explicit NULL labels are to be pushed on unlabeled IP packets that are being steered into a given SR policy. The values of this field are specified in IANA registry "SR Policy ENLP Values" under "Segment Routing" registry group, which was introduced in Section 6.10 of [I-D.ietf-idr-sr-policy-safi].

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

The ENLP reserved values may be used for future extensions and implementations MUST ignore the ENLP TLV with these values. The behavior signaled in this TLV MAY be overridden by local configuration. Section 4.1 of [RFC9256] describes the behavior on the headend for the handling of the explicit null label.

5.4. Invalidation TLV

The INVALIDATION TLV (Figure 9) is an optional TLV for the LSP object.

~~It~~ This TLV is used to control traffic steering into ~~the~~ an LSP 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 would have been destined for that LSP is redirected somewhere else, such as via IGP or 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 whether to enable or disable Drop-upon-invalid (Config).

* PCC -> PCE: PCC reports the current setting of the Drop-upon-invalid (Config) and also whether the LSP is currently in the drop state (Oper).

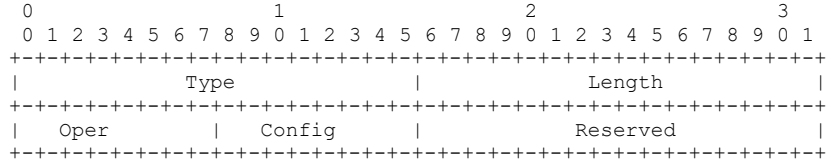


Figure 9: ~~The~~ INVALIDATION TLV ~~F~~format

Type: 70 for "INVALIDATION" TLV.

Length: 4.

Oper: encodes the current state of the LSP, i.e., whether it is actively dropping traffic right now. This field can be set to non-zero values only by the PCC, it MUST be set to 0 by the PCE and MUST be ignored by the PCC. See Section ~~Section~~ 6.6 for IANA information.

Commenté [MB51]: A better description is needed to reflect the use of the oper status.

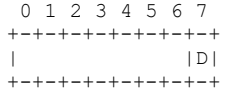


Figure 10: Oper state of Drop-upon-invalid feature

* D: dropping - the LSP is currently attracting traffic and actively dropping it.

* The unassigned bits in the Flag octet MUST be set to zero upon transmission and MUST be ignored upon receipt.

Config: encodes the current setting of the Drop-upon-invalid feature. See Section ~~Section~~ 6.7 for IANA information.

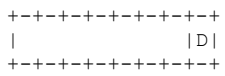


Figure 11: Config state of Drop-upon-invalid feature

* D: drop enabled - the Candidate Path has Drop-upon-invalid feature enabled.

* The unassigned bits in the Flag octet MUST be set to zero upon transmission and MUST be ignored upon receipt.

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

5.4.1. Drop-upon-invalid applies to SR Policy

The Drop-upon-invalid feature is somewhat special among the other SR Policy features in the way that it is enabled/disabled. This feature is enabled only on the whole SR Policy, not on a particular Candidate Path of that SR Policy, i.e., when any Candidate Path has Drop-upon-invalid enabled, it means that the whole SR Policy has the feature enabled. As stated in Section 8.1 of [RFC9256] ~~Section 8.1~~, ~~the~~ an SR Policy is invalid when all its Candidate Paths are invalid.

Once all the Candidate Paths of ~~the~~ an SR Policy have become invalid, then the SR Policy checks whether any of the Candidate Paths have Drop-upon-invalid enabled. If so, the SR Policy enters the drop state and "activates" the highest preference Candidate Path which has the Drop-upon-invalid enabled. Note that only one Candidate Path needs to be reported to the PCE with the D (dropping) flag set.

5.5. Update to RFC 8231

Section 5.8.2 of [RFC8231] ~~Section 5.8.2~~, allows delegation of an LSP in operationally down state, but at the same time mandates the use of PCReq before sending PCRpt. This document updates Section 5.8.2 of [RFC8231] ~~Section 5.8.2~~, by making ~~this~~ that section of [RFC8231] not applicable to SR Policy LSPs. Thus, when a PCC wants to delegate an SR Policy LSP, it MAY proceed directly to sending PCRpt, without first sending PCReq and waiting for PCRep. This has the advantage of reducing the number of PCEP messages and simplifying the implementation.

Furthermore, a PCEP speaker is not required to support PCReq/PCRep at all for SR Policies. The PCEP speaker can indicate support for PCReq/PCRep via the "L-Flag" in the SRPOLICY-CAPABILITY TLV (See Section 5.1). When this flag is cleared, or when the SRPOLICY-CAPABILITY TLV is absent, the given peer MUST NOT be sent PCReq/PCRep messages for SR Policy LSPs. Conversely, when this flag is set, the peer can receive and process PCReq/PCRep messages for SR Policy LSPs.

The above applies only to SR Policy LSPs and does not affect other LSP types, such as RSVP-TE LSPs. For other LSP types, Section 5.8.2 of [RFC8231] ~~Section 5.8.2~~ continues to apply.

6. IANA Considerations

6.1. Association Type

This document defines a new association type: SR Policy Association. IANA is requested to confirm the following allocation in the "ASSOCIATION Type Field" registry ~~[RFC8697]~~ within the "Path Computation Element Protocol (PCEP) Numbers" registry group:

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

Commenté [MB52]: The registry url should be provided instead

6.2. PCEP TLV Type Indicators

This document defines eight new TLVs for carrying additional information about SR Policy and SR Candidate Paths. IANA is requested to confirm the following allocations in 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

68	COMPUTATION-PRIORITY	This.I-D
69	EXPLICIT-NULL-LABEL-POLICY	This.I-D
70	INVALIDATION	This.I-D
71	SRPOLICY-CAPABILITY	This.I-D

6.3. PCEP Errors

This document defines one new Error-Value within the "Mandatory Object Missing" Error-Type, two new Error-Values within the "Association Error" Error-Type and one new Error-Value within the "Reception of an invalid object".

IANA is requested to confirm the following allocations within the "PCEP-ERROR Object Error Types and Values" registry of the "Path Computation Element Protocol (PCEP) Numbers" registry group.

Error-Type	Meaning	Error-value	Reference
6	Mandatory Object Missing		[RFC5440]
		21: Missing SR Policy Mandatory TLV	This.I-D
26	Association Error		[RFC8697]
		20: SR Policy Identifers Mismatch	This.I-D
		21: SR Policy Candidate Path Identifier Mismatch	This.I-D

IANA is requested to make new allocations within the "PCEP-ERROR Object Error Types and Values" registry of the "Path Computation Element Protocol (PCEP) Numbers" registry group.

Error-Type	Meaning	Error-value	Reference
10	Reception of an invalid object		[RFC5440]
		TBA: Missing SRPOLICY-CAPABILITY TLV	This.I-D

6.4. TE-PATH-BINDING TLV Flag field

An earlier version of this document added new bit within the "TE-

PATH-BINDING TLV Flag field" registry of the "Path Computation Element Protocol (PCEP) Numbers" registry group, which was also early allocated by the IANA.

IANA is requested to cancel the early allocation made which is not needed anymore. As per the instructions from the chairs, please mark it as deprecated.

Bit position	Description	Reference
1	Deprecated (Specified-BSID-only)	This.I-D

6.5. SR Policy Candidate Path Protocol Origin field

[Note to IANA: The new registry creation request below is also present in the draft-ietf-idr-bgp-ls-sr-policy. IANA is requested to process the registry creation via the first of these two documents to reach the publication stage and the authors of the other document would update the IANA considerations suitably. Note that draft-ietf-idr-bgp-ls-sr-policy allocates different values in BGP.] [Note to RFC-Editor: Please remove the above and this note before publication.]

Commenté [MB53]: As that doc is in the RFC editor queue, may be it is time to delete this request

This document requests IANA to maintain a new registry under "Segment Routing" registry group. The new registry is called "SR Policy Protocol Origin". New values are to be assigned by "Expert Review" [RFC8126] using the guidelines for Designated Experts as specified in [RFC9256]. The registry contains the following codepoints:

Code Point	Protocol Origin	Reference
0	Reserved (not to be used)	this document
1	PCEP	this document
2	BGP SR Policy	this document
3	Configuration (CLI, YANG model via NETCONF, etc.)	this document
4-9	Unassigned	this document
10	PCEP (In PCEP or when BGP-LS Producer is PCE)	this document
11-19	Unassigned	this document
20	BGP SR Policy (In PCEP or when BGP-LS Producer is PCE)	this document
21-29	Unassigned	this document
30	Configuration (CLI, YANG model via NETCONF, etc.) (In PCEP or when BGP-LS Producer is PCE)	this document
31-250	Unassigned	this document
251-255	Private Use (not to be assigned by IANA)	this document

6.6. SR Policy Invalidation Operational State

This document requests IANA to maintain a new registry under "Path

Computation Element Protocol (PCEP) Numbers" registry group. The new registry is called "SR Policy Invalidation Operational Flags". New values are to be assigned by "IETF review" [RFC8126]. Each bit should be tracked with the following qualities:

* Bit (counting from bit 0 as the most significant bit).

* Description.

* Reference.

Bit	Description	Reference
0 - 6	Unassigned	This.I-D
7	D: dropping - the LSP is currently attracting traffic and actively dropping it.	This.I-D

6.7. SR Policy Invalidation Configuration State

This document requests IANA to maintain a new registry under "Path Computation Element Protocol (PCEP) Numbers" registry group. The new registry is called "SR Policy Invalidation Configuration Flags". New values are to be assigned by "IETF review" [RFC8126]. Each bit should be tracked with the following qualities:

* Bit (counting from bit 0 as the most significant bit).

* Description.

* Reference.

Bit	Description	Reference
0 - 6	Unassigned.	This.I-D
7	D: drop enabled - the Drop-upon-invalid is enabled on the LSP.	This.I-D

6.8. SR Policy Capability TLV Flag field

This document requests IANA to maintain a new registry under "Path Computation Element Protocol (PCEP) Numbers" registry group. The new registry is called "SR Policy Capability TLV Flag Field". New values are to be assigned by "IETF review" [RFC8126]. Each bit should be tracked with the following qualities:

* Bit (counting from bit 0 as the most significant bit).

* Description.

* Reference.

Bit	Description	Reference
0 - 26	Unassigned	This.I-D
27	Stateless Operation	This.I-D
28	Unassigned	This.I-D
29	Invalidation	This.I-D
30	Explicit NULL Label Policy	This.I-D
31	Computation Priority	This.I-D

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: ssidor@cisco.com

7.2. Juniper

* Organization: Juniper Networks

* Implementation: PCC and PCE.

* Description: Everything in -05 except SR Policy Name TLV and SR Policy Candidate Path Name TLV.

* Maturity Level: Production.

* Coverage: Partial.

* Contact: cbarth@juniper.net

8. Security Considerations

The information carried in the newly defined SRPA object and TLVs could provide an eavesdropper with additional information about the SR Policy.

The security considerations described in [RFC5440], [RFC8231], [RFC8281], [RFC8664], [RFC8697], [RFC9256] and [RFC9603] are applicable to this specification.

As per [RFC8231], it is RECOMMENDED that these PCEP extensions can only be activated on authenticated and encrypted sessions across PCEs and PCCs belonging to the same administrative authority, using Transport Layer Security (TLS) [RFC8253] as per the recommendations and best current practices in [RFC9325].

9. Manageability Considerations

All manageability requirements and considerations listed in [RFC5440], [RFC8231], [RFC8664], [RFC9256], and [RFC9603] apply to PCEP protocol extensions defined in this document. In addition, requirements and considerations listed in this section apply.

9.1. Control of Function and Policy

A PCE or PCC implementation MAY allow the capabilities specified in Section 5.1 and the capability for support of SRPA advertised in ASSOC-Type-List TLV to be enabled and disabled.

9.2. ~~Information and~~ Data Models

~~The PCEP YANG module [I-D.ietf-pce-pcep-yang] will be extended with PCEP extensions specified Section 5 of this document.~~
[I-D.ietf-pce-pcep-srv6-yang] defines YANG module with common building blocks for PCEP Extensions described in Section 4.

9.3. 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], [RFC8664], and [RFC9256].

9.4. Verify Correct Operations

Operation verification requirements already listed in [RFC5440], [RFC8231], [RFC8664], [RFC9256], and [RFC9603] are applicable to

mechanisms defined in this document.

An implementation MUST allow the operator to view SR Policy Identifier and SR Policy Candidate Path Identifier advertised in SRPA object.

An implementation SHOULD allow the operator to view the capabilities defined in this document.

An implementation SHOULD allow the operator to view LSPs associated with specific SR Policy Identifier.

9.5. Requirements On Other Protocols

The PCEP extensions defined in this document do not imply any new requirements on other protocols.

9.6. Impact On Network Operations

The mechanisms defined in [RFC5440], [RFC8231], [RFC9256], and [RFC9603] also apply to the PCEP extensions defined in this document.

10. Acknowledgement

Would like to thank Ketan Talaulikar, Dhruv Dhody, Stephane Litkowski, Boris Khasanov, Abdul Rehman, Zoey Rose, Praveen Kumar and Tom Petch for review and suggestions.

11. References

11.1. 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>.

[RFC3032] Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T., and A. Conta, "MPLS Label Stack Encoding", RFC 3032, DOI 10.17487/RFC3032, January 2001, <https://www.rfc-editor.org/info/rfc3032>.

[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>.

[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>.

[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

Commenté [MB54]: What does that mean?

Commenté [MB55]: There are bunch of extensions that are defined out there for SR policy purposes (BGP, for example).

Any considerations about co-existence and interactions between those?

It is tempting to have a mapping between the various objects to make sure that a feature parity (or no) is supported.

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>.

[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>.

[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>.

[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>.

[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>.

[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>.

[RFC9325] Sheffer, Y., Saint-Andre, P., and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 9325, DOI 10.17487/RFC9325, November 2022, <https://www.rfc-editor.org/info/rfc9325>.

[RFC9603] Li, C., Ed., Kaladharan, P., Sivabalan, S., Koldychev, M., and Y. Zhu, "Path Computation Element Communication Protocol (PCEP) Extensions for IPv6 Segment Routing", RFC 9603, DOI 10.17487/RFC9603, July 2024, <https://www.rfc-editor.org/info/rfc9603>.

[I-D.ietf-idr-sr-policy-safi] Previdi, S., Filsfils, C., Talaulikar, K., Mattes, P., and D. Jain, "Advertising Segment Routing Policies in BGP", Work in Progress, Internet-Draft, draft-ietf-idr-sr-policy-safi-13, 6 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-idr-sr-policy-safi-13>.

Commenté [MB56]: This is informative.

11.2. Informative References

[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-12, 8 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-pce-multipath-12>.

[RFC9604] Sivabalan, S., Filsfils, C., Tantsura, J., Previdi, S., and C. Li, Ed., "Carrying Binding Label/SID in PCE-Based Networks", RFC 9604, DOI 10.17487/RFC9604, August 2024, <https://www.rfc-editor.org/info/rfc9604>.

[I-D.ietf-pce-pcep-yang]
Dhody, D., Beeram, V. P., Hardwick, J., and J. Tantsura, "A YANG Data Model for Path Computation Element Communications Protocol (PCEP)", Work in Progress, Internet-Draft, draft-ietf-pce-pcep-yang-30, 26 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pce-pcep-yang-30>.

[I-D.ietf-pce-pcep-srv6-yang]
Li, C., Sivabalan, S., Peng, S., Koldychev, M., and L. Ndifor, "A YANG Data Model for Segment Routing (SR) Policy and SR in IPv6 (SRv6) support in Path Computation Element Communications Protocol (PCEP)", Work in Progress, Internet-Draft, draft-ietf-pce-pcep-srv6-yang-06, 19 October 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-pce-pcep-srv6-yang-06>.

Appendix A. Contributors

Dhruv Dhody
Huawei
India

Email: dhruv.ietf@gmail.com

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

Email: chengli13@huawei.com

Zafar Ali
Cisco Systems, Inc.

Email: zali@cisco.com

Rajesh Melarcode
Cisco Systems, Inc.
2000 Innovation Dr.

Kanata, Ontario
Canada

Email: rmelarco@cisco.com

Authors' Addresses

Mike Koldychev
Ciena Corporation
385 Terry Fox Dr.
Kanata Ontario K2K 0L1
Canada
Email: mkoldych@proton.me

Siva Sivabalan
Ciena Corporation
385 Terry Fox Dr.
Kanata Ontario K2K 0L1
Canada
Email: ssivabal@ciena.com

Samuel Sidor
Cisco Systems, Inc.
Eurovea Central 3.
811 09 Bratislava
Slovakia
Email: ssidor@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