Network Working Group
Internet-Draft
Intended status: Experimental
Expires: 28 February 2026

G. Fioccola
T. Zhou
Huawei
G. Mishra
Verizon Inc.
X. Wang
Ruijie
G. Zhang
China Mobile
M. Cociglio
27 August 2025

Application of the Alternate Marking Method to the Segment Routing Header
draft-fz-spring-srv6-alt-mark-17

Abstract

This document describes an alternative experimental approach for the application of the Alternate-Marking Method to SRv6. It uses an experimental TLV in the Segment Routing Header, and thus participation in this experiment should be between coordinating parties in a controlled domain. This approach has potential scaling and simplification benefits over the technique described in RFC 9343 and the scope of the experiment is to determine whether those are significant and attractive to the community.

This protocol extension has been developed outside the IETF as an alternative to the IETF's standards track specification RFC 9343 and it does not have IETF consensus. It is published here to guide experimental implementation, ensure interoperability among implementations to better determine the value of this approach. Researchers are invited to submit their evaluations of this work to the RFC Editor for consideration as independent submissions or to the IETF SPRING working group as Internet-Drafts.

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/.

Copyright Notice

Table of Contents

1. Introduction

[RFC9341] and [RFC9342] describe a passive performance measurement method, which can be used to measure packet loss, latency and jitter on live traffic. Since this method is based on marking consecutive batches of packets, the method is often referred as the Alternate Marking Method.

The Alternate Marking Method requires a marking field so that packet flows can be distinguished and identified. [RFC9343] defines the standard for how the marking field can be encoded in a new TLV in either Hop-by-hop or Destination Options Headers of IPv6 packets in order to achieve Alternate Marking. The mechanism to carry is equally applicable to Segment Routing for IPv6 (SRv6) networks [RFC8402].

This document describes an alternative experimental approach that encodes the marking field in a new TLV carried in the Segment Routing Header (SRH) [RFC8754] of an SRv6 packet. This approach is applicable only to SRv6 deployments. It is intended to capitalize on the assumption that Segment Routing (SR) nodes are supposed to support fast parsing and processing of the SRH, while the SR nodes may not handle properly Destination Options, as discussed in [RFC9098], [I-D.ietf-6man-eh-limits]. The experiment is to determine whether or not there are significant and attractive advantages to the community: if there are, the work may be brought back for IETF consideration.

This protocol extension has been developed outside the IETF as an alternative to the IETF’s standards track specification [RFC9343] and it does not have IETF consensus. It is published here to guide experimental implementation, ensure interoperability among implementations to better determine the value of this approach. As also highlighted in [I-D.bonica-gendispatch-exp], when two protocol extensions are proposed to solve a single problem, an experiment can be initiated and this is the purpose of this document. See Section 5 for more details about the experimentation.

1.1. Observations on RFC 9343

Like any other IPv6 use case, Hop-by-Hop and Destination Options can also be used when the SRH is present. As specified in [RFC8200], the Hop-by-Hop Options Header is used to carry optional information that needs to be examined at every hop along the path, while the Destination Options Header is used to carry optional information that needs to be examined only by the packet’s destination node(s).

When a Routing Header exists, because the SRH is a Routing Header, Destination Options present in the IPv6 packet before the SRH header are processed by destination indicated in the SRH's route list. As specified in [RFC8754], SR segment endpoint nodes process the local SID corresponding to the packet destination address. Then, the destination address is updated according to the segment list. The SRH TLV provides metadata for segment processing, while processing the SID, if the node is locally configured to do so. Both the Destination Options Header before SRH and the SRH TLV are processed at the node being indicated in the destination address field of the IPv6 header.

The distinction between the alternatives is most notable for SRv6 packets that traverse a network where the paths between sequential segment end points include multiple hops. If the Hop-by-Hop Option is used, then every hop along the path will process the AltMark data. If the Destination Option positioned before the SRH is used, or the SRH AltMark TLV is used, then only the segment end points will process the AltMark data.

Both [RFC9343] and the approach specified in this document can co-exist. Indeed, this document does not change or invalidate any procedures defined in [RFC9343]. However, deployment issues may arise, as further discussed below.

The rest of this document is structured as follows: Section 2 covers the application of the Alternate Marking to SRv6, Section 3 specifies the AltMark SRH TLV to carry the base data fields (Section 3.1) and the extended data fields (Section 3.2), Section 4 discusses the use of the AltMark TLV, and Section 5 describes the experiment and the objectives of the experimentation (Section 5.1).

1.2. 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. Application of the Alternate Marking to SRv6

SRv6 leverages the IPv6 SRH, that can embed TLVs to provide metadata for segment processing, as described in [RFC8754]. This document defines the SRH AltMark TLV to carry Alternate Marking data fields for use in SRv6 networks and it is an alternative to [RFC9343]. [RFC9343] defines how the Alternate Marking Method can be carried in the Option Headers (Hop-by-hop or Destination) of an IPv6 packet.

The AltMark data fields format defined in [RFC9343] is the basis of the AltMark SRH TLV introduced in Section 3.

In addition to the base data fields of [RFC9343], it is also allowed the insertion of optional extended data fields which are not present in [RFC9343]. These extended data fields can support metadata for additional telemetry requirements, as further described below.

2.1. Controlled Domain

[RFC8799] introduces the concept of specific limited domain solutions and notes application of the Alternate Marking Method as an example.

Despite the flexibility of IPv6, when innovative applications are proposed they are often applied within controlled domains to help constrain the domain-wide policies, options supported, the style of network management, and security requirements. This is also the case for the application of the Alternate Marking Method to SRv6.

Therefore, the experimentation of the Alternate Marking Method to SRv6 MUST be deployed only within a controlled domain. For SRv6, the controlled domain corresponds to an SR domain, as defined in [RFC8402]. The Alternate-Marking measurement domain overlaps with the controlled domain.

The use of a controlled domain is also appropriate for the deployment of an experimental protocol extension. Carefully bounding the domain reduces the risk of the experiment leaking out and clashing with other experiments of causing unforeseen consequences in wider deployments.

3. Definition of the SRH AltMark TLV

The AltMark SRH TLV is defined to carry the data fields associated with the Alternate Marking Method. The TLV has some initial fields that are always present, and further extension fields that are present when Enhanced Alternate Marking is in use.

Figure 1 shows the format of the AltMark TLV.

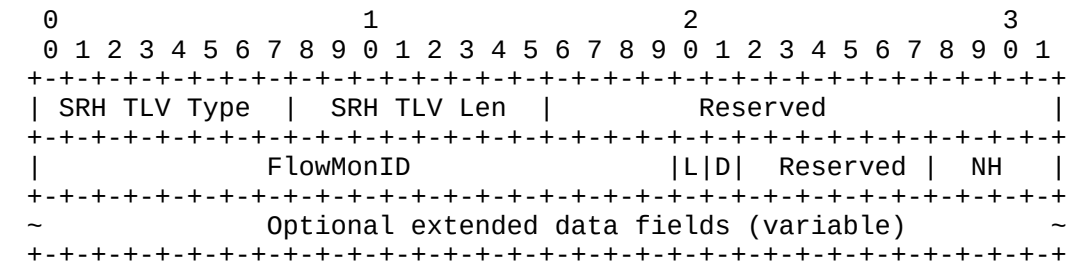

Figure 1: AltMark: SRH TLV for alternate marking

The fields of this TLV are as follows:

* SRH TLV Type: 8 bit identifier of the Alternate Marking SRH TLV. The value for this field is taken from the range 124-126. It is an Experimental code point that indicates a TLV that does not change en route. Experimentation of this document must coordinate the value used by all implementations participating in the experiment. Therefore, experiments should carefully consider any other implementations running in the controlled domain to avoid clashes with other SRH TLVs.

* SRH TLV Len: The length of the Data Fields of this TLV in bytes. This is set to 6 when Enhanced Alternate Marking is not in use.

* Reserved: Reserved for future use. These bits MUST be set to zero on transmission and ignored on receipt.

* FlowMonID: Flow Monitoring Identification field, 20 bits unsigned integer. It is defined in [RFC9343].

* L: Loss flag, as defined in [RFC9343].

* D: Delay flag, as defined in [RFC9343].

* NH: The NH (NextHeader) field is used to indicate extended data fields are present to support Enhanced Alternate Marking as follows:

  - NextHeader value of 0x0 means that there is no extended data field attached.

  - NextHeader values of 0x1-0x8 are reserved for further usage.

  - NextHeader value of 0x9 indicates the extended data fields are present as described in Section 3.2.

- NextHeader values of 0xA-0xF are reserved for further usage.

* Optional extended data fields may be present according to the setting of the NH field and as described in Section 3.2.

3.1. Base Alternate Marking Data Fields

The base AltMark data fields are: Loss Flag (L), Delay Flag (D) and Flow Monitoring Identification field (FlowMonID), as in [RFC9343].

L and D are the marking fields of the Alternate Marking Method while FlowMonID is used to identify monitored flows and aids the optimization of implementation and scaling of the Alternate Marking Method. Note that, as already highlighted in [RFC9343], the FlowMonID is used to identify the monitored flow because it is not possible to utilize the Flow Label field of the IPv6 Header.

It is important to note that if the 20 bit FlowMonID is set by the domain entry nodes, there is a chance of collision even when the values are chosen using a pseudo-random algorithm; therefore it may be not be sufficient to uniquely identify a monitored flow. In such cases the packets need to be tagged with additional flow information to allow disambiguation. Such additional tagging can be carried in the extended data fields described in Section 3.2.

3.2. Optional Extended Data Fields for Enhanced Alternate Marking

The optional extended data fields to support Enhanced Alternate Marking are illustrated in Figure 2. They are present when the NH field of the AltMark TLV is set to 0x9.

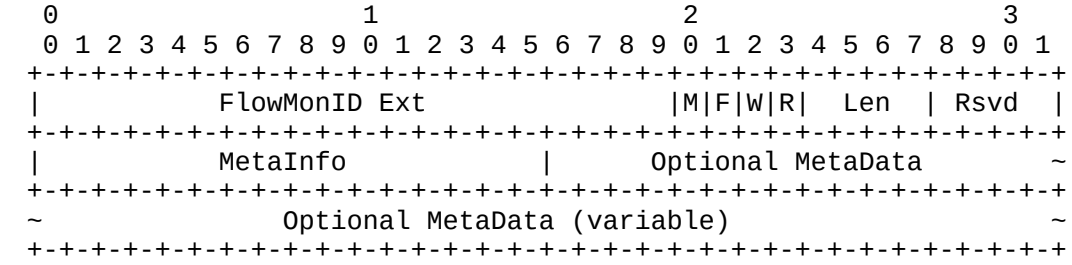

Figure 2: Optional Extended Data Fields for Enhanced Alternate Marking

The extended data fields are as follows:

* FlowMonID Ext - 20 bits unsigned integer. This is used to extend the FlowMonID in order to reduce the conflict when random allocation is applied. The disambiguation of the FlowMonID field is discussed in IPv6 AltMark Option [RFC9343].

* Four bit-flags indicate special-purpose usage.

  M bit: Measurement mode. If M=0, it indicates that it is for segment-by-segment monitoring. If M=1, it indicates that it is for end-to-end monitoring.

  F bit: Fragmentation. If F=1, it indicates that the original packet is fragmented, therefore it is necessary to only count a single packet, ignoring all the following fragments with F set to 1. Note that F is set to 0 for the first fragment.

  W bit: Flow direction identification. This flag is used if backward direction flow monitoring is requested to be set up automatically, so that the egress node is instructed to setup the backward flow monitoring. If W=1, it indicates that the flow direction is forward. If W=0, it indicates that the flow direction is backward.

  R bit: Reserved. This bit MUST be set to zero and ignored on receipt.

* Len - Length. Indicates the length of the extended data fields in bytes for enhanced alternate marking. It includes all of the fields shown in Figure 2 including any meta data that is present.

* Rsvd - Reserved for further use. These bits MUST be set to zero on transmission and ignored on receipt.

* MetaInfo - A 16-bit Bitmap to indicate more meta data attached in the Optional MetaData field for enhanced functions. More than one bit may be set, in which case the additional meta data is present in the order that the bits are set. MetaInfo bits are numbered from 0 as the most significant bit. Three bits and associated meta data are defined as follows:

  bit 0: If set to 1, it indicates that a 6 byte Timestamp is present as shown in Figure 3.

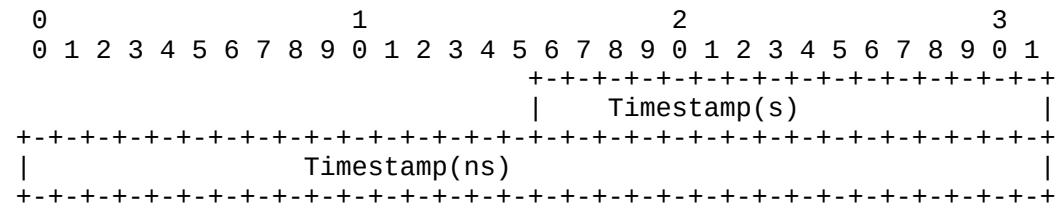

Figure 3: The Timestamp Extended Data Field

This Timestamp can be filled by the encapsulation node, and is taken all the way to the decapsulation node so that all the intermediate nodes can compare it against their local time, and measure the one way delay. The timestamp consists of two fields:

Timestamp(s) is a 16 bit integer that carries the number of seconds.

Timestamp(ns) is a 32 bit integer that carries the number of nanoseconds.

Note that the timestamp data field enables all the intermediate nodes to measure the one way delay. It can be correlated with the implementation of [I-D.ietf-opsawg-ipfix-on-path-telemetry] and [I-D.ietf-ippm-on-path-telemetry-yang]. [I-D.ietf-opsawg-ipfix-on-path-telemetry] introduces new IP Flow Information Export (IPFIX) information elements to expose the On-Path Telemetry measured delay, similarly, [I-D.ietf-ippm-on-path-telemetry-yang] defines a YANG data model for monitoring On-Path Telemetry data, including the path delay.

bit 1: If set to 1, it indicates the control information to set up the backward direction flow monitoring based on the trigger packet presence as shown in Figure 4.

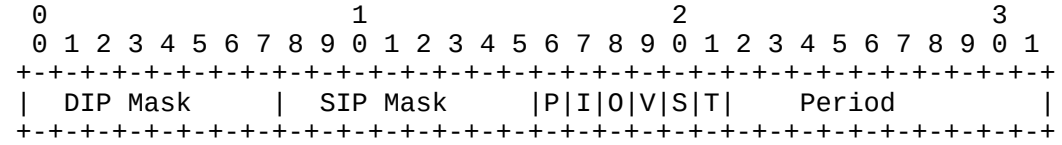

Figure 4: Control Information for Backward Direction Flow Monitoring

The control information includes several fields and flags to match in order to set up the backward direction:

DIP Mask: The length of the destination IP prefix used to match the flow.

SIP Mask: The length of the source IP prefix used to match the flow.

P bit: If set to 1, it indicates to match the flow using the protocol identifier in the trigger packet.

I bit: If set to 1, it indicates to match the source port.

O bit: If set to 1, it indicates to match the destination port.

V bit: If set to 1, the node will automatically set up reverse direction monitoring, and allocate a FlowMonID.

S bit: If set to 1, it indicates to match the DSCP.

T bit: Used to control the scope of tunnel measurement. T=1 means measure between Network-to-Network Interfaces (i.e., NNI to NNI). T=0 means measure between User-to-Network Interfaces (i.e., UNI to UNI).

Period: Indicates the alternate marking period counted in seconds.

bit 2: If set to 1, it indicates that a 4 byte sequence number is present as shown in Figure 5.

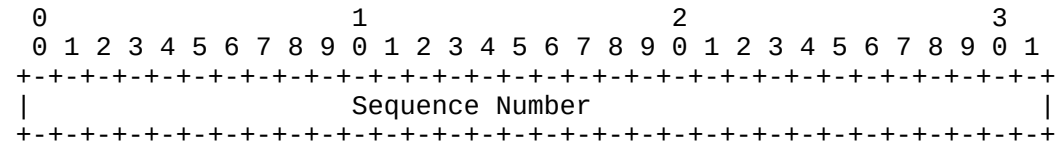

Figure 5: Sequence Number Data Field

The unique Sequence Number can be used to detect the out-of-order packets, in addition to enabling packet loss measurement. Moreover, the Sequence Number can be used together with the latency measurement, to access per packet timestamps.

4. Use of the SRH AltMark TLV

Since the measurement domain is congruent with the SR controlled domain, the procedure for AltMark data encapsulation in the SRv6 SRH is summarized as follows:

* Ingress SR Node: As part of the SRH encapsulation, the Ingress SR Node of an SR domain or an SR Policy [RFC9256] that supports the mechanisms defined in this document and that wishes to perform the Alternate Marking Method adds the AltMark TLV in the SRH of the data packets.

* Intermediate SR Node: The Intermediate SR Node is any node receiving an IPv6 packet where the destination address of that packet is a local Segment Identifier (SID). If an Intermediate SR Node is not capable of processing AltMark TLV, it simply ignores it according to the processing rules of [RFC8754]. If an Intermediate SR Node is capable of processing AltMark TLV, it checks if SRH AltMark TLV is present in the packet and processes it.

* Egress SR Node: The Egress SR Node is the last node in the segment list of the SRH. The processing of AltMark TLV at the Egress SR Node is the same as the processing of AltMark TLV at the Intermediate SR Nodes.

The use of the AltMark TLV may be combined with the network programming capability of SRv6 ([RFC8986]). Specifically, the ability for an SRv6 endpoint to determine whether to process or ignore some specific SRH TLVs (such as the AltMark TLV) may be based on the SID function associated with the SID advertised by an Intermediate or Egress SR Node and used in the Destination Address field of the SRv6 packet. When a packet is addressed to a SID which does not support the Alternate Marking functionality, the receiving node does not have to look for or process the SRH AltMark TLV and can simply ignore it. This also enables collection of Alternate Marking data only from the supporting segment endpoints.

4.1. Compatibility

As highlighted in Section 1.1, the use of the Destination Option to carry the AltMark data preceding the SRH is equivalent to the SRH AltMark TLV. Therefore, it is important to analyze what happens when both the SRH AltMArk TLV and the Destination Option are present, and how that would impact processing and complexity.

It is worth mentioning that the SRH AltMark TLV and the the Destination Option carrying AltMark data can coexist without problems. If both are present, the only issue could be the duplication of information but this will not affect in any way the device and the network services. The security requirement of controlled domain applies to both this document and [RFC9343], and it also confines this duplication to a single service provider networks. However, duplication of the same information in different places should be avoided and it is recommended to only analyze the use of SRH AltMark TLV for the experimentation.

5. Experimentation Overview

The protocol extension, described in this document, is built on existing technology using an Experimental code point. Experimentation of this document must use a code point chosen from the Experimental range, as noted in Section 3, and should make it possible for the operator to configure the value used in a deployment such that it is possible to conduct multiple non-conflicting experiments within the same network.

This experiment aims to determine whether or not the use of the SRH AltMark TLV brings advantages, in particular in consideration of implementations that cannot support multiple IPv6 extension headers in the same packet, or which do not support Destination Options Header processing, or which process the Destination Options Header on the slow path.

This experiment also needs to determine whether the proposed protocol extensions achieve the desired function and can be supported in the presence of normal SRv6 processing. In particular, the experiment needs to verify the ability to support SR network programming, SID function control and the support or non-support of the AltMark TLV.

It is anticipated that this experiment will be contained within a single service provider network in keeping with the constraints of an SR Domain, and also in keeping with the limits in sharing performance monitoring data collected on the path of packets in the network. The scope of the experimental deployment may depend on the availability of implementations and the willingness of operators to deploy it on live networks.

The results of this experiment will be collected and shared with the RFC Editor for consideration as independent submission or with the IETF SPRING working group as Internet-Draft, to help forward the discussions that will determine the correct development of Alternate Marking Method solutions in SRv6 networks. It is expected that a first set of results will be made available within two years of the publication of this document as an RFC.

5.1. Objective of the Experiment

Researchers are invited to evaluate the SRH AltMark TLV against the existing approach in [RFC9343]. There are several potential areas of exploration for this experimentation that need to be analyzed:

- Does the use of the SRH AltMark TLV survive across a network better or worse than the extension headers usage?

- Does the SRH TLV processing represent a performance improvement or hindrance on the device compared to the Destination Option?

- Is the forwarding plane performance impacted across different device architecture types comparing the use of SRH TLV and Destination Option?

- How does the use of the extended data fields, introduced in Section 3.2, compare to other on path telemetry methods from the point of view of the operators?

6. Security Considerations

The security considerations of SRv6 are discussed in [RFC8754] and [RFC8986], and the security considerations of Alternate Marking in general and its application to IPv6 are discussed in [RFC9341] and [RFC9343].

[RFC9343] analyzes different security concerns and related solutions. These aspects are valid and applicable also to this document. In particular the fundamental security requirement is that Alternate Marking MUST only be applied in a limited domain, as also mentioned in [RFC8799] and Section 2.1.

Alternate Marking is a feature applied to a trusted domain, where a single operator decides on leveraging and configuring Alternate Marking according to their needs. Additionally, operators need to properly secure the Alternate Marking domain to avoid malicious configuration and attacks, which could include injecting malicious packets into a domain. So the implementation of Alternate Marking is applied within a controlled domain where the network nodes are

locally administered and where packets containing the AltMark TLV are prevented from entering or leaving the domain. A limited administrative domain provides the network administrator with the means to select, monitor and control the access to the network.

7. IANA Considerations

This document makes no requests for IANA actions.

8. Acknowledgements

The authors would like to thank Eliot Lear, Adrian Farrel, Joel M. Halpern and Haoyu Song for the precious comments and suggestions.

9. Contributors

The following people provided relevant contributions to this document:

Fabio Bulgarella
Telecom Italia
Email: fabio.bulgarella@guest.telecomitalia.it

Massimo Nilo
Telecom Italia
Email: massimo.nilo@telecomitalia.it

Fabrizio Milan
Telecom Italia
Email: fabrizio.milan@telecomitalia.it

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>.

[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>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

[RFC9341] Fioccola, G., Ed., Cociglio, M., Mirsky, G., Mizrahi, T., and T. Zhou, "Alternate-Marking Method", RFC 9341, DOI 10.17487/RFC9341, December 2022, <https://www.rfc-editor.org/info/rfc9341>.

[RFC9342] Fioccola, G., Ed., Cociglio, M., Sapio, A., Sisto, R., and T. Zhou, "Clustered Alternate-Marking Method", RFC 9342, DOI 10.17487/RFC9342, December 2022, <https://www.rfc-editor.org/info/rfc9342>.

[RFC9343] Fioccola, G., Zhou, T., Cociglio, M., Qin, F., and R. Pang, "IPv6 Application of the Alternate-Marking Method", RFC 9343, DOI 10.17487/RFC9343, December 2022, <https://www.rfc-editor.org/info/rfc9343>.

10.2. Informative References

[I-D.bonica-gendispatch-exp]
Bonica, R. and A. Farrel, "IETF Experiments", Work in Progress, Internet-Draft, draft-bonica-gendispatch-exp-06, 22 July 2025, <https://datatracker.ietf.org/doc/html/draft-bonica-gendispatch-exp-06>.

[I-D.ietf-6man-eh-limits]
Herbert, T., "Limits on Sending and Processing IPv6 Extension Headers", Work in Progress, Internet-Draft, draft-ietf-6man-eh-limits-19, 27 February 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-6man-eh-limits-19>.

[I-D.ietf-ippm-on-path-telemetry-yang]
Fioccola, G., Zhou, T., Zhu, Y., Zhang, W., and K. Zhu, "On-Path Telemetry YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-ippm-on-path-telemetry-yang-01, 2 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ippm-on-path-telemetry-yang-01>.

[I-D.ietf-opsawg-ipfix-on-path-telemetry]
Graf, T., Claise, B., and A. H. Feng, "Export of Delay Performance Metrics in IP Flow Information eXport (IPFIX)", Work in Progress, Internet-Draft, draft-ietf-opsawg-ipfix-on-path-telemetry-20, 23 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-opsawg-ipfix-on-path-telemetry-20>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/info/rfc8754>.

[RFC8799] Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", RFC 8799, DOI 10.17487/RFC8799, July 2020, <https://www.rfc-editor.org/info/rfc8799>.

[RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <https://www.rfc-editor.org/info/rfc8986>.

[RFC9098] Gont, F., Hilliard, N., Doering, G., Kumari, W., Huston, G., and W. Liu, "Operational Implications of IPv6 Packets with Extension Headers", RFC 9098, DOI 10.17487/RFC9098, September 2021, <https://www.rfc-editor.org/info/rfc9098>.

[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>.

Authors' Addresses

Giuseppe Fioccola
Huawei
Viale Martesana, 12
20055 Vimodrone (Milan)
Italy
Email: giuseppe.fioccola@huawei.com

Tianran Zhou
Huawei
156 Beiqing Rd.
Beijing
100095
China
Email: zhoutianran@huawei.com

Gyan S. Mishra
Verizon Inc.
Email: gyan.s.mishra@verizon.com

Xuewei Wang
Ruijie
Email: wangxuewei1@ruijie.com.cn

Geng Zhang
China Mobile
Email: zhanggeng@chinamobile.com

Mauro Cociglio
Email: mauro.cociglio@outlook.com