DetNet Working Group
Internet-Draft
Intended status: Informational
Expires: February 8, 2021

G. Mirsky
ZTE Corp.
M. Chen
Huawei
D. Black
Dell EMC

August 7, 2020

Operations, Administration and Maintenance (OAM) for Deterministic Networks (DetNet) with IP Data Plane
draft-mirsky-detnet-ip-oam-03

Abstract

This document defines the principles for using Operations, Administration, and Maintenance protocols and mechanisms in the Deterministic Networking networks with the IP data plane.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

[RFC8655] introduces and explains Deterministic Networks (DetNet) architecture.

Operations, Administration and Maintenance (OAM) protocols are used to detect, localize defects in the network, and monitor network performance. Some OAM functions, e.g., failure detection, work in the network proactively, while others, e.g., defect localization, usually performed on-demand. These tasks achieved by a combination of active and hybrid, as defined in [RFC7799], OAM methods.

[I-D.ietf-detnet-mpls-oam] 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. Also, the document defines the OAM use principals for the DetNet networks with the IP data plane.

2. Conventions used in this document

2.1. Terminology

The term "DetNet OAM" used in this document interchangeably with longer version "set of OAM protocols, methods and tools for Deterministic Networks".

DetNet Deterministic Networks

DiffServ Differentiated Services

OAM: Operations, Administration and Maintenance

PREF Packet Replication and Elimination Function

POF Packet Ordering Function

RDI Remote Defect Indication

ICMP Internet Control Message Protocol

Underlay Network or Underlay Layer: The network that provides connectivity between the DetNet nodes. MPLS network providing LSP connectivity between DetNet nodes is an example of the underlay layer.

DetNet Node - a node that is an actor in the DetNet domain. DetNet domain edge node and node that performs PREF within the domain are examples of DetNet node.

2.2. Keywords

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. Active OAM for DetNet Networks with the IP Data Plane

OAM protocols and mechanisms act within the data plane of the particular networking layer. And thus it is critical that the data plane encapsulation supports OAM mechanisms in such a way that DetNet OAM packets are in-band with a DetNet flow being monitored, i.e., DetNet OAM test packets follow precisely the same path as DetNet data plane traffic both for unidirectional and bi-directional DetNet paths.

The DetNet data plane encapsulation in a transport network with IP encapsulations specified in Section 6 of [I-D.ietf-detnet-ip]. For the IP underlay network, DetNet flows are identified by the ordered match to the provisioned information set that, among other elements, includes the IP protocol, source port number, destination port number. Active IP OAM protocols like Bidirectional Forwarding Detection (BFD) [RFC5880] or STAMP [RFC8762], use UDP transport and the well-known UDP port numbers as the destination port. Thus a DetNet node MUST be able to associate an IP DetNet flow with the particular test session to ensure that test packets experience the same treatment as the DetNet flow packets.

Most of on-demand failure detection and localization in IP networks is being done by using the Internet Control Message Protocol (ICMP) Echo Request, Echo Reply and the set of defined error messages, e.g., Destination Unreachable, with the more detailed information provided through code points. [RFC0792] and [RFC4443] define the ICMP for IPv4 and IPv6 networks, respectively. Because ICMP is another IP protocol like, for example, UDP, a DetNet node MUST able to associate an ICMP packet generated by the specified IP DetNet node and addressed to the another IP DetnNet node with an IP DetNet flow between this pair of endpoints.

3.1. Active OAM Using DetNet-in-UDP Encapsulation

Active OAM in IP DetNet can be realized using DetNet-in-UDP encapsulation [Ed.note: Do we define it in this document or start a new one?]. Using DetNet-in-UDP tunnel between IP DetNet nodes ensures that active OAM test packets are fate-sharing with the monitored IP DetNet flow packets. As a result, a test packet shares the tunnel with the IP DetNet flow and shares the fate, statistically speaking, of the IP DetNet flow being monitored.

3.2. Mapping Active OAM and IP DetNet flows

IP OAM protocols that use UDP transport, e.g., BFD and STAMP, can be used to detect failures or performance degradation that affects an IP DetNet flow. When the UDP destination port number used by the OAM protocol is one of the assigned by IANA, then the UDP source port can be used to achieve co-routedness of OAM, and the monitored IP DetNet flow in the multipath environments, e.g., LAG or ECMP. To maximize the accuracy of OAM results in detecting failures and monitoring performance of IP DetNet, test packets should receive the same treatment by the nodes as experienced by the IP DetNet packet. Hence, the DSCP value used for a test packet MUST be mapped to DetNet.

3.3. Active OAM Using GRE-in-UDP Encapsulation

[RFC8086] has defined the method of encapsulating GRE (Generic Routing Encapsulation) headers in UDP. GRE-in-UDP encapsulation can be used for IP DetNet OAM as it eases the task of mapping an OAM test session to a particular IP DetNet flow that is identified by N-tuple. Matching a GRE-in-UDP tunnel to the monitored IP DetNet flow enables the use of Y.1731/G.8013 [ITU-T.1731] as a comprehensive toolset of OAM. The Protocol Type field in GRE header MUST be set to 0x8902 assigned by IANA to IEEE 802.1ag Connectivity Fault Management (CFM) Protocol / ITU-T Recommendation Y.1731. Y.1731/G.8013 supports necessary for IP DetNet OAM functions, i.e., continuity check, one-way packet loss and packet delay measurement.

4. 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]. One of the advantages of the use of AMM in a DetNet domain with the IP data plane is that the marking is applied to a data flow, thus ensuring that measured metrics are directly applicable to the DetNet flow.

5. OAM of DetNet IP Interworking with OAM of non-IP DetNet domains

A domain in which IP data plane provides DetNet service could be used in conjunction with a TSN and a DetNet domain with MPLS data plane to deliver end-to-end service. In such scenarios, the ability to detect defects and monitor performance using OAM is essential. [I-D.ietf-detnet-mpls-oam] identified two OAM interworking models - peering and tunneling. Interworking between DetNet domains with IP and MPLS data planes analyzed in Section 6.2 of [I-D.ietf-detnet-mpls-oam]. Also, requirements and recommendations for OAM interworking between a DetNet domain with MPLS data plane and OAM of a TSN equally apply to a DetNet domain with an IP data plane.

6. IANA Considerations

This document does not have any requests for IANA allocation. This section can be deleted before the publication of the draft.

7. Security Considerations

This document describes the applicability of the existing Fault Management and Performance Monitoring IP OAM protocols, and does not raise any security concerns or issues in addition to ones common to networking or already documented for the referenced DetNet and OAM protocols.

8. Acknowledgment

TBA

9. References

9.1. Normative 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.

[I-D.ietf-detnet-mpls-oam]
Mirsky, G. and M. Chen, "Operations, Administration and Maintenance (OAM) for Deterministic Networks (DetNet) with MPLS Data Plane", draft-ietf-detnet-mpls-oam-01 (work in progress), July 2020.

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, DOI 10.17487/RFC0792, September 1981, <https://www.rfc-editor.org/info/rfc792>.

[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>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/info/rfc4443>.

[RFC8086] Yong, L., Ed., Crabbe, E., Xu, X., and T. Herbert, "GRE-in-UDP Encapsulation", RFC 8086, DOI 10.17487/RFC8086, March 2017, <https://www.rfc-editor.org/info/rfc8086>.

[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>.

9.2. Informational References

[ITU-T.1731] ITU-T, "Operations, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks", ITU-T G.8013/Y.1731, August 2015.

[RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <https://www.rfc-editor.org/info/rfc5880>.

[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>.

[RFC8762] Mirsky, G., Jun, G., Nydell, H., and R. Foote, "Simple Two-Way Active Measurement Protocol", RFC 8762, DOI 10.17487/RFC8762, March 2020, <https://www.rfc-editor.org/info/rfc8762>.

Authors' Addresses

Greg Mirsky
ZTE Corp.

Email: gregimirsky@gmail.com

Mach(Guoyi) Chen
Huawei

Email: mach.chen@huawei.com

David Black
Dell EMC
176 South Street
Hopkinton, MA 01748
United States of America

Email: david.black@dell.com