Operations, Administration and Maintenance (OAM) features for DetNet
                 draft-theoleyre-detnet-oam-support-00

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 (SLO), such
   as packet delay, delay variation, and packet loss ratio, assigned to
   each data flow.

Copyright Notice

Table of Contents

1. TEMPORARY EDITORIAL NOTES

   This document is an Internet Draft, so it is work-in-progress by
   nature. It contains the following work-in-progress elements:

o "TODO" statements are elements which have not yet been written by
   the authors for some reason (lack of time, ongoing discussions
   with no clear consensus, etc). The statement does indicate that
   the text will be written at some time.

2. 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. Their
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 packet delay, delay variation, and packet
loss ratio, assigned to each data flow.

2.1. Terminology

We adopt here the following terminology:

o OAM entity: a data flow to be monitored for defects and/or its
   performance metrics measured.

o Maintenance End Point (MEP): OAM systems traversed by a data flow
   when entering/exiting the network. In DetNet, it corresponds with
   the source and destination of a data flow. OAM messages can be
   exchanged between two MEPs.

o Maintenance Intermediate endPoint (MIP): an OAM system along the
   flow; a MIP MAY respond to an OAM message generated by the MEP.

o Control and management plane: the control and management planes
   are used to configure and control the network (long-term).

Relative to a data flow, the control and/or management plane can
be out-of-band.

o Active measurement methods (as defined in [RFC7799]) modify a
   normal data flow by inserting novel fields, injecting specially
   constructed test packets [RFC2544]). It is critical for the
   quality of information obtained using an active method that
   generated test packets are in-band with the monitored data flow.
   In other words, a test packet is required to cross the same
   network nodes and links and receive the same Quality of Service
   (QoS) treatment as a data packet.

o Passive measurement methods [RFC7799] infer information by
   observing unmodified existing flows.

o Hybrid measurement methods [RFC7799] is the combination of
   elements of both active and passive measurement methods.

2.2. Acronyms

OAM: Operations, Administration, and Maintenance

DetNet: Deterministic Networking

SLO: Service Level Objective

QoS: Quality of Service

SNMP: Simple Network Management Protocol

SDN: Software Defined Network

<TODO> we need here an exhaustive list, to be completed after the
document has evolved.

2.3. 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.

3. 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 data 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 the 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.

Fault-tolerance also assumes that multiple paths could be provisioned
so that an end-to-end circuit is maintained 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 PREOF can also be controlled by a set of distributed
controllers, in those scenarios where DetNet solutions involve more
than one single central controller.

4. Operation

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

4.1. Information Collection

Information about the state of the network can be collected using
several mechanisms. Some protocols, e.g., Simple Network Management
Protocol (SNMP), send queries. Others, e.g., YANG-based data models,
generate notifications based on the publish-subscribe method. In
either way, information about the state of the network being
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 out-of-band or in-band with the data flow.

4.2. 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 endpoints
A and B.

4.3. 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.

   In particular, resources have to be reserved for a given flow, so
   they are booked for use without being impacted by other flows.
   Similarly, the destination does not receive packets from different
   flows through its interface.

   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.

4.4. 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.

   DetNet with IP data plane is NOT RECOMMENDED to use multiple paths or
   links, i.e., Equal-Cost Multipath (ECMP) [I-D.ietf-detnet-ip]. As
   the result, OAM in IP ECMP environment is outside the scope of this
   document.

4.5. 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 to detect when a fault has
   occurred. 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.

4.6. Fault Isolation/identification

   The network has isolated and identified the cause of the fault. For
   instance, the replication process behaves not as expected to a
   specific intermediary router.

5. Administration

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

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

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

   The following metrics SHOULD be collected:

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

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

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

5.1. 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.

5.2. 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.

6. Maintenance

   DetNet needs to implement a self-healing and self-optimization
   approach. 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.

6.1. Replication / Elimination

   When multiple paths are reserved between two maintenance endpoints,
   packet replication may be used to introduce redundancy and alleviate
   transmission errors and collisions. For instance, in Figure 1, the
   source node S is transmitting the packet to both parents, nodes A and
   B. Each maintenance endpoint will decide to trigger the packet
   replication, elimination or the ordering process when a set of
   metrics passes a threshold value.

```
                  ===> (A) => (C) => (E) ===
                 //         \\//   \\//        \\
         source (S)         //\\   //\\          (R) (root)
                 \\         // \\ // \\        //
                  ===> (B) => (D) => (F) ===
```
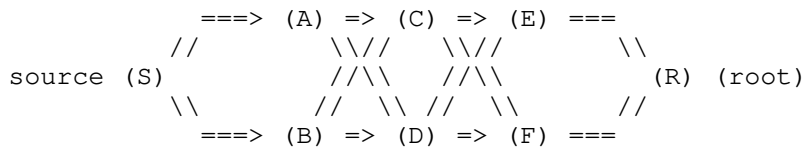
   Figure 1: Packet Replication: S transmits twice the same data packet,
                       to DP(A) and AP (B).

6.2. Resource Reservation

   Because the QoS 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.

6.3. Soft transition after reconfiguration

   Since DetNet expects to support real-time flows, DetNet OAM MUST
   support soft-reconfiguration, where the novel resources are reserved
   before the ancient ones 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.)

7. IANA Considerations

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

8. Security Considerations

   This section will be expanded in future versions of the draft.

9. Acknowledgments

   TBD

10. Informative References

   [I-D.ietf-detnet-ip]
              Varga, B., Farkas, J., Berger, L., Fedyk, D., and S.
              Bryant, "DetNet Data Plane: IP", draft-ietf-detnet-ip-07
              (work in progress), July 2020.

   [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>.

   [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>.

   [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>.

   [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>.

Authors' Addresses

   Fabrice Theoleyre
   CNRS
   300 boulevard Sebastien Brant - CS 10413
   Illkirch - Strasbourg 67400
   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 Chataigneraie
   Cesson-Sevigne - Rennes 35510
   FRANCE

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

   Grek Mirsky
   ZTE Corp.

   Email: gregimirsky@gmail.com

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

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