Workgroup: PCE working group
Internet-Draft:
draft-ietf-lsr-pce-discovery-security-support-13
Updates: 5088, 5089, 8231, 8306
Published: 11 October 2022
Intended Status: Standards Track
Expires: 14 April 2023

Authors: D. Lopez (Telefonica I+D), Q. Wu (Huawei), D. Dhody (Huawei), Q. Ma (Huawei)

D. King
Old Dog Consulting

IGP extension for PCEP security capability support in PCE discovery

Abstract

When a Path Computation Element (PCE) is a Label Switching Router (LSR) participating in the Interior Gateway Protocol (IGP), or even a server participating in the IGP, its presence and path computation capabilities can be advertised using IGP flooding. The IGP extensions for PCE discovery (RFC 5088 and RFC 5089) define a method to advertise path computation capabilities using IGP flooding for OSPF and IS-IS respectively. However these specifications lack a method to advertise PCE Communication Protocol (PCEP) security (e.g., Transport Layer Security (TLS), TCP Authentication Option (TCP-AO)) support capability.

This document defines capability flag bits for the PCE-CAP-FLAGS sub-TLV that can be announced as an attribute in the IGP advertisement to distribute PCEP security support information. In addition, this document updates RFC 5088 and RFC 5089 to allow advertisement of a Key ID or Key Chain Name Sub-TLV to support TCP-AO security capability. Further, this document updates RFC 8231 and RFC 8306.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Copyright Notice

Table of Contents

1. Introduction

As described in [RFC5440], Path Computation Element Communication Protocol (PCEP) communication privacy and integrity are important issues, as an attacker that intercepts a PCEP message could obtain sensitive information related to computed paths and resources. Authentication and integrity checks allow the receiver of a PCEP message to know that the message genuinely comes from the node that purports to have sent it and to know whether the message has been modified.

Among the possible solutions mentioned in that document, Transport Layer Security (TLS) [RFC8446] provides support for peer authentication, and message encryption and integrity while TCP Authentication Option (TCP-AO) [RFC5925] and Cryptographic Algorithms for TCP-AO [RFC5926] offer significantly improved security for applications using TCP. As specified in section 4 of [RFC8253], in order for a Path Computation Client (PCC) to establish a connection with a PCE server using TLS or TCP-AO, the PCC needs to know whether PCE server supports TLS or TCP-AO as a secure transport.

[RFC5088] and [RFC5089] define a method to advertise path computation capabilities using IGP flooding for OSPF and IS-IS respectively. However, these specifications lack a method to advertise PCEP security (e.g., TLS) support capability.

This document defines capability flag bits for the PCE-CAP-FLAGS sub-TLV that can be announced as attributes in the IGP advertisement to distribute PCEP security support information. In addition, this document updates [RFC5088] and [RFC5089] to allow advertisement of a Key ID or Key Chain Name Sub-TLV to support TCP-AO security capability.

As per [RFC5088], the IANA created a top-level OSPF registry, the "Path Computation Element (PCE) Capability Flags" registry. This document updates [RFC5088] and moves the registry to "Interior Gateway Protocol (IGP) Parameters". [RFC5089] states that the IS-IS uses the same registry as OSPF. This document updates [RFC5089] to refer to the new IGP registry. Further, this document updates [RFC8231] where it references the registry location as "Open Shortest Path First (OSPF) Parameters" registry to "Interior Gateway Protocol (IGP) Parameters" registry. This document updates [RFC8306] where it uses the term "OSPF PCE Capability Flag" and request assignment from OSPF Parameters registry with "PCE Capability Flag" and the IGP Parameters registry.

Note that [RFC5557] uses the term "OSPF registry" instead of the "IGP registry" whereas [RFC8623] and [RFC9168] uses the term "OSPF Parameters" instead of "IGP Parameters".

Note that the PCEP Open message exchange is another way to discover PCE capabilities information, but in this instance, the TCP security related key parameters need to be known before the PCEP session is established and the PCEP Open messages are exchanged. Thus, the use of the PCE discovery and capabilities advertisement of the IGP needs to be leveraged.

2. Conventions used in this document

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.

3. IGP extension for PCEP security capability support

[RFC5088] defines a PCE Discovery (PCED) TLV carried in an OSPF Router Information Link State Advertisement (LSA) as defined in [RFC7770] to facilitate PCE discovery using OSPF. This document defines two capability flag bits in the OSPF PCE Capability Flags to indicate TCP Authentication Option (TCP-AO) support [RFC5925] [RFC5926] and PCEP over TLS support [RFC8253] respectively.

Similarly, [RFC5089] defines the PCED sub-TLV for use in PCE discovery using IS-IS. This document will use the same flag for the OSPF PCE Capability Flags sub-TLV to allow IS-IS to indicate TCP Authentication Option (TCP-AO) support, PCEP over TLS support respectively.

The IANA assignments for shared OSPF and IS-IS Security Capability Flags are documented in Section 8.1 ("PCE Capability Flags") of this document.

3.1. Use of PCEP security capability support for PCE discovery

TCP-AO, PCEP over TLS support flag bits are advertised using IGP flooding.

- PCE supports TCP-AO: IGP advertisement SHOULD include TCP-AO support flag bit.

- PCE supports TLS: IGP advertisement SHOULD include PCEP over TLS support flag bit.

If the PCE supports multiple security mechanisms, it SHOULD include all corresponding flag bits in its IGP advertisement.

A client's configuration MAY indicate that support for a given security capability is required. If a client is configured to require that its PCE server supports TCP-AO, the client MUST verify that the TCP-AO flag bit in the PCE-CAP-FLAGS sub-TLV for a given server is set before it opens a connection to that server. Similarly, if the client is configured to require that its PCE server supports TLS, the client MUST verify that the PCEP over TLS support flag bit in the PCE-CAP-FLAGS sub-TLV for a given server is set before it opens a connection to that server.

3.2. KEY-ID Sub-TLV

The KEY-ID sub-TLV specifies an identifier that can be used by the PCC to identify the TCP-AO key [RFC5925] (referred to as KeyID).

3.2.1. IS-IS

The KEY-ID sub-TLV MAY be present in the PCED sub-TLV carried within the IS-IS Router CAPABILITY TLV when the capability flag bit of PCE-CAP-FLAGS sub-TLV in IS-IS is set to indicate TCP Authentication Option (TCP-AO) support.

The KEY-ID sub-TLV has the following format:

*Type: 6

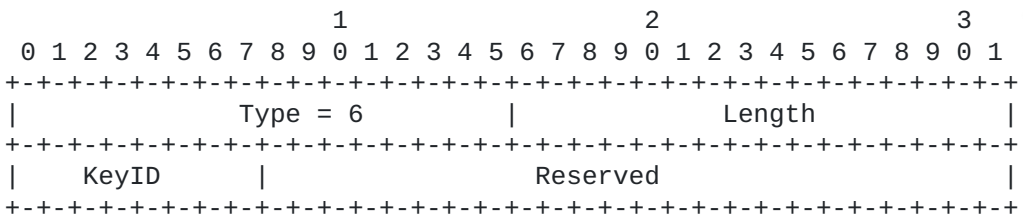
*Length: 1

*KeyID: The one octet Key ID as per [RFC5925] to uniquely identify the Master Key Tuple (MKT).

3.2.2. OSPF

Similarly, this sub-TLV MAY be present in the PCED TLV carried within OSPF Router Information LSA when the capability flag bit of PCE-CAP-FLAGS sub-TLV in OSPF is set to indicate TCP-AO support.

The format of KEY-ID sub-TLV is as follows:



*Type: 6

*Length: 4

*KeyID: The one octet Key ID as per [RFC5925] to uniquely identify the Master Key Tuple (MKT).

*Reserved: MUST be set to zero while sending and ignored on receipt.

3.3. KEY-CHAIN-NAME Sub-TLV

The KEY-CHAIN-NAME sub-TLV specifies a keychain name that can be used by the PCC to identify the keychain. The keychain name could be manually configured via CLI or installed in the YANG datastore (see [RFC8177]) at the PCC.

3.3.1. IS-IS

The KEY-CHAIN-NAME sub-TLV MAY be present in the PCED sub-TLV carried within the IS-IS Router CAPABILITY TLV when the capability flag bit of the PCE-CAP-FLAGS sub-TLV in IS-IS is set to indicate TCP Authentication Option (TCP-AO) support.

The KEY-CHAIN-NAME sub-TLV has the following format:

*Type: 7

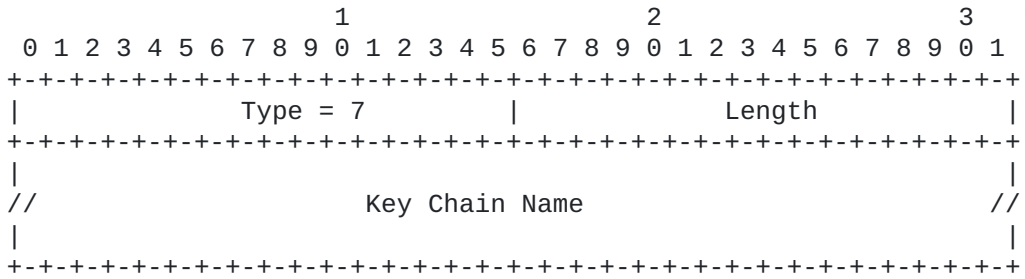
*Length: Variable, encodes the length of the value field.

*Key Name: The Key Chain Name contains a string of 1 to 255 octets to be used to identify the key chain. It MUST be encoded using UTF-8. A receiving entity MUST NOT interpret invalid UTF-8 sequences and ignore them. This field is not NULL terminated. UTF-8 "Shortest Form" encoding is REQUIRED to guard against the technical issues outlined in [UTR36].

3.3.2. OSPF

Similarly, this sub-TLV MAY be present in the PCED TLV carried within the OSPF Router Information LSA when the capability flag bit of PCE-CAP-FLAGS sub-TLV in OSPF is set to indicate TCP-AO support. The sub-TLV MUST be zero-padded so that the sub-TLV is 4-octet aligned.

The format of KEY-CHAIN-NAME sub-TLV is as follows:



*Type: 7

*Length: Variable, padding is not included in the Length field

*Key Name: The Key Chain Name contains a string of 1 to 255 octets to be used to identify the key chain. It MUST be encoded using UTF-8. A receiving entity MUST NOT interpret invalid UTF-8 sequences and ignore them. This field is not NULL terminated. UTF-8 "Shortest Form" encoding is REQUIRED to guard against the technical issues outlined in [UTR36]. The sub-TLV MUST be zero-padded so that the sub-TLV is 4-octet aligned.

4. Update to RFCs

Section 4 of [RFC5088] states that no new sub-TLVs will be added to the PCED TLV, and no new PCE information will be carried in the Router Information LSA. This document updates [RFC5088] by allowing the two sub-TLVs defined in this document to be carried in the PCED TLV advertised in the Router Information LSA.

Section 4 of [RFC5089] states that no new sub-TLVs will be added to the PCED TLV, and no new PCE information will be carried in the Router CAPABLITY TLV. This document updates [RFC5089] by allowing the two sub-TLVs defined in this document to be carried in the PCED TLV advertised in the Router CAPABILITY TLV.

This introduction of additional sub-TLVs should be viewed as an exception to the [RFC5088][RFC5089] policy, justified by the requirement to discover the PCEP security support prior to establishing a PCEP session. The restrictions defined in [RFC5088] [RFC5089] should still be considered to be in place. If in the future new advertisements are required, alternative mechanisms such as using [RFC6823] or [I-D.ietf-lsr-ospf-transport-instance] should be considered.

The registry for the PCE Capability Flags assigned in section 8.3 of [RFC5557], section 8.1 of [RFC8231], section 6.9 of [RFC8306], section 11.1 of [RFC8623], and section 10.5 of [RFC9168] has changed to the IGP Parameters "Path Computation Element (PCE) Capability Flags" registry created in this document.

5. Backward Compatibility Considerations

An LSR that does not support the IGP PCE capability bits specified in this document silently ignores those bits.

An LSR that does not support the KEY-ID and KEY-CHAIN-NAME sub-TLVs specified in this document silently ignores these sub-TLVs.

IGP extensions defined in this document do not introduce any new interoperability issues.

6. Management Considerations

Manageability considerations for PCE Discovery are addressed in Section 4.10 of [RFC4674] and Section 9 of [RFC5088] [RFC5089].

6.1. Control of Policy and Functions

A PCE implementation SHOULD allow the following parameters to be configured on the PCE:

- *support for TCP-AO
- *the KeyID used by TCP-AO
- *Key Chain Name
- *support for TLS

6.2. Information and Data Model

The YANG model for PCEP [I-D.ietf-pce-pcep-yang] supports PCEP security parameters (key, key chain, and TLS).

6.3. Liveness Detection and Monitoring

Normal operations of the IGP meet the requirements for liveness detection and monitoring.

6.4. Verify Correct Operations

The correlation of PCEP security information advertised against information received can be achieved by comparing the information in

the PCED sub-TLV received by the PCC with that stored at the PCE using the PCEP YANG.

6.5. Requirements on Other Protocols and Functional Components

There are no new requirements on other protocols.

6.6. Impact on Network Operations

Frequent changes in PCEP security information advertised in the PCED sub-TLV may have a significant impact on IGP and might destabilize the operation of the network by causing the PCCs to reconnect sessions with PCE(s). Section 4.10.4 of [RFC4674] and Section 9.6 of [RFC5088] [RFC5089] list techniques that are applicable to this document as well.

7. Security Considerations

Security considerations as specified by [RFC5088] and [RFC5089] are applicable to this document.

As described in Section 10.2 of [RFC5440], an PCEP speaker MUST support TCP MD5 [RFC2385], so no capability advertisement is needed to indicate support. However, as noted in [RFC6952], TCP MD5 has been obsoleted by TCP-AO [RFC5925] because of security concerns. However, TCP-AO is not widely implemented and so it is, therefore, RECOMMENDED (per [RFC8253] which updates [RFC5440]) that PCEP is secured using TLS. An implementation SHOULD offer at least one of the two security capabilities defined in this document.

The information related to PCEP security is sensitive and due care needs to be taken by the operator. This document defines new capability bits that are susceptible to a downgrade attack by setting them to zero. The content of Key ID or Key Chain Name Sub-TLV can be altered to enable an on-path attack. Thus, before advertising the PCEP security parameters, using the mechanism described in this document, the IGP MUST be known to provide authentication and integrity for the PCED TLV using the mechanisms defined in [RFC5304], [RFC5310] or [RFC5709].

Moreover, as stated in the Security Considerations of [RFC5088] and [RFC5089], there are no mechanisms defined in OSPF or IS-IS to protect the confidentiality of the PCED TLV. For this reason, the operator must ensure that no private data is carried in the TLV, e.g. that key-ids or key-chain names do not reveal sensitive information about the network.

8. IANA Considerations

8.1. PCE Capability Flags

IANA is requested to move the "Path Computation Element (PCE) Capability Flags" registry from the "Open Shortest Path First v2 (OSPFv2) Parameters" grouping to the "Interior Gateway Protocol (IGP) Parameters" grouping.

IANA is requested to make the following additional assignments from the "Path Computation Element (PCE) Capability Flags" registry.

Bit	Capability Description	Reference
xx	TCP-AO Support	[This.I.D]
xx	PCEP over TLS support	[This.I.D]

The grouping is located at: https://www.iana.org/assignments/igp-parameters/igp-parameters.xhtml.

8.2. PCED sub-TLV Type Indicators

The PCED sub-TLVs were defined in [RFC5088] and [RFC5089], but they did not create a registry for it. This document requests IANA to create a new registry called "PCED sub-TLV type indicators" under the "Interior Gateway Protocol (IGP) Parameters" grouping. The registration policy for this registry is "Standards Action" [RFC8126]. Values in this registry come from the range 0-65535.

This registry should be populated with:

Value	Description	Reference
0	Reserved	[This.I.D][RFC5088]
1	PCE-ADDRESS	[This.I.D][RFC5088]
2	PATH-SCOPE	[This.I.D][RFC5088]
3	PCE-DOMAIN	[This.I.D][RFC5088]
4	NEIG-PCE-DOMAIN	[This.I.D][RFC5088]
5	PCE-CAP-FLAGS	[This.I.D][RFC5088]
6	KEY-ID	[This.I.D]
7	KEY-CHAIN-NAME	[This.I.D]

This registry is used by both the OSPF PCED TLV and the IS-IS PCED sub-TLV.

This grouping is located at: https://www.iana.org/assignments/igp-parameters/igp-parameters.xhtml.

9. Acknowledgments

The authors of this document would also like to thank Acee Lindem, Julien Meuric, Les Ginsberg, Ketan Talaulikar, Tom Petch, Aijun Wang, Adrian Farrel for the review and comments.

The authors would also like to special thank Michale Wang for his major contributions to the initial version.

Thanks to John Scudder for providing an excellent AD review. Thanks to Carlos Pignataro, Yaron Sheffer, Ron Bonica, and Will (Shucheng) LIU for directorate reviews.

Thanks to Lars Eggert, Robert Wilton, Roman Danyliw, Eric Vyncke, Paul Wouters, Murray Kucherawy, and Warren Kumari for IESG reviews.

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>.

[RFC5088] Le Roux, JL., Ed., Vasseur, JP., Ed., Ikejiri, Y., and R. Zhang, "OSPF Protocol Extensions for Path Computation Element (PCE) Discovery", RFC 5088, DOI 10.17487/RFC5088, January 2008, <https://www.rfc-editor.org/info/rfc5088>.

[RFC5089] Le Roux, JL., Ed., Vasseur, JP., Ed., Ikejiri, Y., and R. Zhang, "IS-IS Protocol Extensions for Path Computation Element (PCE) Discovery", RFC 5089, DOI 10.17487/RFC5089, January 2008, <https://www.rfc-editor.org/info/rfc5089>.

[RFC5557] Lee, Y., Le Roux, JL., King, D., and E. Oki, "Path Computation Element Communication Protocol (PCEP) Requirements and Protocol Extensions in Support of Global Concurrent Optimization", RFC 5557, DOI 10.17487/RFC5557, July 2009, <https://www.rfc-editor.org/info/rfc5557>.

[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>.

[RFC8177] Lindem, A., Ed., Qu, Y., Yeung, D., Chen, I., and J. Zhang, "YANG Data Model for Key Chains", RFC 8177, DOI 10.17487/RFC8177, June 2017, <https://www.rfc-editor.org/info/rfc8177>.

[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>.

[RFC7770] Lindem, A., Ed., Shen, N., Vasseur, JP., Aggarwal, R., and S. Shaffer, "Extensions to OSPF for Advertising Optional Router Capabilities", RFC 7770, DOI 10.17487/RFC7770, February 2016, <https://www.rfc-editor.org/info/rfc7770>.

[RFC5304] Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication", RFC 5304, DOI 10.17487/RFC5304, October 2008, <https://www.rfc-editor.org/info/rfc5304>.

[RFC5310] Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, DOI 10.17487/RFC5310, February 2009, <https://www.rfc-editor.org/info/rfc5310>.

[RFC5709] Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M., Li, T., and R. Atkinson, "OSPFv2 HMAC-SHA Cryptographic Authentication", RFC 5709, DOI 10.17487/RFC5709, October 2009, <https://www.rfc-editor.org/info/rfc5709>.

[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>.

[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>.

[RFC8306] Zhao, Q., Dhody, D., Ed., Palleti, R., and D. King, "Extensions to the Path Computation Element Communication Protocol (PCEP) for Point-to-Multipoint Traffic Engineering Label Switched Paths", RFC 8306, DOI 10.17487/RFC8306, November 2017, <https://www.rfc-editor.org/info/rfc8306>.

[RFC8623] Palle, U., Dhody, D., Tanaka, Y., and V. Beeram, "Stateful Path Computation Element (PCE) Protocol Extensions for Usage with Point-to-Multipoint TE Label Switched Paths (LSPs)", RFC 8623, DOI 10.17487/RFC8623, June 2019, <https://www.rfc-editor.org/info/rfc8623>.

[RFC9168] Dhody, D., Farrel, A., and Z. Li, "Path Computation Element Communication Protocol (PCEP) Extension for Flow Specification", RFC 9168, DOI 10.17487/RFC9168, January 2022, <https://www.rfc-editor.org/info/rfc9168>.

10.2. Informative References

[RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, DOI 10.17487/RFC2385, August 1998, <https://www.rfc-editor.org/info/rfc2385>.

[RFC4674] Le Roux, J.L., Ed., "Requirements for Path Computation Element (PCE) Discovery", RFC 4674, DOI 10.17487/RFC4674, October 2006, <https://www.rfc-editor.org/info/rfc4674>.

[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>.

[RFC5926] Lebovitz, G. and E. Rescorla, "Cryptographic Algorithms for the TCP Authentication Option (TCP-AO)", RFC 5926, DOI 10.17487/RFC5926, June 2010, <https://www.rfc-editor.org/info/rfc5926>.

[RFC6823] Ginsberg, L., Previdi, S., and M. Shand, "Advertising Generic Information in IS-IS", RFC 6823, DOI 10.17487/RFC6823, December 2012, <https://www.rfc-editor.org/info/rfc6823>.

[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>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[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-19, 11 July 2022, <https://www.ietf.org/archive/id/draft-ietf-pce-pcep-yang-19.txt>.

[I-D.ietf-lsr-ospf-transport-instance] Lindem, A., Qu, Y., Roy, A., and S. Mirtorabi, "OSPF-GT (Generalized Transport)", Work in Progress, Internet-Draft, draft-ietf-lsr-ospf-transport-instance-03, 9 July 2022, <https://www.ietf.org/archive/id/draft-ietf-lsr-ospf-transport-instance-03.txt>.

[UTR36] Davis, M., "Unicode Technical Report #36, Character Encoding Model", UTR17 https://www.unicode.org/unicode/reports/tr36/, February 2005.

Authors' Addresses

Diego R. Lopez
Telefonica I+D
Spain

Email: diego.r.lopez@telefonica.com

Qin Wu
Huawei Technologies
101 Software Avenue, Yuhua District
Nanjing
Jiangsu, 210012
China

Email: bill.wu@huawei.com

Dhruv Dhody
Huawei Technologies
Divyashree Techno Park, Whitefield
Bangalore 560037
Karnataka
India

Email: dhruv.ietf@gmail.com

Qiufang Ma
Huawei
101 Software Avenue, Yuhua District
Nanjing
Jiangsu, 210012
China

Email: maqiufang1@huawei.com

Daniel King
Old Dog Consulting
United Kingdom

Email: daniel@olddog.co.uk