Authors:

C. Li   H. Zheng   S. Sivabalan   S. Sidor
Huawei Technologies   *Huawei Technologies*   *Ciena*   *Cisco Systems, Inc.*

Z. Ali
Cisco Systems, Inc.

RFC 9752
Conveying Vendor-Specific Information in the Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE

Abstract

This document specifies extensions to the Path Computation Element Communication Protocol (PCEP) that enable the inclusion of vendor-specific information in stateful Path Computation Element (PCE) operations. These extensions allow vendors to incorporate proprietary data within PCEP messages, facilitating enhanced network optimization and functionality in environments requiring vendor-specific features. The extensions maintain compatibility with existing PCEP implementations and promote interoperability across diverse network deployments. RFC 7470 defines a facility to carry vendor-specific information in stateless PCEP messages. This document extends this capability for the Stateful PCEP messages.

This document updates RFC 7470 to revise the reference to the IANA registry for managing Enterprise Numbers.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9752.

Copyright Notice

Table of Contents

1. Introduction

The Path Computation Element Communication Protocol (PCEP) [RFC5440] provides mechanisms for a Path Computation Element (PCE) to perform path computation in response to a Path Computation Client (PCC) request.

A Stateful PCE is capable of considering, for the purposes of path computation, not only the network state in terms of links and nodes (referred to as the Traffic Engineering Database or TED) but also the status of active services (previously computed paths, and currently reserved

resources, stored in the Label Switched Paths Database (LSP-DB)). [RFC8051] describes general considerations for a Stateful PCE deployment and examines its applicability and benefits, as well as its challenges and limitations through a number of use cases.

[RFC8231] describes a set of extensions to PCEP to provide stateful control. A Stateful PCE has access to not only the information carried by the network's Interior Gateway Protocol (IGP), but also the set of active paths and their reserved resources for its computations. The additional state allows the PCE to compute constrained paths while considering individual LSPs and their interactions. [RFC8281] describes the setup, maintenance, and teardown of PCE-initiated LSPs under the Stateful PCE model. These extensions add new messages in PCEP for Stateful PCE.

[RFC7470] defines the Vendor Information object, which can carry arbitrary, proprietary information, such as vendor-specific constraints, in stateless PCEP. It also defines the VENDOR-INFORMATION-TLV, which allows arbitrary information to be embedded within any existing or future PCEP object that supports TLVs.

While originally designed for stateless PCEP, the Vendor Information object and VENDOR-INFORMATION-TLV are also useful in the Stateful PCE model. The VENDOR-INFORMATION-TLV can already be included in any of the stateful PCEP objects per [RFC7470]. This document further extends stateful PCEP messages to support the use of the Vendor Information object.

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.

1.2. Use of RBNF

The message formats in this document are illustrated using Routing Backus-Naur Form (RBNF) encoding, as specified in [RFC5511]. The use of RBNF is illustrative only and may omit certain important details; the normative specification of messages is found in the descriptive text. If there is any divergence between the RBNF and the descriptive text, the descriptive text is considered authoritative.

2. Procedures for the Vendor Information Object

A Path Computation LSP State Report message (also referred to as PCRpt message; see Section 6.1 of [RFC8231]) is a PCEP message sent by a PCC to a PCE to report the current state of an LSP. A PCC that wants to convey proprietary or vendor-specific information or metrics to a PCE does so by including a Vendor Information object in the PCRpt message. The contents and format of the object, including the VENDOR-INFORMATION object and the VENDOR-INFORMATION-TLV, are described in Section 4 of [RFC7470]. The PCE determines how to interpret the information in the Vendor Information object by examining the Enterprise Number it contains.

[RFC7470] stated that:

> Enterprise Numbers are assigned by IANA and managed through an IANA registry [RFC2578].

This document updates [RFC7470] and replaces this text with:

> Enterprise Numbers are assigned by IANA and managed through the "Private Enterprise Numbers (PENs)" registry as described in [RFC9371].

The Vendor Information object is **OPTIONAL** in a PCRpt message. Multiple instances of the object **MAY** be contained in a single PCRpt message. Different instances of the object **MAY** have different Enterprise Numbers.

The format of the PCRpt message (with Section 6.1 of [RFC8231] as the base) is updated as follows:

```
<PCRpt Message> ::= <Common Header>
                    <state-report-list>
```

Where:

```
<state-report-list> ::= <state-report>[<state-report-list>]

<state-report> ::= [<SRP>]
                   <LSP>
                   <path>
                   [<vendor-info-list>]
```

Where:

```
<vendor-info-list> ::= <VENDOR-INFORMATION>
                       [<vendor-info-list>]

<path> is defined in [RFC8231].
```

A Path Computation LSP Update Request message (also referred to as PCUpd message; see Section 6.2 of [RFC8231]) is a PCEP message sent by a PCE to a PCC to update the attributes of an LSP. The Vendor Information object can be included in a PCUpd message to convey proprietary or vendor-specific information.

The format of the PCUpd message (with Section 6.2 of [RFC8231] as the base) is updated as follows:

```
    <PCUpd Message> ::= <Common Header>
                        <update-request-list>
```

Where:

```
   <update-request-list> ::= <update-request>
                        [<update-request-list>]

   <update-request> ::= <SRP>
                        <LSP>
                        <path>
                        [<vendor-info-list>]
```

Where:

```
   <vendor-info-list> ::= <VENDOR-INFORMATION>
                          [<vendor-info-list>]

   <path> is defined in [RFC8231].
```

A Path Computation LSP Initiate Message (also referred to as PCInitiate message; see Section 5.1 of [RFC8281]) is a PCEP message sent by a PCE to a PCC to trigger an LSP instantiation or deletion. The Vendor Information object can be included in a PCInitiate message to convey proprietary or vendor-specific information.

The format of the PCInitiate message (with Section 5.1 of [RFC8281] as the base) is updated as follows:

```
   <PCInitiate Message> ::= <Common Header>
                            <PCE-initiated-lsp-list>
```

Where:

```
   <PCE-initiated-lsp-list> ::= <PCE-initiated-lsp-request>
                             [<PCE-initiated-lsp-list>]

   <PCE-initiated-lsp-request> ::=
                        (<PCE-initiated-lsp-instantiation>|
                         <PCE-initiated-lsp-deletion>)

   <PCE-initiated-lsp-instantiation> ::= <SRP>
                                         <LSP>
                                         [<END-POINTS>]
                                         <ERO>
                                         [<attribute-list>]
                                         [<vendor-info-list>]
```

Where:

```
        <vendor-info-list> ::= <VENDOR-INFORMATION>
                               [<vendor-info-list>]
```

<PCE-initiated-lsp-deletion> and <attribute-list> are as defined in [RFC8281].

A legacy implementation that does not recognize the Vendor Information object will act according to the procedures set out in [RFC8231] and [RFC8281]. An implementation that supports the Vendor Information object, but receives one carrying an Enterprise Number that it does not support, **MUST** ignore the object in the same way as described in Section 2 of [RFC7470].

3. Procedures for the Vendor Information TLV

The Vendor Information TLV can be used to carry vendor-specific information that applies to a specific PCEP object by including the TLV in the object. This includes objects used in Stateful PCE extensions such as Stateful PCE Request Parameter (SRP) and LSP objects. All of the procedures are as described in Section 3 of [RFC7470].

4. Manageability Considerations

All manageability requirements and considerations listed in [RFC5440], [RFC7470], [RFC8231], and [RFC8281] apply to the PCEP protocol extensions defined in this document. In addition, the requirements and considerations listed in this section apply.

4.1. Control of Function and Policy

The requirements for control of function and policy for vendor-specific information as set out in [RFC7470] continue to apply to Stateful PCEP extensions specified in this document.

4.2. Information and Data Models

The PCEP YANG module is specified in [PCEP-YANG]. Any standard YANG module will not include details of vendor-specific information. However, a standard YANG module could be extended to report the use of the Vendor Information object or TLV and the Enterprise Numbers that the objects and TLVs contain.

4.3. 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].

4.4. Verifying Correct Operations

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

4.5. Requirements On Other Protocols

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

4.6. Impact on Network Operations

Mechanisms defined in [RFC5440] and [RFC8231] also apply to PCEP extensions defined in this document.

Section 6.6 of [RFC7470] highlights how the presence of additional vendor-specific information in PCEP messages may congest the operations and how to detect and handle it. This also applies to stateful PCEP messages as outlined in Section 2. Specifically, a PCEP speaker **SHOULD NOT** include vendor information in stateful PCEP message if it believes the recipient does not support that information.

Encoding optimization for the Vendor Information object, for example, in case the object has the same content encoded for multiple LSPs, is considered out of the scope of this document and may be proposed in the future as a separate document applicable to other PCEP objects.

5. IANA Considerations

This document has no IANA actions.

6. Security Considerations

The protocol extensions defined in this document do not change the nature of PCEP. Therefore, the security considerations set out in [RFC5440], [RFC7470], [RFC8231], and [RFC8281] apply unchanged.

As per [RFC8231], it is **RECOMMENDED** that these PCEP extensions only be activated on authenticated and encrypted sessions across PCEs and PCCs using Transport Layer Security (TLS) [RFC8253], as per the recommendations and best current practices in RFC 9325 [BCP195].

The use of vendor-specific information as defined in [RFC7470] and in this document may provide a covert channel that could be misused by PCEP speaker implementations or by malicious software at PCEP speakers. While there is limited protection against this, an operator monitoring the PCEP sessions can detect the use of vendor-specific information, be aware of the decoding mechanism for this data, and inspect it accordingly. It is crucial for the operator to remain vigilant and monitor for any potential misuse of this object. Appropriate steps need to be taken to prevent the installation of malicious software at the PCEP speaker by implementing robust integrity, authentication, and authorization techniques for installation and updating, which are out of scope of this document.

7. References

7.1. Normative References

[BCP195]   Best Current Practice 195, <https://www.rfc-editor.org/info/bcp195>.
At the time of writing, this BCP comprises the following:

Moriarty, K. and S. Farrell, "Deprecating TLS 1.0 and TLS 1.1", BCP 195, RFC 8996, DOI 10.17487/RFC8996, March 2021, <https://www.rfc-editor.org/info/rfc8996>.

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>.

[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>.

[RFC5511]   Farrel, A., "Routing Backus-Naur Form (RBNF): A Syntax Used to Form Encoding Rules in Various Routing Protocol Specifications", RFC 5511, DOI 10.17487/RFC5511, April 2009, <https://www.rfc-editor.org/info/rfc5511>.

[RFC7470]   Zhang, F. and A. Farrel, "Conveying Vendor-Specific Constraints in the Path Computation Element Communication Protocol", RFC 7470, DOI 10.17487/RFC7470, March 2015, <https://www.rfc-editor.org/info/rfc7470>.

[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>.

7.2. Informative References

[PCEP-YANG]

Dhody, D., Ed., 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>.

[RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, DOI 10.17487/RFC2578, April 1999, <https://www.rfc-editor.org/info/rfc2578>.

[RFC8051] Zhang, X., Ed. and I. Minei, Ed., "Applicability of a Stateful Path Computation Element (PCE)", RFC 8051, DOI 10.17487/RFC8051, January 2017, <https://www.rfc-editor.org/info/rfc8051>.

[RFC8253] Lopez, D., Gonzalez de Dios, O., Wu, Q., and D. Dhody, "PCEPS: Usage of TLS to Provide a Secure Transport for the Path Computation Element Communication Protocol (PCEP)", RFC 8253, DOI 10.17487/RFC8253, October 2017, <https://www.rfc-editor.org/info/rfc8253>.

[RFC9371] Baber, A. and P. Hoffman, "Registration Procedures for Private Enterprise Numbers (PENs)", RFC 9371, DOI 10.17487/RFC9371, March 2023, <https://www.rfc-editor.org/info/rfc9371>.

Acknowledgments

Contributors

Dhruv Dhody
Huawei
India
Email: dhruv.ietf@gmail.com

Mike Koldychev
Ciena
Email: mkoldych@proton.me

Authors' Addresses

Cheng Li
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing
100095
China
Email: c.l@huawei.com

Haomian Zheng
Huawei Technologies
H1, Huawei Xiliu Beipo Village, Songshan Lake
Dongguan
Guangdong, 523808
China
Email: zhenghaomian@huawei.com

Siva Sivabalan
Ciena
385 Terry Fox Drive
Kanata Ontario K2K 0L1
Canada
Email: msiva282@gmail.com

Samuel Sidor
Cisco Systems, Inc.
Email: ssidor@cisco.com

Zafar Ali
Cisco Systems, Inc.
Email: zali@cisco.com