In-situ OAM IPv4 Options
draft-gafni-ippm-ioam-ipv4-options-00

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 IPv4.

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 September 10, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents.
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 the IPv4 [RFC0791].

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

OAM: Operations, Administration, and Maintenance

3. In-situ OAM Metadata Transport in IPv4

An IPv4 option is defined corresponding to each of the IOAM data fields defined in [I-D.ietf-ippm-ioam-data]. These mechanisms of in-situ OAM in IPv4 are used to enhance diagnostics of IPv4 networks. IOAM is carried in IPv4 packets as a new single option, with an option type identifier TBD_IOAM that will be defined by IANA, and according to the options definition in [RFC0791]. While specifying a new option to carry IOAM data, one may see this as an extension to the already defined "record route" and "internet timestamp" options in [RFC0791], which allows a packet to record its route and collect timestamps throughout the network. The various IOAM data fields defined in [I-D.ietf-ippm-ioam-data] are added as TLVs within the new IPv4 option. In an administrative domain where IOAM is used, insertion of the IOAM header in IPv4 is enabled at the IOAM domain edge, which serve as IOAM encapsulating/decapsulating nodes by means of configuration.

An IPv4 option format for carrying in-situ OAM data fields:
3.1. Considerations for in-situ OAM in IPv4 options

In the scope of IPv4 header and its options in [RFC0791], there are unique considerations for embedding in-situ OAM in the IPv4 options.

3.1.1. Alignment

Within an IPv4 options stack there is no requirement for alignment outside the octet granularity, which doesn’t limit the granularity of the in-situ OAM, since it is already 4-octects aligned.
3.1.2. Total available length

There are three fields that may affect the total available length for in-situ OAM data to be incorporated in the IPv4 options:

1. The IPv4 header’s IHL, as described in [RFC0791] in section 3.1:
   This 4-bit field can reach up to 15 times 4 octets, including the IPv4 header, which is 20 octets. This leaves a maximum actual length of 40 octets to the options. Reducing 4 octets for the use of the option’s header, it leaves 36 octets for the use of the in-situ OAM data. In the context of the trace type, which has an 8 octets header, this leaves 28 bytes for actual data to be collected during the packet’s traverse through the network.

2. The option’s length, as described here above in section 3: This 8-bit field can reach up to 255 octets. Doesn’t further restrict the in-situ OAM length, because of the above restrictions that are already applied.

3. Datagram’s Total length, as described in [RFC0791] in section 3.1: Doesn’t further restrict the in-situ OAM length, because of the above restrictions that are already applied.

3.1.3. Pre-allocation vs. Incremental trace types

Considering the IPv4 architecture, and specifically the "record route" and "internet timestamp" options definitions, the RFC calls for "The size of the option does not change due to adding addresses...", and similarly for the timestamp option. Hence, while incorporating In-situ OAM trace type header, an implementation SHOULD use one of these two techniques:

1. Immediate Export mode, controlled by the I-bit as part of the trace flags.

2. Pre-allocated trace type as described in section 4.1.1 of [I-D.ietf-ippm-ioam-data].

3.1.4. Checksum considerations

3.1.4.1. IP checksum

IPv4 Header Checksum, as described in [RFC0791] MUST be recalculated by a device that is updating the In-situ OAM IPv4 option.
3.1.4.2. TCP checksum

TCP’s pseudo header, as described in [RFC0793], doesn’t include neither the IPv4 options nor the IHL, hence doesn’t need to be recalculated by a device that is adding, removing or updating the in-situ OAM IPv4 option.

3.1.4.3. UDP checksum

UDP’s pseudo header, as described in [RFC0768], doesn’t include neither the IPv4 options nor the IHL, hence doesn’t need to be recalculated by a device that is adding, removing or updating the in-situ OAM IPv4 option.

3.1.5. Fragmentation

Considering the IPv4 architecture, and specifically the "record route" and "internet timestamp" options definitions, [RFC0791] is calling for setting the option’s copy to zero, hence "Not copied on fragmentation, goes in first fragment only". It seems reasonable to the authors to keep this idea to prevent duplication of route data and maintain similar behavior for the operator, hence an implementer SHOULD follow this method.

4. Security Considerations

This document describes the encapsulation of IOAM data fields in IPv4. Security considerations of the specific IOAM data fields for each case (i.e., Trace, Proof of Transit, and E2E) are described in defined in [I-D.ietf-ippm-ioam-data].

As this document describes a new option for IPv4, that is similar in their behavior to an already existing options, the security considerations are similar as well to those of [RFC0791].

5. IANA Considerations

This draft requests the following IPv4 Option Type assignments from sub-registry of Internet Protocol Version 4 (IPv4) Parameters:

TBD

6. References
6.1. Normative References

[I-D.ietf-ippm-ioam-data]
Brockners, F., Bhandari, S., Pignataro, C., Gredler, H.,
Leddy, J., Youell, S., Mizrahi, T., Mozes, D., Lapukhov,
P., Chang, R., and d. daniel.bernier@bell.ca, "Data Fields
for In-situ OAM", draft-ietf-ippm-ioam-data-01 (work in
progress), October 2017.

[RFC2119]  Bradner, S., "Key words for use in RFCs to Indicate
Requirement Levels", BCP 14, RFC 2119,
DOI 10.17487/RFC2119, March 1997,

[RFC8174]  Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,

6.2. Informative References

[RFC0768]  Postel, J., "User Datagram Protocol", STD 6, RFC 768,
DOI 10.17487/RFC0768, August 1980,
<https://www.rfc-editor.org/info/rfc768>.

[RFC0791]  Postel, J., "Internet Protocol", STD 5, RFC 791,
DOI 10.17487/RFC0791, September 1981,

[RFC0793]  Postel, J., "Transmission Control Protocol", STD 7,
RFC 793, DOI 10.17487/RFC0793, September 1981,
<https://www.rfc-editor.org/info/rfc793>.

Authors' Addresses

Barak Gafni
Mellanox Technologies, Inc.
350 Oakmead Parkway, Suite 100
Sunnyvale, CA  94085
U.S.A.

Email: gbarak@mellanox.com