Workgroup: BIER Working Group
Internet-Draft: draft-xzlnp-bier-ioam-07
Published: 1 February 2024
Intended Status: Standards Track
Expires: 4 August 2024
Authors: X. Min Z. Zhang Y. Liu
ZTE Corp. ZTE Corp. China Mobile
N. Nainar C. Pignataro
Cisco Systems, Inc. North Carolina State University

BIER Encapsulation for IOAM Data

Abstract

In-situ Operations, Administration, and Maintenance (IOAM) collects operational and telemetry information in the packet while the packet traverses a path between two points in the network. Bit Index Explicit Replication (BIER) is an architecture that provides optimal multicast forwarding through a "multicast domain", without requiring intermediate routers to maintain any per-flow state or to engage in an explicit tree-building protocol. The BIER header contains a bit-string in which each bit represents exactly one egress router to forward the packet to. This document outlines the requirements to carry IOAM data in BIER header and specifies how IOAM data is encapsulated in BIER header.

Table of Contents

1. Introduction

In-situ Operations, Administration, and Maintenance (IOAM) collects operational and telemetry information in the packet while the packet traverses a path between two points in the network. [RFC9197] defines four IOAM option types with different IOAM data fields used to record OAM information within the packet. [RFC9326] defines IOAM Direct Export (DEX) option type, which indicates OAM information to be collected without being embedded in the data packets. The term "in-situ" refers to the fact that the OAM data is added to the data packets rather than being sent within packets specifically dedicated to OAM.

Bit Index Explicit Replication (BIER), as defined in [RFC8279], is an architecture that provides optimal multicast forwarding through a "multicast domain", without requiring intermediate routers to maintain any per-flow state or to engage in an explicit tree-building protocol. The BIER header, as defined in [RFC8296], contains a bit-string in which each bit represents exactly one egress router to forward the packet to.

This document outlines the requirements to carry IOAM data in BIER header and specifies how IOAM data is encapsulated.

2. Conventions Used in This Document

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:

BFER: Bit Forwarding Egress Router

BFIR: Bit Forwarding Ingress Router

BIER: Bit Index Explicit Replication

DEX: Direct Export

GRE: Generic Routing Encapsulation

IOAM: In-situ Operations, Administration, and Maintenance

OAM: Operations, Administration, and Maintenance

3. Requirements to carry IOAM data

[I-D.ietf-bier-use-cases] lists many use cases for BIER. Usually there are many multicast flows within one network domain, and some of the multicast flows, such as live video and real-time meeting, are sensitive to packet loss, delay and other factors. The network operator wants to know the real-time statistics for these flows, such as delay, sequence, the ingress/egress interface, and the usage of buffer.

So methods are needed for measuring the real-time transportation guarantee of BIER packets. This document attempts to provide a way to carry IOAM data in the BIER packets.

4. IOAM data fields encapsulation in BIER header

The BIER header is defined in [RFC8279]. The BIER OAM header that follows BIER header is defined in [I-D.ietf-bier-ping]. IOAM-Data-Fields can either be carried in BIER using a new type of OAM message

which follows the BIER OAM header (referred to as option 1), or be carried in BIER using a new next protocol header which immediately follows the BIER header (referred to as option 2). In this document, option 2 is selected and the reason is discussed in Section 5.1. An IOAM header is added containing different IOAM-Data-Fields defined in [RFC9197] and [RFC9326].

[Editor's Note: Except for aforementioned option 1 and 2, IOAM-Data-Fields can also be carried in BIER extension header [I-D.zzhang-bier-extension-headers], which is referred to as option 3. Once there is WG consensus to adopt BIER extension header, the selected BIER IOAM Encapsulation would be changed from option 2 to option 3.]

In a BIER domain where IOAM is applied, inserting the IOAM header into the BIER packets is enabled at the BFIRs, which also serve as the IOAM encapsulating nodes by means of configuration. Deleting the IOAM header from the BIER packets is enabled at the BFERs, which also serve as the IOAM decapsulating nodes by means of configuration.

The Encapsulation format for IOAM over BIER is defined as follows:

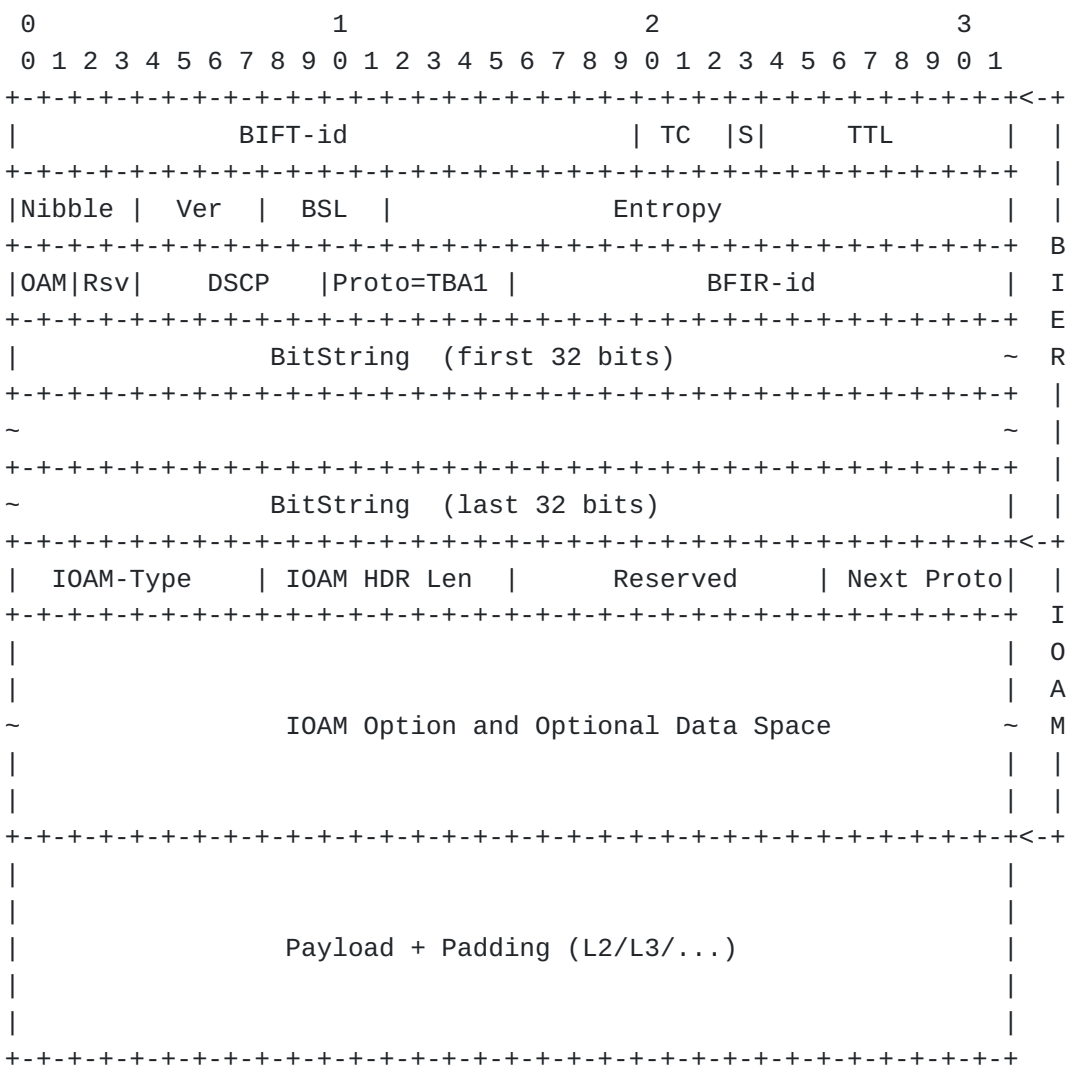

Figure 1: IOAM Encapsulation Format within BIER

The BIER header and fields are defined in [RFC8296]. Within the BIER header, a 6-bit field as "Proto" (Next Protocol) is used to identify the type of the payload immediately following the BIER header, The "Proto" value is set to TBA1 when the IOAM header is present.

The IOAM related fields in BIER are defined as follows:

IOAM-Type: An 8-bit field defining the IOAM option type, as defined in Section 7.1 of [RFC9197] and Section 4.1 of [RFC9326].

IOAM HDR Len: An 8-bit unsigned integer. Length of the IOAM header in 4-octet units.

Reserved: A 10-bit reserved field MUST be set to zero upon transmission and ignored upon receipt.

Next Proto: A 6-bit unsigned integer that identifies the type of payload immediately following this IOAM option. The semantics of this field are identical to the "Proto" field in [RFC8296].

IOAM Option and Optional Data Space: IOAM option header and data as specified by the IOAM-Type field. They're defined in Section 4 of [RFC9197] and Section 3 of [RFC9326].

Multiple IOAM options MAY be included within a BIER encapsulation. For example, if a BIER encapsulation contains two IOAM options preceding a data payload, the "Next Proto" field of the first IOAM option would be set to the value of TBA1 that indicates a second IOAM option follows, while the "Next Proto" field of the second IOAM option would be set to the value of "BIER Next Protocol" indicating the type of the data payload. Each type of IOAM option MUST occur at most once within a BIER encapsulation.

Note that in a BIER multicast network, if the IOAM Trace option is carried in the BIER packets, when the BIER packets are replicated at the branch nodes, the IOAM Trace option would be replicated too. In a case it's a concern to the network operator, the IOAM DEX option may be used as a substitution, or other methods beyond the scope of this document can be applied.

5. Considerations

This section summarizes a set of considerations on the overall approach taken for IOAM data encapsulation in BIER, as well as deployment considerations.

5.1. Selecting the encapsulation approach

Both the encapsulation options for IOAM over BIER described in Section 4 are supposed to be feasible, nevertheless this document needs to select one as the standardized encapsulation. Considering the fact that the encapsulation format of option 2 using a new next protocol header is more concise than option 1 using a new type of OAM message, and many other transport protocols, e.g., GRE, use a new next protocol header to encapsulate IOAM data, the encapsulation format of option 2 is selected as the standardized one.

5.2. Interaction with the BIER OAM field

[RFC8296] defines a two-bit field, referred to as OAM. [I-D.ietf-bier-pmmm-oam] describes how to use the two-bit OAM field for alternate-marking performance measurement method. This document would not change the semantics of the two-bit OAM field. The BIER IOAM header and the BIER OAM field are orthogonal and they can co-exist in one packet, i.e., a BIER packet with IOAM data can set the OAM field and a BIER packet with OAM field set can carry IOAM data.

6. Security Considerations

This document describes the encapsulation of IOAM data in BIER. Security considerations of the specific IOAM data are described in [RFC9197] and [RFC9326].

IOAM is considered a "per domain" feature, where one or several operators decide on configuring IOAM according to their needs. IOAM is expected to be deployed in a limited domain [RFC8799]. As such, it assumes that a node involved in IOAM operation has previously verified the integrity of the path. Still, the operators need to properly secure the IOAM domain to avoid malicious configuration and use, which could include injecting malicious IOAM packets into the domain.

As this document describes new protocol fields within the existing BIER encapsulation, these are similar to the security considerations of [RFC8296].

7. IANA Considerations

In the "BIER Next Protocol Identifiers" registry created for [RFC8296], a new Next Protocol Value for IOAM is requested from IANA as follows:

BIER Next Protocol Identifier	Description	Semantics Definition	Reference
TBA1	In-situ OAM (IOAM)	Section 4	This Document

Table 1: New BIER Next Protocol Identifier

8. Acknowledgements

The authors would like to acknowledge Greg Mirsky for his thorough review and very helpful comments.

9. References

9.1. 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>.

[RFC8279] Wijnands, IJ., Ed., Rosen, E., Ed., Dolganow, A., Przygienda, T., and S. Aldrin, "Multicast Using Bit Index Explicit Replication (BIER)", RFC 8279, DOI 10.17487/RFC8279, November 2017, <https://www.rfc-editor.org/info/rfc8279>.

[RFC8296] Wijnands, IJ., Ed., Rosen, E., Ed., Dolganow, A., Tantsura, J., Aldrin, S., and I. Meilik, "Encapsulation for Bit Index Explicit Replication (BIER) in MPLS and Non-MPLS Networks", RFC 8296, DOI 10.17487/RFC8296, January 2018, <https://www.rfc-editor.org/info/rfc8296>.

[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>.

9.2. Informative References

[I-D.ietf-bier-ping] Nainar, N. K., Pignataro, C., Chen, M., and G. Mirsky, "BIER Ping and Trace", Work in Progress, Internet-Draft, draft-ietf-bier-ping-13, 27 January 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-bier-ping-13>.

[I-D.ietf-bier-pmmm-oam] Mirsky, G., Zheng, L., Chen, M., and G. Fioccola, "Performance Measurement (PM) with Marking Method in Bit Index Explicit Replication (BIER) Layer", Work in Progress, Internet-Draft, draft-ietf-bier-pmmm-oam-15, 11 January 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-bier-pmmm-oam-15>.

[I-D.ietf-bier-use-cases] Nainar, N. K., Asati, R., Chen, M., Xu, X., Dolganow, A., Przygienda, T., Gulko, A., Robinson, D., Arya, V., and C. Bestler, "BIER Use Cases", Work in Progress, Internet-Draft, draft-ietf-bier-use-cases-12, 10 September 2020, <https://datatracker.ietf.org/doc/html/draft-ietf-bier-use-cases-12>.

[I-D.zzhang-bier-extension-headers] Zhang, Z. J., Min, X., Liu, Y., and H. Bidgoli, "BIER Extension Headers", Work in Progress, Internet-Draft, draft-zzhang-bier-extension-

headers-02, 25 January 2024, <https://datatracker.ietf.org/doc/html/draft-zzhang-bier-extension-headers-02>.

[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>.

Authors' Addresses

Xiao Min
ZTE Corp.
Nanjing
China

Email: xiao.min2@zte.com.cn

Zheng(Sandy) Zhang
ZTE Corp.
Nanjing
China

Email: zhang.zheng@zte.com.cn

Yisong Liu
China Mobile
Beijing
China

Email: liuyisong@chinamobile.com

Nagendra Kumar Nainar
Cisco Systems, Inc.
7200-11 Kit Creek Road
Research Triangle Park, NC 27709
United States of America

Email: naikumar@cisco.com

Carlos Pignataro
North Carolina State University
United States of America

Email: cpignata@gmail.com, cmpignat@ncsu.edu