Network
Internet-Draft
Intended status: Standards Track
Expires: 18 May 2026

Shaofu. Peng
ZTE Corporation

14 November 2025

Fragment Header for PREOF
draft-peng-detnet-fh-preof-00

Abstract

This document re-use IPv6 Fragment Header to support DetNet Packet Replication, Elimination, and Ordering Functions (PREOF).

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 18 May 2026.

Copyright Notice

Table of Contents

1. Introduction

DetNet architecture [RFC8655] defined service protection that aims to mitigate or eliminate packet loss due to equipment failures, including random media and/or memory faults. These types of packet loss can be greatly reduced by spreading the data over multiple disjoint forwarding paths. Service protection includes three functions: Packet Replication Function (PRF), Packet Elimination Function (PEF), and Packet Ordering Function (POF). These functions are collectively referred to as PREOF. In general, the use of PREOF require sequencing information to be included in the packets of a DetNet compound flow.

The current IPv6 specification lacks support for sequence number information and relies on other methods, such as inserting MPLS labels and associated control word in IPv6 encapsulation, as defined in [RFC9566], which is high cost and requires the IPv6 data plane to support additional logic beyond pure IPv6 forwarding.

[RFC8200] defines Fragment Header (FH), which can be used by IPv6 sources to fragment packets when their size exceeds the MTU of the transmission path. The identification field of FH is used to identifying multiple fragments belonging to the same original large packet. That is, fragment packets belonging to the same original packet must have the same Identification and flow identifiers (such as IP 5-tuple). If there are different original packets that need to be fragmented between the same source and destination, their identification must be different.

This document re-use the existing Identification field of FH to carry sequence number information, without any new defined functions to the IPv6 data plane, as a low cost encapsulation method to support DetNet PREOF.

1.1. 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. Fragment Header Extensions

As defined in [RFC8200], Fragment Header has the following format:

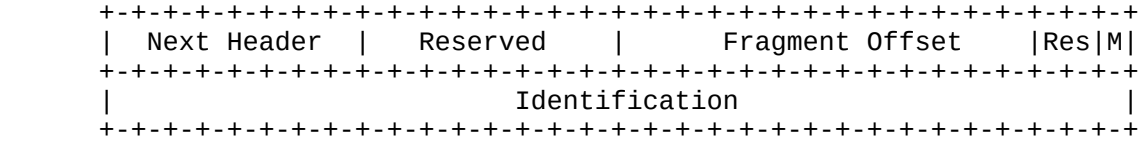

Figure 1

Fragment Offset indicates the offset of the starting position of a fragment relative to the the original fragmented packet. For example, the offset of the first fragment is 0, the offset of the second fragment is the length of the first fragment, and so on.

Flag M indicates whether it is the last fragment of the original packet. If M =0, it is the last fragment; Otherwise, not.

Identification field is used to identify the original package.

This document redefines the Identification field of FH: it is not only used to identify the original packet, but also to represent the sequence number of the original packet of the same flow. The flow identifier may use IP 5-tuple or 6-tuple.

The above new definition make no modifactions to the existing fragment logic, but just impose a constraint on the assignment value of the Identification, i.e., the Identification field MUST be incremented by one for each new App-flow packet sent under the context of that flow.

For data packets that need to be re-ordered, such as packets forwarded along PW (pseudo-wire) or DetNet PREOF paths, FH can be specified to carry the sequence number, by signaling negotiation or configuration, but that is out the scope of this document.

For any flow, the Identification of the first data packet sent by the source must be set to 1, and increased by 1 for each subsequent packet. Here, the mentioned packet is the original packet before fragment.

For a given original packet, if it is not fragmented, the Fragment Offset and flag M are both set to 0, to indicate that the packet is an independent complete packet. This setting is typical in DetNet, where fragmentation should be avoided as suggested in [RFC8939].

For a given original packet, if it is fragmented, the Fragment Offset, flag M, and Identification of each fragment packet is set according to the [RFC8200] . Note that fragments don’t include the transport headers, and may affect the identification of DetNet flow, such as being mistaken for low priority flows. However, EDP (Enhanced DetNet Data Plane) generally contains additional metadata in the IPv6 header for deterministic forwarding, without relying on decapsulate the transport header.

If an IPv6 node implements packets replication or elimination function, it may uniformly determine whether two packets of the same flow are duplicated based on whether their Identification, Fragment Offset and flag M parameters are the same, regardless of whether they are original packet or fragment packet. The original packet may indeed be treated as a special fragment packet.

Eliminating redundant packets and retaining only one copy will make the subsequent reassembly process simpler. However, even without implementing elimination, the fragment reassembly process defined in [RFC8200] can be re-used to filter out duplicate packets.

3. IANA Considerations

There are no IANA requirements in this document.

4. Security Considerations

There are no new DetNet-related security considerations in this document, please refer to [RFC8939] for basic security considerations in DetNet IP data plane.

5. Acknowledgements

TBD.

6. 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>.

[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>.

[RFC8655] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <https://www.rfc-editor.org/info/rfc8655>.

[RFC8939] Varga, B., Ed., Farkas, J., Berger, L., Fedyk, D., and S. Bryant, "Deterministic Networking (DetNet) Data Plane: IP", RFC 8939, DOI 10.17487/RFC8939, November 2020, <https://www.rfc-editor.org/info/rfc8939>.

[RFC9566] Varga, B., Farkas, J., and A. Malis, "Deterministic Networking (DetNet) Packet Replication, Elimination, and Ordering Functions (PREOF) via MPLS over UDP/IP", RFC 9566, DOI 10.17487/RFC9566, April 2024, <https://www.rfc-editor.org/info/rfc9566>.

Author’s Address

Shaofu Peng
ZTE Corporation
China
Email: peng.shaofu@zte.com.cn