Stream: Internet Engineering Task Force (IETF)
RFC: 9486
Category: Standards Track
Published: September 2023
ISSN: 2070-1721
Authors: S. Bhandari, Ed. F. Brockners, Ed.
Thoughtspot *Cisco*

RFC 9486
IPv6 Options for In Situ Operations, Administration, and Maintenance (IOAM)

Abstract

In situ Operations, Administration, and Maintenance (IOAM) records operational and telemetry information in the packet while the packet traverses a path between two points in the network. This document outlines how IOAM Data-Fields are encapsulated in IPv6.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

In situ Operations, Administration, and Maintenance (IOAM) records operational and telemetry information in the packet while the packet traverses a path between two points in the network. IOAM concepts and associated nomenclature as well as IOAM Data-Fields are defined in [RFC9197]. This document outlines how IOAM Data-Fields are encapsulated in IPv6 [RFC8200] and discusses deployment requirements for networks that use IPv6-encapsulated IOAM Data-Fields.

The terms "encapsulation" and "decapsulation" are used in this document in the same way as in [RFC9197]: An IOAM encapsulating node incorporates one or more IOAM Option-Types into packets that IOAM is enabled for.

2. Conventions

2.1. 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.

2.2. Abbreviations

Abbreviations used in this document:

E2E: Edge-to-Edge

IOAM: In situ Operations, Administration, and Maintenance as defined in [RFC9197]

OAM: Operations, Administration, and Maintenance

POT: Proof of Transit

3. In situ OAM Metadata Transport in IPv6

IOAM in IPv6 is used to enhance diagnostics of IPv6 networks. It complements other mechanisms designed to enhance diagnostics of IPv6 networks, such as the "IPv6 Performance and Diagnostic Metrics (PDM) Destination Option" described in [RFC8250].

At the time this document was written, several implementations of IOAM for IPv6 exist, e.g., IOAM for IPv6 in the Linux Kernel (supported from Kernel version 5.15 onward, IPv6 IOAM in Linux Kernel) and IOAM for IPv6 in Vector Packet Processing (VPP).

IOAM Data-Fields can be encapsulated with two types of extension headers in IPv6 packets -- either the hop-by-hop options header or the destination options header. Multiple options with the same option type **MAY** appear in the same hop-by-hop options or destination options header with distinct content.

An IPv6 packet carrying IOAM data in an extension header can have other extension headers, compliant with [RFC8200].

```
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |  Option-Type  |  Opt Data Len |    Reserved     | IOAM Opt-Type |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+<-+
    |                                                               |  |
    .                                                               .  I
    .                                                               .  O
    .                                                               .  A
    .                                                               .  M
    .                                                               .  .
    .                          Option Data                          .  O
    .                                                               .  P
    .                                                               .  T
    .                                                               .  I
    .                                                               .  O
    .                                                               .  N
    |                                                               |  |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+<-+
```

Figure 1: IPv6 Hop-by-Hop and Destination Option Format for Carrying IOAM Data-Fields

Option-Type: 8-bit option type identifier as defined in Section 6.

Opt Data Len: 8-bit unsigned integer. Length of this option, in octets, not including the first 2 octets.

Reserved: 8-bit field **MUST** be set to zero by the source.

IOAM Option-Type: Abbreviated to "IOAM Opt-Type" in the diagram above: 8-bit field as defined in Section 4.1 of [RFC9197].

Option Data: Variable-length field. The data is specific to the Option-Type, as detailed below.

Pre-allocated Trace Option: The IOAM Pre-allocated Trace Option-Type, defined in Section 4.4 of [RFC9197], is represented as an IPv6 option in the hop-by-hop extension header:

Option-Type: 0x31 (8-bit identifier of the IPv6 Option-Type for IOAM).

IOAM Type: IOAM Pre-allocated Trace Option-Type.

Proof of Transit Option-Type: The IOAM POT Option-Type, defined in Section 4.5 of [RFC9197], is represented as an IPv6 option in the hop-by-hop extension header:

Option-Type: 0x31 (8-bit identifier of the IPv6 Option-Type for IOAM).

IOAM Type: IOAM POT Option-Type.

Edge-to-Edge Option: The IOAM E2E Option, defined in Section 4.6 of [RFC9197], is represented as an IPv6 option in destination extension header:

Option-Type: 0x11 (8-bit identifier of the IPv6 Option-Type for IOAM).

IOAM Type: IOAM E2E Option-Type.

Direct Export (DEX) Option: The IOAM Direct Export Option-Type, defined in Section 3.2 of [RFC9326], is represented as an IPv6 option in the hop-by-hop extension header:

Option-Type: 0x11 (8-bit identifier of the IPv6 Option-Type for IOAM).

IOAM Type: IOAM Direct Export (DEX) Option-Type.

All the IOAM IPv6 options defined here have alignment requirements. Specifically, they all require alignment on multiples of 4 bytes. This ensures that fields specified in [RFC9197] are aligned at a multiple-of-4 offset from the start of the hop-by-hop and destination options header.

IPv6 options can have a maximum length of 255 octets. Consequently, the total length of IOAM Option-Types including all data fields is also limited to 255 octets when encapsulated into IPv6.

4. IOAM Deployment in IPv6 Networks

4.1. Considerations for IOAM Deployment and Implementation in IPv6 Networks

IOAM deployments in IPv6 networks **MUST** take the following considerations and requirements into account.

C1: IOAM **MUST** be deployed in an IOAM-Domain. An IOAM-Domain is a set of nodes that use IOAM. An IOAM-Domain is bounded by its perimeter or edge. The set of nodes forming an IOAM-Domain may be connected to the same physical infrastructure (e.g., a service provider's network). They may also be remotely connected to each other (e.g., an enterprise VPN or an overlay). It is expected that all nodes in an IOAM-Domain are managed by the same administrative entity. Please refer to [RFC9197] for more details on IOAM-Domains.

C2: Implementations of IOAM **MUST** ensure that the addition of IOAM Data-Fields does not alter the way routers forward packets or the forwarding decisions they make. Packets with added IOAM information must follow the same path within the domain as an identical packet without IOAM information would, even in the presence of Equal-Cost Multipath (ECMP). This behavior is important for deployments where IOAM Data-Fields are only added "on-demand". Implementations of IOAM **MUST** ensure that ECMP behavior for packets with and without IOAM Data-Fields is the same. In order for IOAM to work in IPv6 networks, IOAM **MUST** be explicitly enabled per interface on every node within the IOAM-Domain. Unless a particular interface is explicitly enabled (i.e., explicitly configured) for IOAM, a router **MUST** ignore IOAM Options.

C3: In order to maintain the integrity of packets in an IOAM-Domain, the Maximum Transmission Unit (MTU) of transit routers and switches must be configured to a value that does not lead to an "ICMP Packet Too Big" error message being sent to the originator and the packet being dropped. The PMTU tolerance range must be identified, and IOAM encapsulation operations or data field insertion must not exceed this range. Control of the

MTU is critical to the proper operation of IOAM. The PMTU tolerance must be identified through configuration, and IOAM operations must not exceed the packet size beyond PMTU.

C4: [RFC8200] precludes insertion of IOAM data directly into the original IPv6 header of in-flight packets. IOAM deployments that do not encapsulate/decapsulate IOAM on the host but desire to encapsulate/decapsulate IOAM on transit nodes **MUST** add an additional IPv6 header to the original packet. IOAM data is added to this additional IPv6 header.

4.2. IOAM-Domains Bounded by Hosts

For deployments where the IOAM-Domain is bounded by hosts, hosts will perform the operation of IOAM Data-Field encapsulation and decapsulation, i.e., hosts will place the IOAM Data-Fields directly in the IPv6 header or remove the IOAM Data-Fields directly from the IPv6 header. IOAM data is carried in IPv6 packets as hop-by-hop or destination options as specified in this document.

4.3. IOAM-Domains Bounded by Network Devices

For deployments where the IOAM-Domain is bounded by network devices, network devices such as routers form the edge of an IOAM-Domain. Network devices will perform the operation of IOAM Data-Field encapsulation and decapsulation. Network devices will encapsulate IOAM Data-Fields in an additional, outer, IPv6 header that carries the IOAM Data-Fields.

5. Security Considerations

This document describes the encapsulation of IOAM Data-Fields in IPv6. For general IOAM security considerations, see [RFC9197]. Security considerations of the specific IOAM Data-Fields for each case (i.e., Trace, POT, and E2E) are also described and defined in [RFC9197].

As this document describes new options for IPv6, the security considerations of [RFC8200] and [RFC8250] apply.

From a network-protection perspective, there is an assumed trust model such that any node that adds IOAM to a packet, removes IOAM from a packet, or modifies IOAM Data-Fields of a packet is assumed to be allowed to do so. By default, packets that include IPv6 extension headers with IOAM information **MUST NOT** be leaked through the boundaries of the IOAM-Domain.

IOAM-Domain boundary routers **MUST** filter any incoming traffic from outside the IOAM-Domain that contains IPv6 extension headers with IOAM information. IOAM-Domain boundary routers **MUST** also filter any outgoing traffic leaving the IOAM-Domain that contains IPv6 extension headers with IOAM information.

In the general case, an IOAM node only adds, removes, or modifies an IPv6 extension header with IOAM information, if the directive to do so comes from a trusted source and the directive is validated.

Problems may occur if the above behaviors are not implemented or if the assumed trust model is violated (e.g., through a security breach). In addition to the security considerations discussed in [RFC9197], the security considerations associated with IPv6 extension headers listed in [RFC9098] apply.

5.1. Applicability of Authentication Header (AH)

The network devices in an IOAM-Domain are trusted to add, update, and remove IOAM options according to the constraints specified in [RFC8200]. IOAM-Domain does not rely on the AH as defined in [RFC4302] to secure IOAM options. The use of IOAM options with AH and its processing are not defined in this document. Future documents may define the use of IOAM with AH and its processing.

6. IANA Considerations

IANA has assigned the IPv6 Option-Types from the "Destination Options and Hop-by-Hop Options" subregistry of "Internet Protocol Version 6 (IPv6) Parameters" <https://www.iana.org/assignments/ipv6-parameters/>.

Hex Value	Binary Value			Description	Reference
	act	chg	rest		
0x11	00	0	10001	IOAM Destination Option and IOAM Hop-by-Hop Option	RFC 9486
0x31	00	1	10001	IOAM Destination Option and IOAM Hop-by-Hop Option	RFC 9486

Table 1

7. References

7.1. 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>.

[RFC9197] Brockners, F., Ed., Bhandari, S., Ed., and T. Mizrahi, Ed., "Data Fields for In Situ Operations, Administration, and Maintenance (IOAM)", RFC 9197, DOI 10.17487/RFC9197, May 2022, <https://www.rfc-editor.org/info/rfc9197>.

[RFC9326] Song, H., Gafni, B., Brockners, F., Bhandari, S., and T. Mizrahi, "In Situ Operations, Administration, and Maintenance (IOAM) Direct Exporting", RFC 9326, DOI 10.17487/RFC9326, November 2022, <https://www.rfc-editor.org/info/rfc9326>.

7.2. Informative References

[IPV6-RECORD-ROUTE] Kitamura, H., "Record Route for IPv6 (RR6) Hop-by-Hop Option Extension", Work in Progress, Internet-Draft, draft-kitamura-ipv6-record-route-00, 17 November 2000, <https://datatracker.ietf.org/doc/html/draft-kitamura-ipv6-record-route-00>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <https://www.rfc-editor.org/info/rfc4302>.

[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>.

[RFC8250] Elkins, N., Hamilton, R., and M. Ackermann, "IPv6 Performance and Diagnostic Metrics (PDM) Destination Option", RFC 8250, DOI 10.17487/RFC8250, September 2017, <https://www.rfc-editor.org/info/rfc8250>.

[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>.

Acknowledgements

The authors would like to thank Tom Herbert, Éric Vyncke, Nalini Elkins, Srihari Raghavan, Ranganathan T S, Karthik Babu Harichandra Babu, Akshaya Nadahalli, Stefano Previdi, Hemant Singh, Erik Nordmark, LJ Wobker, Mark Smith, Andrew Yourtchenko, and Justin Iurman for the comments and advice. For the IPv6 encapsulation, this document leverages concepts described in [IPV6-RECORD-ROUTE]. The authors would like to acknowledge the work done by the author Hiroshi Kitamura and people involved in writing it.

Contributors

This document was the collective effort of several authors. The text and content were contributed by the editors and the coauthors listed below.

Carlos Pignataro
Cisco Systems, Inc.
7200-11 Kit Creek Road
Research Triangle Park, NC 27709
United States of America
Email: cpignata@cisco.com

Hannes Gredler
RtBrick Inc.
Email: hannes@rtbrick.com

John Leddy
Email: john@leddy.net

Stephen Youell
JP Morgan Chase
25 Bank Street
London
E14 5JP
United Kingdom
Email: stephen.youell@jpmorgan.com

Tal Mizrahi
Huawei Network.IO Innovation Lab
Israel
Email: tal.mizrahi.phd@gmail.com

Aviv Kfir
Mellanox Technologies, Inc.
350 Oakmead Parkway, Suite 100
Sunnyvale, CA 94085
United States of America
Email: avivk@mellanox.com

Barak Gafni
Mellanox Technologies, Inc.
350 Oakmead Parkway, Suite 100
Sunnyvale, CA 94085
United States of America
Email: gbarak@mellanox.com

Petr Lapukhov
Facebook
1 Hacker Way
Menlo Park, CA 94025
United States of America
Email: petr@fb.com

Mickey Spiegel
Barefoot Networks, an Intel company
4750 Patrick Henry Drive
Santa Clara, CA 95054
United States of America
Email: mickey.spiegel@intel.com

Suresh Krishnan
Kaloom
Email: suresh@kaloom.com

Rajiv Asati
Cisco Systems, Inc.
7200 Kit Creek Road
Research Triangle Park, NC 27709
United States of America
Email: rajiva@cisco.com

Mark Smith
PO BOX 521
Heidelberg VIC 3084
Australia
Email: markzzzsmith+id@gmail.com

Authors' Addresses

Shwetha Bhandari (EDITOR)
Thoughtspot
3rd Floor, Indiqube Orion
24th Main Rd, Garden Layout, HSR Layout
Bangalore 560 102
Karnataka
India
Email: shwetha.bhandari@thoughtspot.com

Frank Brockners (EDITOR)
Cisco Systems, Inc.
Hansaallee 249, 3rd Floor
40549 Duesseldorf
Germany
Email: fbrockne@cisco.com