Workgroup: PCE Working Group
Internet-Draft: draft-dong-pce-pcep-nrp-00
Published: 11 March 2023
Intended Status: Standards Track
Expires: 12 September 2023
Authors: J. Dong
Huawei Technologies
S. Fang
Huawei Technologies
Q. Xiong
ZTE Corporation
S. Peng
ZTE Corporation
L. Han
China Mobile
M. Wang
China Mobile
V. Beeram
Juniper Networks
T. Saad
Cisco Systems

Path Computation Element Communication Protocol (PCEP) Extensions for Network Resource Partition (NRP)

Abstract

This document specifies the extensions to Path Computation Element Communication Protocol (PCEP) to carry Network Resource Partition (NRP) related information in the PCEP messages. The extensions in this document can be used to indicate the NRP-specific constraints and information needed in path computation, path status report and path initialization.

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 12 September 2023.

Table of Contents

1. Introduction

[RFC5440] describes the Path Computation Element (PCE) Communication Protocol (PCEP). PCEP enables the communication between a Path Computation Client (PCC) and a PCE, or between PCE and PCE, for the purpose of computation of Multi-protocol Label Switching (MPLS) as well as Generalized MPLS (GMPLS) Traffic Engineering Label Switched Path (TE LSP) characteristics. As depicted in [RFC4655], a PCE MUST be able to compute the path of a TE LSP by operating on the TED and considering bandwidth and other constraints applicable to the TE LSP service request.

[RFC8231] specifies a set of extensions to PCEP to enable stateful control of TE LSPs within and across PCEP sessions in compliance with [RFC4657]. It includes mechanisms to effect LSP State Synchronization between PCCs and PCEs, delegation of control over LSPs to PCEs, and PCE control of timing and sequence of path computations within and across PCEP sessions. The model of operation where LSPs are initiated from the PCE is described in [RFC8281]. [RFC8664] specifies PCEP extensions to allow a stateful PCE to compute and initiate TE paths, as well as a PCC to request a path

subject to certain constraints and optimization criteria in SR networks.

With the introduction and evolvement of 5G and other network scenarios, existing or emerging applications or customers may require connectivity services with additional characteristics. As described in [I-D.ietf-teas-ietf-network-slices], an IETF Network Slice enables connectivity service between a set of Service Demarcation Points (SDPs) with specific Service Level Objectives (SLOs) and Service Level Expectations (SLEs) over a common underlay network. For the realization of IETF network slice service, the concept Network Resource Partition (NRP) is introduced in [I-D.ietf-teas-ietf-network-slices]. A Network Resource Partition (NRP) is a subset of the buffer/queuing/ scheduling resources and associated policies on each of a connected set of links in the underlay network.

[I-D.ietf-teas-enhanced-vpn] describes a framework and the candidate technologies for providing VPN+ services. It introduces the concept of Virtual Transport Network (VTN), which consists of a set of dedicated or shared network resources allocated from the physical underlay network, and is associated with a customized logical network topology. VPN+ services can be delivered by mapping one or a group of overlay VPNs to the appropriate VTNs as the underlay, so as to provide the network characteristics required by the VPN+ customers. NRP can be seen as an instantiation of VTN in the context of IETF network slicing. Without loosing generality, this document uses the term NRP to refer to the set of network resources on a set of connected links in the underlay network.

In MPLS or SR based network, the set of network resources allocated to an NRP can be identified using resource-aware SR SIDs as defined in [I-D.ietf-spring-resource-aware-segments] [I-D.ietf-spring-sr-for-enhanced-vpn], or the VTN Resource ID as defined in [I-D.ietf-6man-enhanced-vpn-vtn-id]. The logical topology associated with an NRP could be specified using mechanisms such as Multi-Topology [RFC4915], [RFC5120] or Flex-Algo [RFC9350], etc.

To meet specific service requirement, traffic flows of an IETF network slice service need be steered onto TE paths of the corresponding NRP. A PCC may request the PCE for computing a TE path within an NRP, so that the path computation would take the resource attributes and the associated topology of the NRP into consideration. Correspondingly, a PCE may reply or initiate a TE path with NRP specific control plane and data plane information to a PCC.

This document specifies the extensions to PCEP to carry Network Resource Partition (NRP) related information in the PCEP messages.

The extensions can be used in the basic PCE computation, the stateful PCE and the PCE-initiated LSP mechanisms to indicate the NRP-specific constraints and information needed in path computation, path status report and path initialization.

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. PCEP Extensions

2.1. New TLV in LSPA Object

A new NRP TLV for use in the LSPA Object is defined to indicate the NRP ID and the related information which needs to be considered in path computation or instantiation. The format of the NRP TLV is as follows:

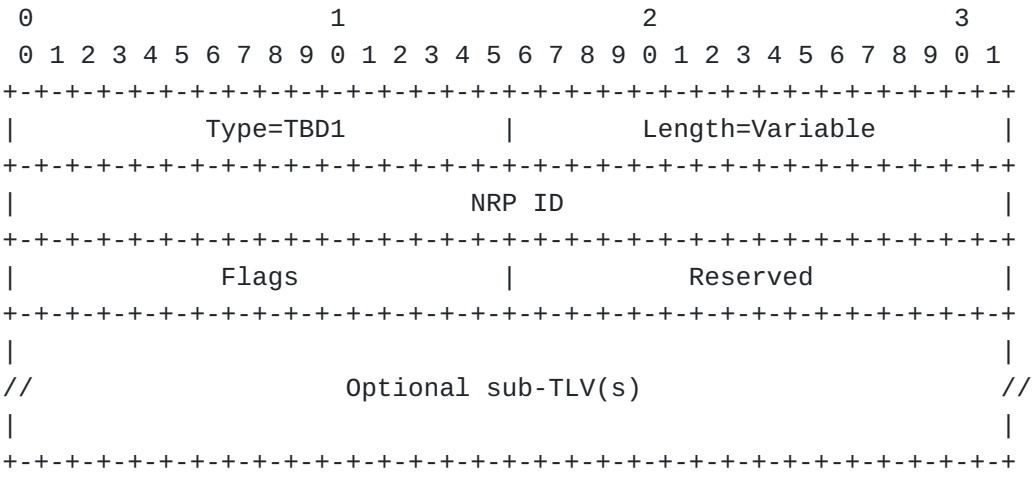

Figure 1: NRP TLV Format

Where:

*NRP ID: A network-wide unique 32-bit identifier which is used to identify an NRP.

*Flags: 16-bit flags. Currently all the flags are reserved for future use. They SHOULD be set to zero on transmission and MUST be ignored on receipt.

*Reserved: 16-bit reserved field for future use. All the bits SHOULD be set to zero on transmission and MUST be ignored on receipt.

*Optional sub-TLVs: Additional information which can be used in NRP-specific constraints. Currently no sub-TLV is defined in this document.

2.2. Capability Advertisement

A PCEP speaker indicates whether it supports NRP-specific path computation using a new PCEP capability called "NRP-CAPABILITY". When the PCEP session is created, it sends an Open message with an OPEN Object containing the NRP-CAPABILITY TLV. The format of this TLV is as follows:

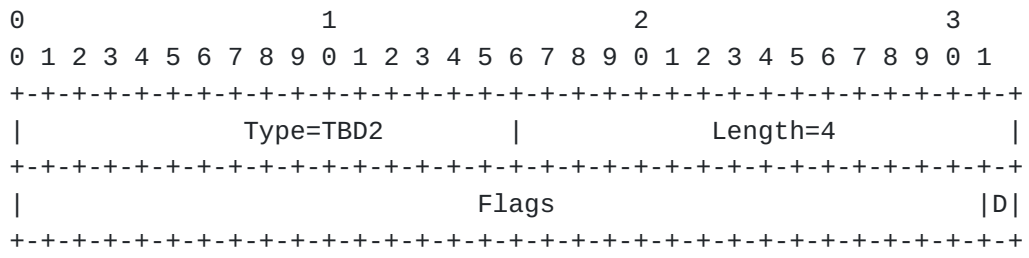

Figure 2: NRP CAPABILITY TLV

The type (16 bits) of the TLV is TBA. The length field is 16 bits long and has a fixed value of 4.

The value comprises a single field -- Flags (32 bits):

*D (Data Plane NRP ID CAPABILITY - 1 bit): if set to 1 by a PCC, the D flag indicates that the PCC supports the encapsulation of data plane NPR ID in data packet; if set to 1 by a PCE, it indicates that the PCE supports to provide path computation result with the data plane NRP ID used for the path.

*Unassigned bits in the Flags field MUST be set to zero on transmission and ignored on receipt.

3. Operations

The NRP TLV defined in this document can be used for NRP-aware TE path computation, NRP-specific path status report and NRP-specific path instantiation, thus it is applicable to both the basic PCE mechanisms and the stateful PCE mechanisms.

3.1. NRP-aware Path Computation

NRP-aware TE path computation SHOULD be performed based on the constraints and network resources associated with a specific NRP. Information about the NRP-specific network resource and topology attributes may be obtained by the PCE either from the network planning system, or using a distributed control plane such as IGP or BGP-LS with necessary extensions. The detailed mechanism is out of the scope of this document.

In a PCReq message, the NRP TLV SHOULD be carried in the LSPA Object to indicate that the path computation needs to be executed using the network resource and topological attributes of the NRP. The PCE SHOULD use the network resource and topology attributes associated with the specified NRP as the parameters in path computation. In a PCRep message, the NRP TLV MAY be carried in the LSPA Object in case of failure to indicate the path computation in the specified NRP was not successful.

3.2. NRP-specific Path Update and Report

The NRP TLV defined in this document can be used for NRP-specific path update and report in the stateful PCE mechanisms.

A PCE MAY include the NRP TLV in PCUpd Message to indicate the NRP in which the TE path needs to be updated. The NRP ID SHOULD be the same as the NRP ID of the existing TE path. If a PCC receives an PCUpd message in which the NRP ID does not match with the NRP ID of the path, the PCC MUST keep the LSP state unchanged, and include an LSP Error Code value of "NRP Mismatch" (TBD3) in LSP State Report message. On successful update of a TE path, the NRP TLV SHOULD be included in the PCRpt message to indicate the NRP in which the TE path is reported.

3.3. NRP-specific Path Initiation

The NRP TLV defined in this document can be used for NRP-specific path initiation in the PCE-Initiated LSP mechanisms.

In a PCInitiate message, the NRP TLV MAY be included to indicate the NRP in which the path needs to be initiated. Depending on the setting of the D flag in the NRP Capability, the PCC will use either the resources-aware SIDs associated with the NRP or the data plane NRP ID in constructing the NRP specific TE path. If the PCC determines that the LSP parameters proposed in the PCInitiate message are unacceptable, it MUST send a PCErr message with Error-type=24 (PCE instantiation error) and Error-value=1 (Unacceptable instantiation parameters). On successful completion of the LSP instantiation, the NRP TLV SHOULD be included in the PCRpt message to indicate the NRP in which the TE path was instantiated.

4. Security Considerations

This document defines a new NRP TLV that do not add any new security concerns beyond those discussed in [RFC5440] in itself. Some deployments may find the NRP information to be extra sensitive and could be used to influence path computation and setup with adverse effect. Additionally, snooping of PCEP messages with such data or using PCEP messages for network reconnaissance may give an attacker sensitive information about the operations of the network. Thus, such deployment should employ suitable PCEP security mechanisms like TCP Authentication Option (TCP-AO) [RFC5925] or Transport Layer Security (TLS) [RFC8253]. The procedure based on TLS is considered a security enhancement and thus is much better suited for the sensitive information.

5. IANA Considerations

This document makes following requests to IANA for action.

IANA is requested to make the following allocations in the "PCEP TLV Type Indicators" subregistry of the "Path Computation Element Protocol (PCEP) Numbers" registry:

Value	Description	Reference
TBD1	NRP	This document
TBD2	NRP CAPABILITY	This document

IANA is requested to allocate a new error code in the "LSP-ERROR-CODE TLV Error Code Field" sub-registry of the "Path Computation Element Protocol (PCEP) Numbers" registry:

Value	Description	Reference
TBD3	NRP Mismatch	This document

6. Contributors

Dhruv Dhody
Email: dhruv.ietf@gmail.com

Zhibo Hu
Email: huzhibo@huawei.com

7. Acknowledgments

The authors would like to thank Zhenbin Li for his review and valuable comments.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, DOI 10.17487/RFC5440, March 2009, <https://www.rfc-editor.org/info/rfc5440>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8231] Crabbe, E., Minei, I., Medved, J., and R. Varga, "Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE", RFC 8231, DOI 10.17487/RFC8231, September 2017, <https://www.rfc-editor.org/info/rfc8231>.

[RFC8281] Crabbe, E., Minei, I., Sivabalan, S., and R. Varga, "Path Computation Element Communication Protocol (PCEP) Extensions for PCE-Initiated LSP Setup in a Stateful PCE Model", RFC 8281, DOI 10.17487/RFC8281, December 2017, <https://www.rfc-editor.org/info/rfc8281>.

[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>.

[RFC9350] Psenak, P., Ed., Hegde, S., Filsfils, C., Talaulikar, K., and A. Gulko, "IGP Flexible Algorithm", RFC 9350, DOI 10.17487/RFC9350, February 2023, <https://www.rfc-editor.org/info/rfc9350>.

8.2. Informative References

[RFC4655] Farrel, A., Vasseur, J.-P., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, DOI 10.17487/RFC4655, August 2006, <https://www.rfc-editor.org/info/rfc4655>.

[RFC4657] Ash, J., Ed. and J.L. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol Generic

Requirements", RFC 4657, DOI 10.17487/RFC4657, September 2006, <https://www.rfc-editor.org/info/rfc4657>.

[RFC4915] Psenak, P., Mirtorabi, S., Roy, A., Nguyen, L., and P. Pillay-Esnault, "Multi-Topology (MT) Routing in OSPF", RFC 4915, DOI 10.17487/RFC4915, June 2007, <https://www.rfc-editor.org/info/rfc4915>.

[RFC5120] Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", RFC 5120, DOI 10.17487/RFC5120, February 2008, <https://www.rfc-editor.org/info/rfc5120>.

[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>.

[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-teas-ietf-network-slices]
Farrel, A., Drake, J., Rokui, R., Homma, S., Makhijani, K., Contreras, L. M., and J. Tantsura, "A Framework for IETF Network Slices", Work in Progress, Internet-Draft, draft-ietf-teas-ietf-network-slices-19, 21 January 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slices-19>.

[I-D.ietf-teas-enhanced-vpn] Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for Enhanced Virtual Private Network (VPN+)", Work in Progress, Internet-Draft, draft-ietf-teas-enhanced-vpn-12, 23 January 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-enhanced-vpn-12>.

[I-D.ietf-spring-resource-aware-segments]
Dong, J., Bryant, S., Miyasaka, T., Zhu, Y., Qin, F., Li, Z., and F. Clad, "Introducing Resource Awareness to SR Segments", Work in Progress, Internet-Draft, draft-ietf-spring-resource-aware-segments-06, 11 October 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-resource-aware-segments-06>.

[I-D.ietf-spring-sr-for-enhanced-vpn]
Dong, J., Bryant, S., Miyasaka, T., Zhu, Y., Qin, F., Li, Z., and F. Clad, "Segment Routing based Virtual Transport

Network (VTN) for Enhanced VPN", Work in Progress, Internet-Draft, draft-ietf-spring-sr-for-enhanced-vpn-04, 11 October 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-spring-sr-for-enhanced-vpn-04>.

[I-D.ietf-6man-enhanced-vpn-vtn-id] Dong, J., Li, Z., Xie, C., Ma, C., and G. S. Mishra, "Carrying Virtual Transport Network (VTN) Information in IPv6 Extension Header", Work in Progress, Internet-Draft, draft-ietf-6man-enhanced-vpn-vtn-id-02, 24 October 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-enhanced-vpn-vtn-id-02>.

Authors' Addresses

Jie Dong
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing
100095
China

Email: jie.dong@huawei.com

Sheng Fang
Huawei Technologies
Huawei Campus, No. 156 Beiqing Rd.
Beijing
100095
China

Email: fangsheng@huawei.com

Quan Xiong
ZTE Corporation
No. 6 Huashi Park Rd
Wuhan
Hubei, 430223
China

Email: xiong.quan@zte.com.cn

Shaofu Peng
ZTE Corporation
No. 50 Software Avenue
Nanjing
Jiangsu, 210012
China

Email: peng.shaofu@zte.com.cn

Liuyan Han
China Mobile
Beijing
China

Email: hanliuyan@chinamobile.com

Minxue Wang
China Mobile
Beijing
China

Email: wangminxue@chinamobile.com

Vishnu Pavan Beeram
Juniper Networks

Email: vbeeram@juniper.net

Tarek Saad
Cisco Systems

Email: tsaad.net@gmail.com