PCE Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 5, 2021

C. Li
H. Zheng
Huawei Technologies
S. Sivabalan
Ciena
S. Sidor
Z. Ali
Cisco Systems, Inc.
November 1, 2020

Conveying Vendor-Specific Information in the Path Computation Element (PCE) Communication Protocol (PCEP) extensions for Stateful PCE. draft-dhody-pce-stateful-pce-vendor-11

Abstract

A Stateful Path Computation Element (PCE) maintains information on the current network state, including: computed Label Switched Path (LSPs), reserved resources within the network, and the pending path computation requests. This information may then be considered when computing new traffic engineered LSPs, and for the associated and the dependent LSPs, received from a Path Computation Client (PCC).

RFC 7470 defines a facility to carry vendor-specific information in Path Computation Element Communication Protocol (PCEP).

This document extends this capability for the Stateful PCEP messages.

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 May 5, 2021.

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 the 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 set up, maintenance and teardown of PCE-initiated LSPs under the Stateful PCE model. These extensions added new messages in PCEP for Stateful PCE.

[RFC7470] defined Vendor Information object that can be used to carry arbitrary, proprietary information such as vendor-specific constraints. It also defined VENDOR-INFORMATION-TLV that can be used to carry arbitrary information within any existing or future PCEP object that supports TLVs.

This document extend the usage of Vendor Information Object and VENDOR-INFORMATION-TLV to Stateful PCE. The VENDOR-INFORMATION-TLV can be carried inside any of the new objects added in PCEP for Stateful PCE as per [RFC7470], this document extend the stateful PCEP messages to also include the Vendor Information Object as well.

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. Procedures for the Vendor Information Object

A Path Computation LSP State Report message [RFC8231] (also referred to as PCRpt message) 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 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.

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

The format of the PCRpt message (with [RFC8231] as 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) is a PCEP message sent by a PCE to a PCC to update 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 [RFC8231] as 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) 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 [RFC8281] as 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> is as per [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 [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 extension such as SRP and LSP object. All the procedures as per section 3 of [RFC7470].

4. Vendor Information Object and TLV

[RFC7470] specify the format of VENDOR-INFORMATION Object and VENDOR-INFORMATION-TLV.

5. Manageability Considerations

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

5.1. Control of Function and Policy

As stated in [RFC7470], this capability, the associated vendor specific information and policy SHOULD made configurable. This information can be used in Stateful PCEP messages as well.

5.2. Information and Data Models

The PCEP YANG module is specified in [I-D.ietf-pce-pcep-yang]. It is NOT RECOMMENDED that standard YANG module be augmented with details of vendor information. It MAY be extended to include the use of this information and the Enterprise Numbers that the object and TLVs contain.

5.3. 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].

5.4. Verify Correct Operations

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

5.5. Requirements On Other Protocols

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

5.6. Impact On Network Operations

Mechanisms defined in [RFC5440] and [RFC8231] also apply to PCEP extensions defined in this document. Further, the mechanism described in this document can help the operator to request control of the LSPs at a particular PCE.

6. IANA Considerations

There are no IANA consideration in this document.

7. Implementation Status

[NOTE TO RFC EDITOR : This whole section and the reference to RFC 7942 is to be removed before publication as an RFC]

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 Systems

- Organization: Cisco Systems, Inc.
- Implementation: Cisco IOS-XR PCE and PCC
- Description: Vendor Information Object used in PCRpt, PCUpd and PCInitiate messages.
- Maturity Level: Production
- Coverage: Full
- Contact: ssidor@cisco.com

8. 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 stated in [RFC6952], PCEP implementations SHOULD support the TCP-AO [RFC5925] and not use TCP MD5 because of TCP MD5's known vulnerabilities and weakness. PCEP also support Transport Layer Security (TLS) [RFC8253] as per the recommendations and best current practices in [RFC7525].

9. Acknowledgments

Thanks to Avantika, Mahendra Singh Negi, Udayasree Palle and Swapna K for their 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>.

[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>.

10.2. Informative References

[I-D.ietf-pce-pcep-yang]
Dhody, D., Hardwick, J., Beeram, V., and J. Tantsura, "A YANG Data Model for Path Computation Element Communications Protocol (PCEP)", draft-ietf-pce-pcep-yang-15 (work in progress), October 2020.

[RFC5925] Touch, J., Mankin, A., and R. Bonica, "The TCP Authentication Option", RFC 5925, DOI 10.17487/RFC5925, June 2010, <https://www.rfc-editor.org/info/rfc5925>.

[RFC6952] Jethanandani, M., Patel, K., and L. Zheng, "Analysis of BGP, LDP, PCEP, and MSDP Issues According to the Keying and Authentication for Routing Protocols (KARP) Design Guide", RFC 6952, DOI 10.17487/RFC6952, May 2013, <https://www.rfc-editor.org/info/rfc6952>.

[RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <https://www.rfc-editor.org/info/rfc7525>.

[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>.

[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>.

Appendix A. Contributor Addresses

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

EMail: dhruv.ietf@gmail.com

Mike Koldychev
Cisco Systems
Kanata, Ontario
Canada

EMail: mkoldych@cisco.com

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
P.R.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