detnet
Internet-Draft
Intended status: Standards Track
Expires: January 29, 2021

F. Theoleyre
CNRS
G. Papadopoulos
IMT Atlantique
G. Mirsky
ZTE Corp.
C. Bernardos
Universidad Carlos III de Madrid

July 28, 2020

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

Abstract

Status of This Memo

Copyright Notice

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. 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]. It defines a toolset for fault detection and isolation, and for performance measurement.

The main purpose of this document is to detail the specific requirements of the OAM features recommended to construct a predictable communication infrastructure on top of a collection of wireless segments. This document describes the benefits, problems, and trade-offs for using OAM in deterministic networks.

In this document, the term OAM will be used according to its definition specified in [RFC6291]. We expect to implement an OAM

framework in detnet networks to maintain a real-time view of the network infrastructure, and its ability to respect the Service Level Objectives (SLO), such as delay and reliability, assigned to each data flow.

1.1. Terminology

- OAM entity: a data flow to be controlled;
- Maintenance End Point (MEP): OAM devices crossed when entering/ exiting the network. In RAW, it corresponds mostly to the source or destination of a data flow. OAM message can be exchanges between two MEPs;
- Maintenance Intermediate end Point (MIP): OAM devices along the flow; OAM messages can be exchanged between a MEP and a MIP;
- Defect: a temporary change in the network (e.g. a radio link which is broken due to a mobile obstacle);
- Fault: a definite change which may affect the network performance, e.g. a node runs out of energy.

1.2. Acronyms

OAM Operations, Administration, and Maintanence

DetNet Deterministic Networking

SLO Service Level Objective

QoS Quality of Service

SNMP Simple Network Management Protocol

SDN Software Defined Network

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 RAW

detnet networks expect to make the communications reliable and predictable. Most critical applications will define an SLO to be required for the data flows it generates.

To respect strict guarantees, detnet relies on an orchestrator able to monitor and maintain the network. Typically, a Software Defined Network (SDN) controller is in charge of scheduling the transmissions in the deployed network, based on the radio link characteristics, SLO of the flows, the number of packets to forward. Thus, resources have to be provisioned a priori to handle any defect. OAM represents the core of the over provisioning process, and maintains the network operational by updating the schedule dynamically.

Fault-tolerance also assumes that multiple paths have to be provisioned so that an end-to-end circuit keeps on existing whatever the conditions. The replication/elimination processes (PREOF) on a node is typically controlled by the central controller/orchestrator. OAM is in charge of controlling that PREOF is working properly on a node and within the domain.

RAW supports both proactive and on-demand troubleshooting.

3. Operation

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

3.1. Information Collection

Several solutions (e.g., Simple Network Management Protocol (SNMP), YANG-based data models) are already in charge of collecting the statistics. That way, we can encapsulate these statistics in specific monitoring packets, to send them to the controller.

3.2. Continuity Check

We need to verify that two endpoints are connected. In other words, there exists "one" way to deliver the packets between two endpoints A and B.

3.3. Connectivity Verification

Additionally, to the Continuity Check, we have to verify the connectivity. This verification considers additional constraints, i.e., the absence of misconnection.

In particular, the resources have to be reserved by a given flow, and no packets from other flows steal the corresponding resources. Similarly, the destination does not receive packets from different flows through its interface.

It is worth noting that the control and data packets may not follow the same path, and the connectivity verification has to be conducted in-band without impacting the data traffic. Test packets must share the fate with the monitored data traffic without introducing congestion in normal network conditions.

3.4. Route Tracing

Ping and traceroute are two very common tools for diagnostic. 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, we need to define route tracing tools able to track the route for a specific flow.

Multipath routing can be considered to make the network fault-tolerant. In that way, each Maintenance Intermediate Endpoint has several possible next hops in the forwarding plane. Thus, all the possible paths between two maintenance endpoints should be retrieved.

3.5. Fault Verification/detection

detnet expects to operate fault-tolerant networks. Thus, we need mechanisms able to detect faults, before they impact the network performance.

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.

3.6. Fault Isolation/identification

The network has isolated and identified the cause of the fault. For instance, the quality of a specific link has decreased, requiring more retransmissions, or the level of external interference has locally increased.

4. Administration

The network has to 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.

These metrics should be collected:

- 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;

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

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

4.1. Collection of metrics

We have to minimize the number of statistics / measurements to exchange. Localized and centralized mechanisms have to be combined together, and additional control packets have to be triggered only after a fault detection.

4.2. Worst-case metrics

detnet aims to enable real-time communications on top of a heterogeneous 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. They must allow the controller to predict the worst-case.

5. Maintenance

denet needs to implement a self-healing and self-optimization approach. The network must continuously retrieve the state of the network, to judge 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. Multipath Routing

To be fault-tolerant, several paths can be reserved between two maintenance endpoints. They must be node-disjoint so that a path can be available at any time.

5.2. Replication / Elimination

When multiple paths are reserved between two maintenance endpoints, they may decide to replicate the packets to introduce redundancy, and thus to 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 replication/elimination process when a set of metrics passes through a threshold value.

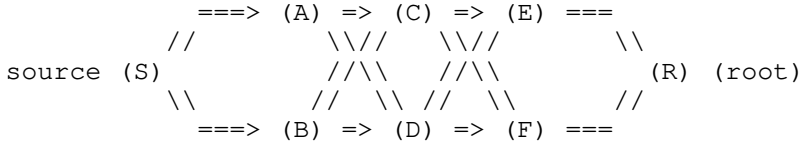

Figure 1: Packet Replication: S transmits twice the same data packet, to its DP (A) and to its AP (B).

5.3. 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.

5.4. Soft transition after reconfiguration

Since detnet expects to support real-time flows, we have to 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.)

6. IANA Considerations

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

7. Security Considerations

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

8. Acknowledgments

TBD

9. Informative References

[ipath] Gao, Y., Dong, W., Chen, C., Bu, J., Wu, W., and X. Liu, "iPath: path inference in wireless sensor networks.", 2016, <https://doi.org/10.1109/TNET.2014.2371459>.

[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>.

[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>.

[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
Building B
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

Email: cjbc@it.uc3m.es