

Workgroup: DetNet

Internet-Draft:

draft-ietf-detnet-oam-framework-11

Published: 8 January 2024

Intended Status: Informational

Expires: 11 July 2024

Authors: G. Mirsky    F. Theoleyre    G.Z. Papadopoulos  
         Ericsson        CNRS                    IMT Atlantique  
         CJ. Bernardos    B. Varga            J. Farkas  
         UC3M                    Ericsson            Ericsson

**Framework of Operations, Administration and Maintenance (OAM) for  
Deterministic Networking (DetNet)**

**Abstract**

Deterministic Networking (DetNet), as defined in RFC 8655, aims to provide bounded end-to-end latency on top of the network infrastructure, comprising both Layer 2 bridged and Layer 3 routed segments. This document's primary purpose is to detail the specific requirements of the Operation, Administration, and Maintenance (OAM) recommended to maintain a deterministic network. The document will be used in future work that defines the applicability of and extension of OAM protocols for a deterministic network. With the implementation of the OAM framework in DetNet, an operator will have a real-time view of the network infrastructure regarding the network's ability to respect the Service Level Objective, such as packet delay, delay variation, and packet loss ratio, assigned to each DetNet flow.

**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 11 July 2024.

## Copyright Notice

Copyright (c) 2024 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 carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

- [1. Introduction](#)
    - [1.1. Definitions](#)
    - [1.2. Abbreviations](#)
    - [1.3. Requirements Language](#)
  - [2. Role of OAM in DetNet](#)
  - [3. Operation](#)
    - [3.1. Information Collection](#)
    - [3.2. Continuity Check](#)
    - [3.3. Connectivity Verification](#)
    - [3.4. Route Tracing](#)
    - [3.5. Fault Verification/Detection](#)
    - [3.6. Fault Localization and Characterization](#)
    - [3.7. Use of Hybrid OAM in DetNet](#)
  - [4. Administration](#)
    - [4.1. Collection of metrics](#)
    - [4.2. Worst-case metrics](#)
  - [5. Maintenance](#)
    - [5.1. Replication / Elimination](#)
    - [5.2. Resource Reservation](#)
  - [6. Requirements](#)
    - [6.1. For the DetNet Forwarding Sub-layer](#)
    - [6.2. For the DetNet Service Sub-layer](#)
  - [7. IANA Considerations](#)
  - [8. Security Considerations](#)
  - [9. Privacy Considerations](#)
  - [10. Acknowledgments](#)
  - [11. References](#)
    - [11.1. Normative References](#)
    - [11.2. Informative References](#)
- [Authors' Addresses](#)

## 1. Introduction

Deterministic Networking (DetNet) [[RFC8655](#)] has proposed to provide a bounded end-to-end latency on top of the network infrastructure, comprising both Layer 2 bridged and Layer 3 routed segments. That work encompasses the data plane, OAM, time synchronization, management, control, and security aspects.

Operations, Administration, and Maintenance (OAM) Tools are of primary importance for IP networks [[RFC7276](#)]. DetNet OAM should provide a toolset for fault detection, localization, and performance measurement.

This document's primary purpose is to detail the specific requirements of the OAM features recommended to maintain a deterministic/reliable network. Specifically, it investigates the requirements for a deterministic network, supporting critical flows.

In this document, the term OAM will be used according to its definition specified in [[RFC6291](#)]. DetNet expects to implement an OAM framework to maintain a real-time view of the network infrastructure, and its ability to respect the Service Level Objectives (SLOs), such as in-order packet delivery, packet delay, delay variation, and packet loss ratio, assigned to each DetNet flow.

This document lists the functional requirements toward OAM for a DetNet domain. The list can further be used for gap analysis of available OAM tools to identify possible enhancements of existing or whether new OAM tools are required to support proactive and on-demand path monitoring and service validation.

### 1.1. Definitions

This document uses definitions, particularly of a DetNet flow, provided in Section 2.1 of [[RFC8655](#)]. The following terms are used throughout this document as defined below:

\*DetNet OAM domain: a DetNet network used by the monitored DetNet flow. A DetNet OAM domain (also referred to in this document as "OAM domain") may have MEPs on its edge and MIPs within.

\*DetNet OAM instance: a function that monitors a DetNet flow for defects and/or measures its performance metrics. Within this document, a shorter version, OAM instance, is used interchangeably.

\*Maintenance End Point (MEP): an OAM instance that is capable of generating OAM test packets in the particular sub-layer of the DetNet OAM domain.

\*Maintenance Intermediate Point (MIP): an OAM instance along the DetNet flow in the particular sub-layer of the DetNet OAM domain. An active MIP MUST respond to an OAM message generated by the MEP at its sub-layer of the same DetNet OAM domain.

\*Control and management plane: the control and management planes are used to configure and control the network. Relative to a DetNet flow, the control and/or management plane can be out-of-band.

\*Active measurement methods (as defined in [[RFC7799](#)]) modify a DetNet flow by injecting specially constructed test packets [[RFC2544](#)]).

\*Passive measurement methods [[RFC7799](#)] infer information by observing unmodified existing flows.

\*Hybrid measurement methods [[RFC7799](#)] is the combination of elements of both active and passive measurement methods.

\*In-band OAM is an active OAM that is in-band within the monitored DetNet OAM domain when it traverses the same set of links and interfaces receiving the same QoS and Packet Replication, Elimination, and Ordering Functions (PREOF) treatment as the monitored DetNet flow.

\*Out-of-band OAM is an active OAM whose path through the DetNet domain is not topologically identical to the path of the monitored DetNet flow, or its test packets receive different QoS and/or PREOF treatment, or both.

\*On-path telemetry can be realized as a hybrid OAM method. The origination of the telemetry information is inherently in-band as packets in a DetNet flow are used as triggers. Collection of the on-path telemetry information can be performed using in-band or out-of-band OAM methods.

## 1.2. Abbreviations

OAM: Operations, Administration, and Maintenance

DetNet: Deterministic Networking

PREOF: Packet Replication, Elimination and Ordering Functions

SLO: Service Level Objective

### 1.3. 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. The requirements language is used in [Section 1.1](#), [Section 6](#), and applies to the implementations of DetNet OAM.

## 2. Role of OAM in DetNet

DetNet networks expect to provide communications with predictable low packet delay, packet loss, and packet misordering. Most critical applications will define a set of SLOs to be required for the DetNet flows it generates.

To respect strict guarantees, DetNet can use an orchestrator able to monitor and maintain the network. Typically, a Software-Defined Network controller places DetNet flows in the deployed network based on their SLOs. Thus, resources have to be provisioned a priori for the regular operation of the network.

Most of the existing OAM tools can be used in DetNet networks, but they can only cover some aspects of deterministic networking. Fulfilling strict guarantees is essential for DetNet flows, resulting in new DetNet-specific functionalities that must be covered with OAM. Filling these gaps is inevitable and needs accurate consideration of DetNet specifics. Similar to DetNet flows, their OAM also needs careful end-to-end engineering.

For example, appropriate placing of MEPs along the path of a DetNet flow is not always a trivial task and may require proper design, together with the design of the service component of a given DetNet flow.

There are several DetNet-specific challenges for OAM. Bounded network characteristics (e.g., delay, loss) are inseparable service parameters; therefore, Performance Monitoring OAM is a key topic for DetNet. OAM tools are needed to monitor each SLO without impacting the DetNet flow characteristics. A further challenge is strict resource allocation. Resources used by OAM must be considered and allocated to avoid disturbing DetNet flows.

The DetNet Working Group has defined two sub-layers:

- DetNet service sub-layer, at which a DetNet service (e.g., service protection) is provided.

DetNet forwarding sub-layer, which optionally provides resource allocation for DetNet flows over paths provided by the underlying network.

OAM mechanisms exist for the DetNet forwarding sub-layer, but the service sub-layer requires new OAM procedures. These new OAM functions must allow, for example, to recognize/discover DetNet relay nodes, to get information about their configuration, and to check their operation or status.

DetNet service sub-layer functions use a sequence number for PREOF. That creates a challenge for inserting OAM packets in the DetNet flow.

Fault tolerance also assumes that multiple paths could be provisioned to maintain an end-to-end circuit by adapting to the existing conditions. The DetNet Controller Plane, e.g., central controller/orchestrator, controls the PREOF on a node. OAM is expected to support monitoring and troubleshooting PREOF on a particular node and within the domain.

Note that a distributed architecture of the DetNet Control Plane can also control PREOF in those scenarios where DetNet solutions involve more than one single central controller.

The DetNet forwarding sub-layer is based on preexisting technologies and has much better coverage regarding OAM. However, the forwarding sub-layer is terminated at DetNet relay nodes, so the end-to-end OAM state of forwarding may be created only based on the status of multiple forwarding sub-layer segments serving a given DetNet flow (e.g., in case of DetNet MPLS, there may be no end-to-end LSP below the DetNet Pseudowire).

### **3. Operation**

OAM features will enable DetNet with robust operation both for forwarding and routing purposes.

It is worth noting that the test and data packets are expected to follow the same path, i.e., connectivity verification has to be conducted in-band without impacting data traffic. It is expected that test packets share fate with the monitored data traffic without introducing congestion in normal network conditions.

#### **3.1. Information Collection**

Information about the state of the network can be collected using several mechanisms. Some protocols, e.g., Simple Network Management Protocol, polls for updated data. Other protocols, such as YANG-Push [[RFC8641](#)], can be used to set up subscriptions for the data defined

in the YANG data models to be published periodically or when the underlying data changes. In either way, information is collected and sent using the DetNet Controller Plane.

Also, we can characterize methods of transporting OAM information relative to the path of data. For instance, OAM information may be transported in-band or out-of-band relative to the DetNet flow. In case of the former, the telemetry information uses resources allocated for the monitored DetNet flow. If an in-band method of transporting telemetry is used, the amount of generated information needs to be carefully analyzed, and additional resources must be reserved. [RFC9197] defines the in-band transport mechanism where telemetry information is collected in the data packet on which information is generated. Two tracing methods are described - end-to-end, i.e., from the ingress and egress nodes, and hop-by-hop, i.e., like end-to-end with additional information from transit nodes. [RFC9326] and [I-D.mirsky-ippm-hybrid-two-step] are examples of out-of-band telemetry transport. In the former case, information is transported by each node traversed by the data packet of the monitored DetNet flow in a specially constructed packet. In the latter, information is collected in a sequence of follow-up packets that traverse the same path as the data packet of the monitored DetNet flow. In both methods, transport of the telemetry can avoid using resources allocated for the DetNet domain.

### **3.2. Continuity Check**

Continuity check is used to monitor the continuity of a path, i.e., that there exists a way to deliver packets between MEP A and MEP B. The continuity check detects a network failure in one direction, from the MEP transmitting test packets to the remote egress MEP. Continuity check in a DetNet OAM domain monitors the DetNet forwarding sub-layer and thus is not affected by a PREOF that operates at the DetNet service sub-layer ([RFC8655]).

### **3.3. Connectivity Verification**

In addition to the Continuity Check, DetNet solutions have to verify connectivity. This verification considers an additional constraint, i.e, the absence of misconnection. The misconnection error state is entered after several consecutive test packets from other DetNet flows are received. The definition of the conditions for entry and exit of a misconnection error state is outside the scope of this document. Connectivity verification in a DetNet OAM domain monitors the DetNet forwarding sub-layer and thus is not affected by PREOF that operates at the DetNet service sub-layer ([RFC8655]).

### **3.4. Route Tracing**

Ping and traceroute are two ubiquitous tools that help localize and characterize a failure in the network using an echo request/reply mechanism. They help to identify a subset of the routers in the path. However, to be predictable, resources are reserved per flow in DetNet. Thus, DetNet needs to define route tracing tools able to trace the route for a specific flow. Also, tracing can be used for the discovery of the Path Maximum Transmission Unit or location of elements of PREOF for the particular route in the DetNet domain.

DetNet is not expected to use Equal-Cost Multipath (ECMP) [[RFC8939](#)]. As the result, DetNet OAM in an ECMP environment is outside the scope of this document.

### **3.5. Fault Verification/Detection**

DetNet expects to operate fault-tolerant networks. Thus, mechanisms able to detect faults before they impact network performance are needed.

The network has to detect when a fault has occurred, i.e., the network has deviated from its expected behavior. Fault detection can be based on proactive OAM protocols like continuity check or on-demand methods like ping. While the network must report an alarm, the cause may not be identified precisely. Examples of such alarms are significant degradation of the end-to-end reliability, or a buffer overflow occurs.

### **3.6. Fault Localization and Characterization**

An ability to localize a network defect and provide its characterization are necessary elements of network operation.

Fault localization, a process of deducing the location of a network failure from a set of observed failure indications, might be achieved, for example, by tracing the route of the DetNet flow in which the network failure was detected. Another method of fault localization can correlate reports of failures from a set of interleaved sessions monitoring path continuity.

Fault characterization is a process of identifying the root cause of the problem. For instance, misconfiguration or malfunction of PREOF elements can be the cause of erroneous packet replication or extra packets being flooded in the DetNet domain.



### 3.7. Use of Hybrid OAM in DetNet

Hybrid OAM methods are used in performance monitoring and defined in [[RFC7799](#)] as:

Hybrid Methods are Methods of Measurement that use a combination of Active Methods and Passive Methods.

A hybrid measurement method can produce metrics as close to measured using a passive measurement method. The passive methods measure metrics closest to the network's actual conditions. A hybrid method, even if it alters something in a data packet, even if that is as little as the value of a designated field in the packet encapsulation, is considered an approximation of a passive measurement method. One example of such a hybrid measurement method is the Alternate Marking method (AMM) described in [[RFC9341](#)]. As with all on-path telemetry methods, AMM in a DetNet domain with the IP data plane is natively in-band with respect to the monitored DetNet flow. Because the marking is applied to a data flow, measured metrics are directly applicable to the DetNet flow. AMM minimizes the additional load on the DetNet domain by using nodal collection and computation of performance metrics in combination with optionally using out-of-band telemetry collection for further network analysis.

## 4. Administration

The ability to expose a collection of metrics to support an operator's decision-making is essential. The following performance metrics are useful:

- \*Queuing Delay: the time elapsed between enqueueing a packet and its transmission to the next hop.
- \*Buffer occupancy: the number of packets present in the buffer, for each of the existing flows.
- \*Per DetNet flow, a metric reflecting end-to-end performance for a given flow. Each of the paths has to be isolated in a multipath routing environment.
- \*Per path, detection of misbehaving path(s) when multiple paths are used for the service protection.
- \*Per device, detection of a misbehaving device.

### 4.1. Collection of metrics

It is important to optimize the volume and frequency of statistics/measurement collection, whether the mechanisms are distributed,

centralized, or both. Periodic and event-triggered collection information characterizing the state of a network is an example of mechanisms to achieve the optimization.

#### 4.2. Worst-case metrics

DetNet aims to enable real-time communications on top of a heterogeneous multi-hop architecture. To make correct decisions, the DetNet Controller Plane [[RFC8655](#)] needs timely information about packet losses/delays for each flow, and each hop of the paths. In other words, just the average end-to-end statistics are not enough. The collected information must be sufficient to allow a system to predict the worst-case scenario.

### 5. Maintenance

Service protection (provided by the DetNet Service sub-layer) is designed to mitigate simple network failures more rapidly than the expected response time of the DetNet Controller Plane. In the face of events that impact network operation (e.g., link up/down, device crash/reboot, flows starting and ending), the DetNet Controller Plane needs to perform repair and re-optimization actions in order to permanently ensure SLOs of all active flows with minimal waste of resources. The Controller Plane is expected to be able to continuously retrieve the state of the network, to evaluate conditions and trends about the relevance of a reconfiguration, quantifying:

- \*the cost of the sub-optimality: resources may not be used optimally (i.e., a better path exists).

- \*the reconfiguration cost: the DetNet Controller Plane needs an ability to trigger some reconfigurations. For this transient period, resources may be twice reserved, and control packets have to be transmitted.

Thus, reconfiguration may only be triggered if the gain is significant.

#### 5.1. Replication / Elimination

When multiple paths are reserved between two MEPs, packet replication may be used to introduce redundancy and alleviate transmission errors and collisions. For instance, in [Figure 1](#), the source device S transmits a packet to devices A and B to reach the destination node R.

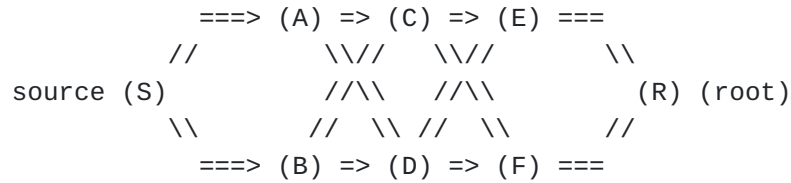


Figure 1: Packet Replication and Elimination Functions

## 5.2. Resource Reservation

Because the quality of service criteria associated with a path may degrade, the network has to provision additional resources along the path.

## 6. Requirements

According to [[RFC8655](#)], DetNet functionality is divided into forwarding and service sub-layers. The DetNet forwarding sub-layer includes DetNet transit nodes and may allocate resources for a DetNet flow over paths provided by the underlay network. The DetNet service sub-layer includes DetNet relay nodes and provides a DetNet service (e.g., service protection). This section lists general requirements for DetNet OAM as well as requirements in each of the DetNet sub-layers of a DetNet domain.

1. It MUST be possible to initiate a DetNet OAM session from a MEP located at a DetNet node towards MEP(s) downstream from that DetNet node within the given domain at a particular DetNet sub-layer.
2. It MUST be possible to initiate a DetNet OAM session from using any of DetNet Controller Plane solutions, e.g., centralized controller.
3. DetNet OAM MUST support proactive OAM monitoring and measurement methods.
4. DetNet OAM MUST support on-demand OAM monitoring and measurement methods.
5. DetNet OAM MUST support unidirectional OAM methods, continuity check, connectivity verification, and performance measurement.
6. DetNet OAM MUST support bi-directional DetNet flows, but is not required to support bi-directional OAM methods for bi-directional DetNet flows. DetNet OAM test packets used for monitoring and measurements of a bi-directional DetNet flow MUST be in-band in both directions.

7. DetNet OAM MUST support proactive monitoring of a DetNet device reachability for a given DetNet flow.
8. DetNet OAM MUST support hybrid performance measurement methods.
9. Calculated performance metrics MUST include but are not limited to throughput, packet loss, out of order, delay, and delay variation metrics. [[RFC6374](#)] provides detailed information on performance measurement and performance metrics.

#### **6.1. For the DetNet Forwarding Sub-layer**

1. DetNet OAM MUST support Path Maximum Transmission Unit discovery.
2. DetNet OAM MUST support Remote Defect Indication notification to the DetNet OAM instance performing continuity checking.
3. DetNet OAM MUST support monitoring levels of resources allocated for a particular DetNet flow. Such resources include but are not limited to buffer utilization and scheduler transmission calendar.
4. DetNet OAM MUST support monitoring any subset of paths traversed through the DetNet domain by a DetNet flow.

#### **6.2. For the DetNet Service Sub-layer**

The OAM functions for the DetNet service sub-layer allow, for example, to recognize/discover DetNet relay nodes, to get information about their configuration, and to check their operation or status.

The requirements on OAM for a DetNet relay node are:

1. DetNet OAM MUST provide OAM functions for the DetNet service sub-layer.
2. DetNet OAM MUST support the discovery of DetNet relay nodes in a DetNet network.
3. DetNet OAM MUST support the discovery of PREOF locations in the domain.
4. DetNet OAM MUST support the collection of the DetNet service sub-layer specific (configuration/operation/status) information from DetNet relay nodes.
5. DetNet OAM MUST support exercising functionality of PREOF in the domain.

6. DetNet OAM MUST work for DetNet data planes - MPLS and IP.
7. DetNet OAM MUST support a defect notification mechanism, like Alarm Indication Signal. Any DetNet relay node providing service for a given DetNet flow MAY originate a defect notification addressed to any subset of DetNet relay nodes along that flow.
8. DetNet OAM MUST be able to measure metrics (e.g. delay) inside a collection of OAM sessions, specially for complex DetNet flows, with PREOF features.

## 7. IANA Considerations

This document has no actionable requirements for IANA. This section can be removed before publication.

## 8. Security Considerations

This document lists the OAM requirements for a DetNet domain and does not raise any security concerns or issues in addition to ones common to networking and those specific to DetNet discussed in Section 9 of [[RFC9055](#)]. Furthermore, the analysis of OAM security concerns in Section 6 of [[RFC7276](#)] also applies to DetNet OAM, including the use of OAM for network reconnaissance.

## 9. Privacy Considerations

Privacy considerations of DetNet discussed in Section 13 of [[RFC9055](#)] are also applicable to DetNet OAM. If any privacy mechanism is used for the monitored DetNet flow, then the same privacy method MUST be applied to the active DetNet OAM used to monitor the flow.

## 10. Acknowledgments

The authors express their appreciation and gratitude to Pascal Thubert for the review, insightful questions, and helpful comments.

## 11. References

### 11.1. 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>>.

[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>>.

## 11.2. Informative References

[I-D.mirsky-ippm-hybrid-two-step] Mirsky, G., Lingqiang, W., Zhui, G., Song, H., and P. Thubert, "Hybrid Two-Step Performance Measurement Method", Work in Progress, Internet-Draft, draft-mirsky-ippm-hybrid-two-step-15, 15 June 2023, <<https://datatracker.ietf.org/doc/html/draft-mirsky-ippm-hybrid-two-step-15>>.

[RFC2544] Bradner, S. and J. McQuaid, "Benchmarking Methodology for Network Interconnect Devices", RFC 2544, DOI 10.17487/RFC2544, March 1999, <<https://www.rfc-editor.org/info/rfc2544>>.

[RFC6291] Andersson, L., van Helvoort, H., Bonica, R., Romascanu, D., and S. Mansfield, "Guidelines for the Use of the "OAM" Acronym in the IETF", BCP 161, RFC 6291, DOI 10.17487/RFC6291, June 2011, <<https://www.rfc-editor.org/info/rfc6291>>.

[RFC6374] Frost, D. and S. Bryant, "Packet Loss and Delay Measurement for MPLS Networks", RFC 6374, DOI 10.17487/RFC6374, September 2011, <<https://www.rfc-editor.org/info/rfc6374>>.

[RFC7276] Mizrahi, T., Sprecher, N., Bellagamba, E., and Y. Weingarten, "An Overview of Operations, Administration, and Maintenance (OAM) Tools", RFC 7276, DOI 10.17487/RFC7276, June 2014, <<https://www.rfc-editor.org/info/rfc7276>>.

[RFC7799] Morton, A., "Active and Passive Metrics and Methods (with Hybrid Types In-Between)", RFC 7799, DOI 10.17487/RFC7799, May 2016, <<https://www.rfc-editor.org/info/rfc7799>>.

[RFC8641] Clemm, A. and E. Voit, "Subscription to YANG Notifications for Datastore Updates", RFC 8641, DOI

10.17487/RFC8641, September 2019, <<https://www.rfc-editor.org/info/rfc8641>>.

[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>>.

[RFC9055] Grossman, E., Ed., Mizrahi, T., and A. Hacker, "Deterministic Networking (DetNet) Security Considerations", RFC 9055, DOI 10.17487/RFC9055, June 2021, <<https://www.rfc-editor.org/info/rfc9055>>.

[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>>.

[RFC9341] Fioccola, G., Ed., Cociglio, M., Mirsky, G., Mizrahi, T., and T. Zhou, "Alternate-Marking Method", RFC 9341, DOI 10.17487/RFC9341, December 2022, <<https://www.rfc-editor.org/info/rfc9341>>.

#### Authors' Addresses

Greg Mirsky  
Ericsson

Email: [gregimirsky@gmail.com](mailto:gregimirsky@gmail.com)

Fabrice Theoleyre  
CNRS  
300 boulevard Sebastien Brant - CS 10413  
67400 Illkirch - Strasbourg  
France

Phone: [+33 368 85 45 33](tel:+33368854533)  
Email: [fabrice.theoleyre@cnrs.fr](mailto:fabrice.theoleyre@cnrs.fr)  
URI: <https://fabrice.theoleyre.cnrs.fr/>

Georgios Z. Papadopoulos  
IMT Atlantique  
Office B00 - 102A  
2 Rue de la Châtaigneraie

35510 Cesson-Sévigné - Rennes  
France

Phone: [+33 299 12 70 04](tel:+33299127004)

Email: [georgios.papadopoulos@imt-atlantique.fr](mailto:georgios.papadopoulos@imt-atlantique.fr)

Carlos J. Bernardos  
Universidad Carlos III de Madrid  
Av. Universidad, 30  
28911 Leganes, Madrid  
Spain

Phone: [+34 91624 6236](tel:+34916246236)

Email: [cjbc@it.uc3m.es](mailto:cjbc@it.uc3m.es)

URI: <http://www.it.uc3m.es/cjbc/>

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

Email: [balazs.a.varga@ericsson.com](mailto:balazs.a.varga@ericsson.com)

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

Email: [janos.farkas@ericsson.com](mailto:janos.farkas@ericsson.com)