Workgroup: DetNet
Internet-Draft:
draft-ietf-detnet-mpls-over-ip-preof-11
Published: 22 February 2024
Intended Status: Informational
Expires: 25 August 2024
Authors: B. Varga J. Farkas A. Malis
Ericsson Ericsson Malis Consulting

Deterministic Networking (DetNet): DetNet PREOF via MPLS over UDP/IP

Abstract

This document describes how DetNet IP data plane can support the Packet Replication, Elimination, and Ordering Functions (PREOF) built on the existing MPLS PREOF solution defined for DetNet MPLS Data Plane and the mechanisms defined by MPLS-over-UDP technology.

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 25 August 2024.

Table of Contents

1. Introduction

The DetNet Working Group has defined Packet Replication (PRF), Packet Elimination (PEF) and Packet Ordering (POF) functions (represented as PREOF) to provide service protection by the DetNet service sub-layer [RFC8655]. The PREOF service protection method relies on copies of the same packet sent over multiple maximally disjoint paths and uses sequencing information to eliminate duplicates. A possible implementation of the PRF and PEF functions is described in [IEEE8021CB] and the related YANG data model is defined in [IEEEP8021CBcv]. A possible implementation of the POF function is described in [I-D.ietf-detnet-pof]. Figure 1 shows a DetNet flow on which PREOF functions are applied during forwarding from the source to the destination.

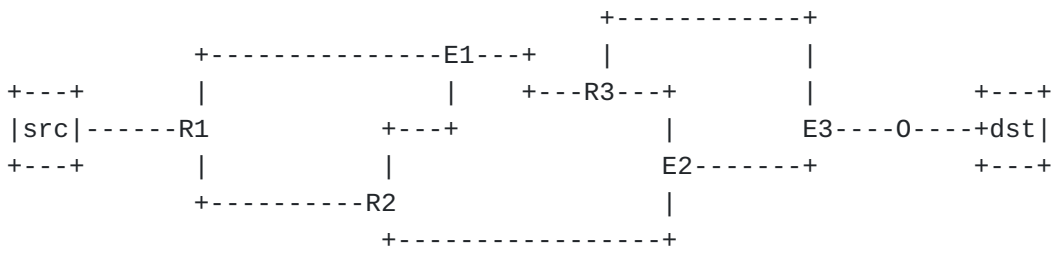

Figure 1: PREOF scenario in a DetNet network

In general, the use of PREOF functions require sequencing information to be included in the packets of a DetNet compound flow. This can be done by adding a sequence number or time stamp as part of DetNet encapsulation. Sequencing information is typically added once, at or close to the source.

The DetNet MPLS data plane [RFC8964] specifies how sequencing information is encoded in the MPLS header. However, the DetNet IP data plane described in [RFC8939] does not specify how sequencing information can be encoded in the IP packet. This document provides sequencing information to DetNet IP nodes, so it results in an improved version of the DetNet IP data plane. As suggested by [RFC8938], the solution uses existing standardized headers and encapsulations. The improvement is achieved by re-using the DetNet MPLS over UDP/IP data plane [RFC9025] with the restriction of using zero F-labels.

2. Terminology

2.1. Terms Used in This Document

This document uses the terminology established in the DetNet architecture [RFC8655], and the reader is assumed to be familiar with that document and its terminology.

2.2. Abbreviations

The following abbreviations are used in this document:

DetNet Deterministic Networking.

PEF Packet Elimination Function.

POF Packet Ordering Function.

PREOF
Packet Replication, Elimination and Ordering Functions.

PRF Packet Replication Function.

3. Requirements for adding PREOF to DetNet IP

The requirements for adding PREOF to DetNet IP are:

- to reuse existing DetNet data plane solutions (e.g., [RFC8964], [RFC9025]).

- to allow the DetNet service sub-layer for IP packet switched networks with minimal implementation effort.

The described solution practically gains from MPLS header fields without requiring the support of the MPLS forwarding plane.

4. Adding PREOF to DetNet IP

4.1. Solution Basics

The DetNet IP encapsulation supporting DetNet Service sub-layer is based on the "UDP tunneling" concept. The solution creates a set of underlay UDP/IP tunnels between an overlay set of DetNet relay nodes.

At the edge of a PREOF capable DetNet IP domain the DetNet flow is encapsulated in an UDP packet containing the sequence number used by PREOF functions within the domain. This solution maintains the 6-tuple-based DetNet flow identification in DetNet transit nodes, which operate at the DetNet forwarding sub-layer between the DetNet service sub-layer nodes; therefore, it is compatible with [RFC8939]. Figure 2 shows how the PREOF capable DetNet IP data plane fits into the DetNet sub-layers.

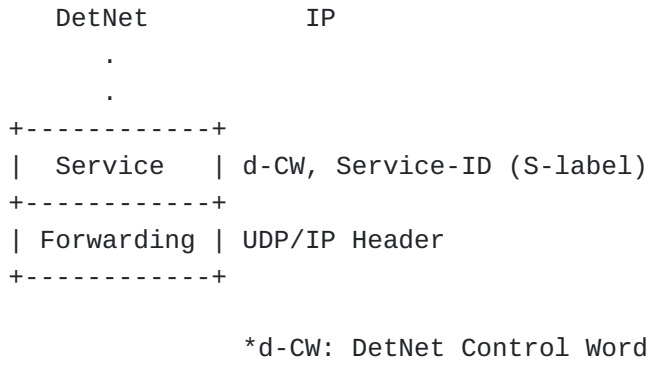

Figure 2: PREOF capable DetNet IP data plane

4.2. Encapsulation

The PREOF capable DetNet IP encapsulation builds on encapsulating DetNet PseudoWire (PW) directly over UDP. That is, it combines DetNet MPLS [RFC8964] with DetNet MPLS-in-UDP [RFC9025], without using any F-Labels as shown in Figure 3. DetNet flows are identified at the receiving DetNet service sub-layer processing node via the S-Label and/or the UDP/IP header information. Sequencing information for PREOF is provided by the DetNet Control Word (d-CW) as per [RFC8964]. The S-label is used to identify both the DetNet flow and the DetNet App-flow type. The UDP tunnel is used to direct the packet across the DetNet domain to the next DetNet service sub-layer processing node.

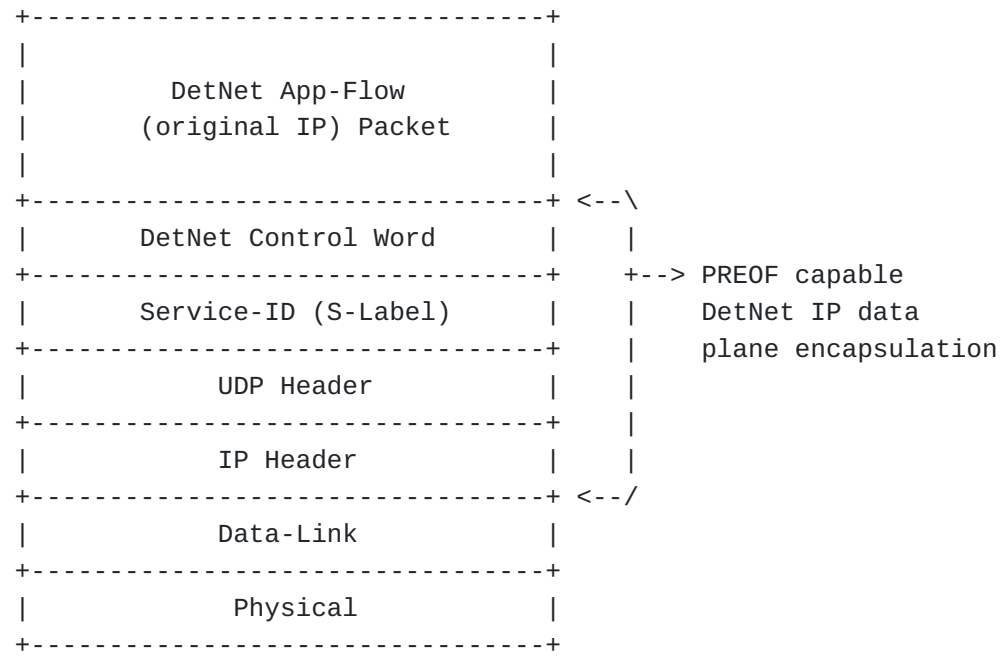

Figure 3: PREOF capable DetNet IP encapsulation

4.3. Packet Processing

IP ingress and egress nodes of the PREOF capable DetNet IP domain add and remove a DetNet service-specific d-CW and Service-ID (i.e., S-Label). Relay nodes can change Service-ID values when processing a DetNet flow, i.e., incoming and outgoing Service-IDs of a DetNet flow can be different. Service-ID values are provisioned per DetNet service via configuration, e.g., via the Controller Plane described in [RFC8938]. In some PREOF topologies, the node performing replication sends the packets to multiple nodes performing e.g., PEF

or POF and the replication node can use different Service-ID values for the different member flows for the same DetNet service.

Note, that Service-IDs is a local ID on the receiver side providing identification of the DetNet flow at the downstream DetNet service sub-layer receiver.

4.4. Flow Aggregation

Two methods can be used for flow aggregation:

- *aggregation using same UDP tunnel,
- *aggregating DetNet flows as a new DetNet flow.

In the first case, the different DetNet PseudoWires use the same UDP tunnel, so they are treated as a single (aggregated) flow at the forwarding sub-layer. At the service sub-layer, each flow uses a different Service ID (see Figure 3).

For the second option, an additional hierarchy is created thanks to an additional Service-ID and d-CW tuple added to the encapsulation. The Aggregate-ID is a special case of a Service-ID, whose properties are known only at the aggregation and de-aggregation end points. It is a property of the Aggregate-ID that it is followed by a d-CW followed by a Service-ID/d-CW tuple. Figure 4 shows the encapsulation in case of aggregation.

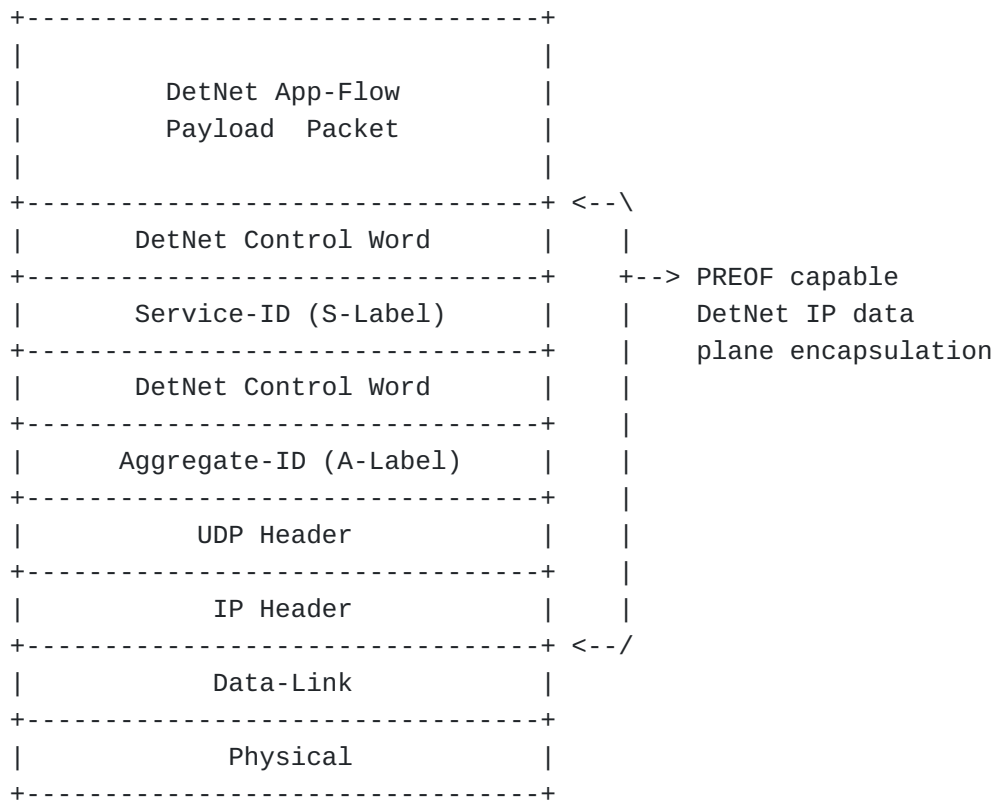

Figure 4: Aggregating DetNet flows as a new DetNet flow

The option used for aggregation is known by configuration of the aggregation/de-aggregation nodes.

If several Detnet flows are aggregated in a single UDP tunnel, they all need to follow the same path in the network.

4.5. PREOF Processing

A node operating on a received DetNet flow at the DetNet service sub-layer uses the local context associated with a received Service-ID to determine which local DetNet operation(s) are applied to received packet. A Service-ID can be allocated to be unique and enabling DetNet flow identification regardless of which input interface or UDP tunnel the packet is received. It is important to note that Service-ID values are driven by the receiver, not the sender.

The DetNet forwarding sub-layer is supported by the UDP tunnel and is responsible for providing resource allocation and explicit routes.

The outgoing PREOF encapsulation and processing can be implemented via the provisioning of UDP and IP header information. Note, when

PRF is performed at the DetNet service sub-layer, there are multiple member flows, and each member flow requires their own Service-ID, UDP and IP header information. The headers for each outgoing packet are formatted according to the configuration information, and the UDP Source Port value is set to uniquely identify the DetNet flow. The packet is then handled as a PREOF capable DetNet IP packet.

The incoming PREOF processing can be implemented via the provisioning of received Service-ID, UDP and IP header information. The provisioned information is used to identify incoming app-flows based on the combination of Service-ID and/or incoming encapsulation header information.

4.6. PREOF capable DetNet IP domain

Figure 5 shows using PREOF in a PREOF capable DetNet IP network, where service protection is provided end to end, an not only within sub-networks like depicted in Figure 4 of [RFC8939].

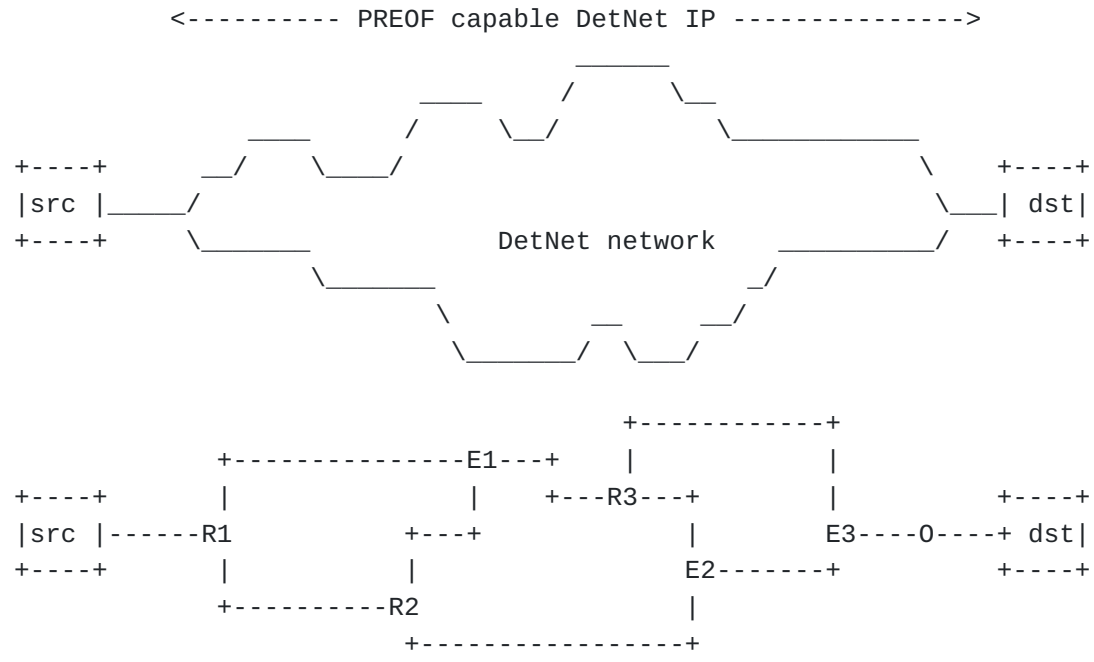

Figure 5: PREOF capable DetNet IP domain

5. Control and Management Plane Parameters

The information needed to identify individual and aggregated DetNet flows is summarized as follows:

* Service-ID information to be mapped to UDP/IP flows. Note that, for example, a single Service-ID can map to multiple sets of UDP/IP information when PREOF is used.

* IPv4 or IPv6 source address field.

* IPv4 or IPv6 source address prefix length, where a zero (0) value effectively means that the address field is ignored.

* IPv4 or IPv6 destination address field.

* IPv4 or IPv6 destination address prefix length, where a zero (0) effectively means that the address field is ignored.

* IPv6 flow label field.

* IPv4 protocol field being equal to "UDP".

* IPv6 (last) next header field being equal to "UDP".

* For the IPv4 Type of Service and IPv6 Traffic Class Fields:

  - Whether or not the DSCP field is used in flow identification as the use of the DSCP field for flow identification is optional.

  - If the DSCP field is used to identify a flow, then the flow identification information (for that flow) includes a list of DSCPs used by the given DetNet flow.

* UDP Source Port. Support for both exact and wildcard matching is required. Port ranges can optionally be used.

* UDP Destination Port. Support for both exact and wildcard matching is required. Port ranges can optionally be used.

* For end systems, an optional maximum IP packet size that should be used for that outgoing DetNet IP flow.

This information is provisioned per DetNet flow via configuration, e.g., via the controller plane.

Ordering of the set of information used to identify an individual DetNet flow can, for example, be used to provide a DetNet service for a specific UDP flow, with unique Source and Destination Port

field values, while providing a different service for the aggregate of all other flows with that same UDP Destination Port value.

The minimum set of information for the configuration of the DetNet service sub-layer is summarized as follows:

- *App-flow identification information.
- *Sequence number length.
- *PREOF + related Service-ID(s).
- *Associated forwarding sub-layer information.
- *Service aggregation information.

The minimum set of information for the configuration of the DetNet forwarding sub-layer is summarized as follows:

- *UDP tunnel specific information.
- *Traffic parameters.

These parameters are defined in the DetNet Flow and Service information model [RFC9016] and the DetNet YANG model.

Note: this document focuses on the use of MPLS over UDP/IP encapsulation throughout an entire DetNet IP network, making MPLS-based DetNet OAM techniques applicable [I-D.ietf-detnet-mpls-oam]. Using the described encapsulation only for a portion of a DetNet IP network that handles the PREOF functionality would complicate OAM.

6. Security Considerations

There are no new DetNet related security considerations introduced by this solution. Security considerations of DetNet MPLS [RFC8964] and DetNet MPLS over UDP/IP [RFC9025] apply.

7. IANA Considerations

This document makes no IANA requests.

8. Acknowledgements

Authors extend their appreciation to Stewart Bryant, Pascal Thubert, David Black, Shirley Yangfan and Greg Mirsky for their insightful comments and productive discussion that helped to improve the document.

9. References

9.1. Normative References

[I-D.ietf-detnet-mpls-oam] Mirsky, G., Chen, M., and B. Varga, "Operations, Administration and Maintenance (OAM) for Deterministic Networks (DetNet) with MPLS Data Plane", Work in Progress, Internet-Draft, draft-ietf-detnet-mpls-oam-15, 12 January 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-detnet-mpls-oam-15>.

[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>.

[RFC8938] Varga, B., Ed., Farkas, J., Berger, L., Malis, A., and S. Bryant, "Deterministic Networking (DetNet) Data Plane Framework", RFC 8938, DOI 10.17487/RFC8938, November 2020, <https://www.rfc-editor.org/info/rfc8938>.

[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>.

[RFC8964] Varga, B., Ed., Farkas, J., Berger, L., Malis, A., Bryant, S., and J. Korhonen, "Deterministic Networking (DetNet) Data Plane: MPLS", RFC 8964, DOI 10.17487/RFC8964, January 2021, <https://www.rfc-editor.org/info/rfc8964>.

[RFC9016] Varga, B., Farkas, J., Cummings, R., Jiang, Y., and D. Fedyk, "Flow and Service Information Model for Deterministic Networking (DetNet)", RFC 9016, DOI 10.17487/RFC9016, March 2021, <https://www.rfc-editor.org/info/rfc9016>.

[RFC9025] Varga, B., Ed., Farkas, J., Berger, L., Malis, A., and S. Bryant, "Deterministic Networking (DetNet) Data Plane: MPLS over UDP/IP", RFC 9025, DOI 10.17487/RFC9025, April 2021, <https://www.rfc-editor.org/info/rfc9025>.

9.2. Informative References

[I-D.ietf-detnet-pof] Varga, B., Farkas, J., Kehrer, S., and T. Heer, "Deterministic Networking (DetNet): Packet Ordering Function", Work in Progress, Internet-Draft, draft-ietf-detnet-pof-11, 15 January 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-detnet-pof-11>.

[IEEE8021CB]
IEEE, "IEEE Standard for Local and metropolitan area networks -- Frame Replication and Elimination for Reliability", DOI 10.1109/IEEESTD.2017.8091139, October 2017, <https://standards.ieee.org/standard/802_1CB-2017.html>.

[IEEEP8021CBcv] Kehrer, S., "FRER YANG Data Model and Management Information Base Module", IEEE P802.1CBcv /D1.2 P802.1CBcv, March 2021, <https://www.ieee802.org/1/files/private/cv-drafts/d1/802-1CBcv-d1-2.pdf>.

Authors' Addresses

Balazs Varga
Ericsson
Budapest
Magyar Tudosok krt. 11.
1117
Hungary

Email: balazs.a.varga@ericsson.com

Janos Farkas
Ericsson
Budapest
Magyar Tudosok krt. 11.
1117
Hungary

Email: janos.farkas@ericsson.com

Andrew G. Malis
Malis Consulting

Email: agmalis@gmail.com