DetNet
Internet-Draft
Intended status: Informational
Expires: 24 December 2021

G. Mirsky
ZTE Corp.
F. Theoleyre
CNRS
G.Z. Papadopoulos
IMT Atlantique
CJ. Bernardos
UC3M

22 June 2021

Framework of Operations, Administration and Maintenance (OAM) for Deterministic Networking (DetNet) draft-ietf-detnet-oam-framework-02

Abstract

Deterministic Networking (DetNet), as defined in RFC 8655, is aimed to provide a 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. 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 24 December 2021.

Table of Contents

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 (SLO), 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 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. Terminology

This document uses definitions, particularly of a DetNet flow, provided in Section 2.1 [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 endPoint (MIP): an OAM instance along the DetNet flow in the particular sub-layer of the DetNet OAM domain. A MIP MAY 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 (long-term). 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 inserting novel fields, 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.

1.2. Acronyms

OAM: Operations, Administration, and Maintenance

DetNet: Deterministic Networking

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.

2. Role of OAM in DetNet

DetNet networks expect to provide communications with predictable low packet delay and packet loss. Most critical applications will define an SLO 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 (SDN) controller places DetNet flows in the deployed network based on their SLO. Thus, resources have to be provisioned a priori for the regular operation of the network. OAM represents the essential elements of the network operation and necessary for OAM resources that need to be accounted for to maintain the network operational.

Many legacy OAM tools can be used in DetNet networks, but they are not able to cover all the 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 itself, their OAM needs careful end-to-end engineering as well.

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, PM is a key topic for DetNet. OAM tools are needed to prove the SLO without impacting the DetNet flow characteristics. A further challenge is the strict resource allocation. Resources used by OAM must be considered and allocated to avoid disturbing DetNet flow(s).

The DetNet Working Group has defined two sub-layers: (1) DetNet service sub-layer, at which a DetNet service (e.g., service protection) is provided and (2) 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, nonetheless, OAM for 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 using a sequence number. 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 central controller/orchestrator typically controls the Packet Replication, Elimination, and Ordering Functions (PREOF) on a node. OAM is expected to support monitoring and troubleshooting PREOF on a particular node and within the domain.

Note that distributed controllers can also control PREOF in those scenarios where DetNet solutions involve more than one single central controller.

DetNet forwarding sub-layer is based on legacy technologies and has a 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 PW).

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 MUST follow the same path, i.e., the connectivity verification has to be conducted in-band without impacting the data traffic. Test packets MUST 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, send queries. Others, e.g., YANG-based data models, generate notifications based on the publish-subscribe method. In either way, information is collected and sent to the controller.

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. [I-D.ietf-ippm-ioam-data] 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. [I-D.ietf-ippm-ioam-direct-export] 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 the packets between two 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.

3.3. Connectivity Verification

In addition to the Continuity Check, DetNet solutions have to verify the connectivity. This verification considers additional constraints, 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 of entry and exit for misconnection error state is outside the scope of this document.

3.4. Route Tracing

Ping and traceroute are two ubiquitous tools that help localize and characterize a failure in the network. They help to identify a subset of the list of routers in the route. However, to be predictable, resources are reserved per flow in DetNet. Thus, DetNet needs to define route tracing tools able to track 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 RECOMMENDED to use multiple paths or links, i.e., Equal-Cost Multipath (ECMP) [RFC8939]. As the result, OAM in 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 the network performance are needed.

The network has to detect when a fault occurred, i.e., the network has deviated from its expected behavior. While the network must report an alarm, the cause may not be identified precisely. For instance, the end-to-end reliability has decreased significantly, or a buffer overflow occurs.

DetNet OAM mechanisms SHOULD allow a fault detection in real time. They MAY, when possible, predict faults based on current network conditions. They MAY also identify and report the cause of the actual/predicted network failure.

3.6. Fault Localization and Characterization

An ability to localize the 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 interleaving 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 may produce metrics as close to passive, but it still alters something in a data packet even if that is the value of a designated field in the packet encapsulation. One example of such a hybrid measurement method is the Alternate Marking method (AMM) described in [RFC8321]. As with all on-path telemetry methods, AMM in a DetNet domain with the IP data plane is natively in-band in

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 network SHOULD expose a collection of metrics to support an operator making proper decisions, including:

* Queuing Delay: the time elapsed between a packet enqueued and its transmission to the next hop.

* Buffer occupancy: the number of packets present in the buffer, for each of the existing flows.

The following metrics SHOULD be collected:

* per a DetNet flow to measure the end-to-end performance for a given flow. Each of the paths has to be isolated in multipath routing strategies.

* per path to detect misbehaving path when multiple paths are applied.

* per device to detect misbehaving device, when it relays the packets of several flows.

4.1. Collection of metrics

DetNet OAM SHOULD optimize the number of statistics / measurements to collected, frequency of collecting. Distributed and centralized mechanisms MAY be used in combination. Periodic and event-triggered collection information characterizing the state of a network MAY be used.

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 controller needs to know the distribution of packet losses/delays for each flow, and each hop of the paths. In other words, the average end-to-end statistics are not enough. The collected information must be sufficient to allow the controller to predict the worst-case.

5. Maintenance

In the face of events that impact the network operation (e.g., link up/down, device crash/reboot, flows starting and ending), the DetNet Controller need to perform repair and re-optimization actions in order to permanently ensure the SLO of all active flows with minimal waste of resources The controller MUST 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 (e.g., a better path exists).

the reconfiguration cost: the controller needs 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 is transmitting the packet to both parents, devices A and B. Each MEP will decide to trigger the packet replication, elimination or the ordering process when a set of metrics passes a threshold value.

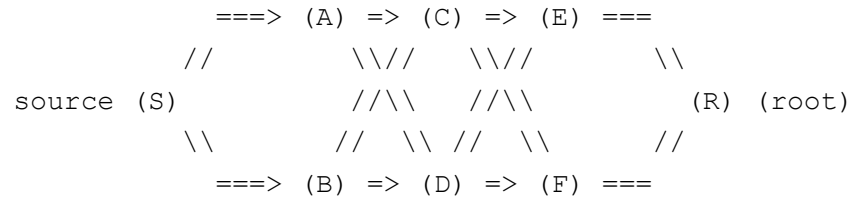

Figure 1: Packet Replication: S transmits twice the same data packet, to DP(A) and AP (B).

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. We need to provide mechanisms to patch the network configuration.

5.3. Soft transition after reconfiguration

Since DetNet expects to support real-time flows, DetNet OAM MUST support soft-reconfiguration, where the the additional resources are reserved before the those previously reserved but not in use are released. Some mechanisms have to be proposed so that packets are forwarded through the novel track only when the resources are ready to be used, while maintaining the global state consistent (no packet reordering, duplication, etc.)

6. Requirements

This section lists requirements for OAM in a DetNet domain:

1. It MUST be possible to initiate a DetNet OAM session from a MEP located at a DetNet node towards downstream MEP(s) within the given domain at a particular DetNet sub-layer. [Ed.note: FT: A MEP may be inside the detnet domain: for instance, for PREOF, an OAM session may be maintained between any pair of replicator / eliminator / egress / ingress.]

2. It MUST be possible to initialize a DetNet OAM session from a centralized controller.

3. DetNet OAM MUST support proactive and on-demand OAM monitoring and measurement methods.

4. DetNet OAM MUST support unidirectional OAM methods, continuity check, connectivity verification, and performance measurement.

5. OAM methods MAY combine in-band monitoring or measurement in the forward direction and out-of-bound notification in the reverse direction, i.e., towards the ingress MEP.

6. DetNet OAM MUST support bi-directional DetNet flows.

7. DetNet OAM MAY support bi-directional OAM methods for bidirectional DetNet flows. OAM test packets used for monitoring and measurements MUST be in-band in both directions.

8. DetNet OAM MUST support proactive monitoring of a DetNet device reachability for a given DetNet flow.

9. DetNet OAM MUST support Path Maximum Transmission Unit discovery.

10. DetNet OAM MUST support the discovery of PREOF along a route in the given DetNet domain.

11. DetNet OAM MUST support Remote Defect Indication (RDI) notification to the DetNet OAM instance performing continuity checking.

12. DetNet OAM MAY support hybrid performance measurement methods.

13. DetNet OAM MUST support unidirectional performance measurement methods. 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.

14. 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.

15. DetNet OAM MUST support defect notification mechanism, like Alarm Indication Signal. Any DetNet device within the given DetNet flow MAY originate a defect notification addressed to any subset of DetNet devices within that flow.

16. DetNet OAM MUST support methods to enable availability of the DetNet domain. These recovery methods MAY use protection switching and restoration.

17. DetNet OAM MUST support the discovery of Packet Replication, Elimination, and Order preservation sub-functions locations in the domain.

18. DetNet OAM MUST support testing of Packet Replication, Elimination, and Order preservation sub-functions in the domain.

19. DetNet OAM MUST support monitoring levels of resources allocated for the particular DetNet flow. Such resources include but not limited to buffer utilization, scheduler transmission calendar.

20. DetNet OAM MUST support monitoring any sub-set of paths traversed through the DetNet domain by the DetNet flow.

7. IANA Considerations

This document has no actionable requirements for IANA. This section can be removed before the 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 a DetNet discussed in [I-D.ietf-detnet-security].

9. Acknowledgments

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

10. References

10.1. 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>.

10.2. Informative References

[I-D.ietf-detnet-security] Grossman, E., Mizrahi, T., and A. J. Hacker, "Deterministic Networking (DetNet) Security Considerations", Work in Progress, Internet-Draft, draft-ietf-detnet-security-16, 2 March 2021, <https://tools.ietf.org/html/draft-ietf-detnet-security-16>.

[I-D.ietf-ippm-ioam-data]
Brockners, F., Bhandari, S., and T. Mizrahi, "Data Fields for In-situ OAM", Work in Progress, Internet-Draft, draft-ietf-ippm-ioam-data-12, 21 February 2021, <https://tools.ietf.org/html/draft-ietf-ippm-ioam-data-12>.

[I-D.ietf-ippm-ioam-direct-export]
Song, H., Gafni, B., Zhou, T., Li, Z., Brockners, F., Bhandari, S., Sivakolundu, R., and T. Mizrahi, "In-situ OAM Direct Exporting", Work in Progress, Internet-Draft, draft-ietf-ippm-ioam-direct-export-03, 17 February 2021, <https://tools.ietf.org/html/draft-ietf-ippm-ioam-direct-export-03>.

[I-D.mirsky-ippm-hybrid-two-step]
Mirsky, G., Lingqiang, W., Zhui, G., and H. Song, "Hybrid Two-Step Performance Measurement Method", Work in Progress, Internet-Draft, draft-mirsky-ippm-hybrid-two-step-10, 17 May 2021, <https://tools.ietf.org/html/draft-mirsky-ippm-hybrid-two-step-10>.

[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>.

[RFC8321] Fioccola, G., Ed., Capello, A., Cociglio, M., Castaldelli, L., Chen, M., Zheng, L., Mirsky, G., and T. Mizrahi, "Alternate-Marking Method for Passive and Hybrid Performance Monitoring", RFC 8321, DOI 10.17487/RFC8321, January 2018, <https://www.rfc-editor.org/info/rfc8321>.

[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>.

Authors' Addresses

Greg Mirsky
ZTE Corp.

Email: gregimirsky@gmail.com, gregory.mirsky@ztetx.com

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

Phone: +33 368 85 45 33
Email: theoleyre@unistra.fr
URI: http://www.theoleyre.eu

Georgios Z. Papadopoulos
IMT Atlantique
Office B00 - 102A
2 Rue de la Châtaigneraie
35510 Cesson-Sévigné - Rennes
France

Phone: +33 299 12 70 04
Email: georgios.papadopoulos@imt-atlantique.fr

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

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/