Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 21, 2021

T. Mizrahi
Huawei
F. Brockners
Cisco
S. Bhandari, Ed.
Thoughtspot
R. Sivakolundu
C. Pignataro
Cisco
A. Kfir
B. Gafni
Nvidia
M. Spiegel
Barefoot Networks
T. Zhou
Huawei
J. Lemon
Broadcom

February 17, 2021

In Situ OAM Profiles
draft-mizrahi-ippm-ioam-profile-04

Abstract

In Situ Operations, Administration and Maintenance (IOAM) is used for monitoring network performance and for detecting traffic bottlenecks and anomalies. This is achieved by incorporating IOAM data into in-flight data packets. This document introduces the concept of use case-driven IOAM profiles. An IOAM profile defines a use case or a set of use cases for IOAM, and an associated set of rules that restrict the scope and features of the IOAM specification, thereby limiting it to a subset of the full functionality. The motivation for defining profiles is to limit the scope of IOAM features, allowing simpler implementation, verification, and interoperability testing in the context of specific use cases that do not require the full functionality of IOAM.

Copyright Notice

Table of Contents

1. Introduction

IOAM [I-D.ietf-ippm-ioam-data] is used for monitoring traffic in the network by incorporating IOAM data fields into in-flight data packets.

This document introduces the concept of use case driven IOAM profiles. The motivation for defining profiles is to limit the scope of IOAM features, allowing simpler implementation, verification, and interoperability testing in the context of specific use cases that do not require the full functionality of IOAM.

An IOAM profile defines a use case or a set of use cases for IOAM, and an associated set of rules that restrict the scope and features of the IOAM specification, thereby limiting it to a subset of the full functionality. Based on the guidelines in this document, future documents may define one or more IOAM profiles. The current document does not specify any IOAM profiles.

This document does not require any changes to the Data Fields for In-situ OAM [I-D.ietf-ippm-ioam-data]. Furthermore, it is expected that future IOAM profile specifications will not require changes to IOAM, since a profile, by definition, derives a subset of the existing functionality.

2. Specifying an IOAM Profile

2.1. Overview

A profile defines a set of rules that limit the scope or functionality of IOAM. By default, any detail in IOAM that is not specifically addressed or limited by the profile is as defined in IOAM [I-D.ietf-ippm-ioam-data]. The rest of this section presents a set of topics that may be addressed in a profile specification. A profile may include some or all of these topics, and optionally other topics.

A profile may in part be defined using a specific assignment to the IOAM YANG model. The IOAM YANG model [I-D.ietf-ippm-ioam-yang] defines a set of IOAM-related attributes, such as which IOAM option types are enabled, and which data fields are used. For example, an IOAM profile that only uses the icremental trace option may be defined as such by an assignment to the respective attributes that are defined in the YANG model. It should be noted that while the YANG model assists in the definition of a profile, it does not replace the profile definition. Specifically, a profile definition includes the use case(s) for using the profile, and possibly some

properties that cannot be defined by an assignment to the YANG model, such as the semantics of the Opaque State Snapshot field.

2.2. Use Cases

An IOAM profile should define the use case(s) for using the profile. The use case may describe deployment scenarios or specific applications that make use of IOAM data. The use case should typically define the required functionality from IOAM. For example, an IOAM profile may be defined such that it requires transit delay monitoring, but does not require path tracing. These requirements then affect which IOAM data fields are used in the profile.

2.3. IOAM Options

IOAM data may be represented in one of four possible IOAM options: Pre-allocated Trace Option, Incremental Trace Option, Proof Of Transit (POT) Option, and Edge-to-Edge Option. An IOAM profile may specify a subset of allowed options. A profile may define some options as mandatory in the current profile, or some options as forbidden in the current profile. Moreover, in cases where IOAM defines several possible modes of operation, a profile may choose one of these modes of operation as the only allowed mode.

For each IOAM option, a profile specification may limit the scope of the profile to certain features. For example, a profile may be defined to use the Incremental Trace Option such that only specific data types are used in the profile, while others are not.

2.4. IOAM Option Header Field Values

An IOAM profile may define specific values or specific value range for some of the fields in the IOAM option headers. For example, a profile may define a specific value that is allowed to be used in the Flags field of the trace option header.

2.5. Opaque State Snapshot

The Opaque State Snapshot, as defined in [I-D.ietf-ippm-ioam-data], is a variable length field that may be used in IOAM trace options. The Opaque State Snapshot is defined in a flexible Type/Length/Value manner. An IOAM profile may define a specific format for the Opaque State Snapshot including for example a specific length and a specific interpretation of the opaque data. In this case, the IOAM profile ought to also specify a Schema ID value.

2.6. Timestamp Format

A profile may specify a specific timestamp format to be used in IOAM data fields.

3. IANA Considerations

This document does not include any requests from IANA.

[RFC-Editor Note: feel free to remove this Section.]

4. Security Considerations

The security considerations of IOAM in general are discussed in [I-D.ietf-ippm-ioam-data]. This document presents the concept of IOAM profiles; since an IOAM profile is a specific use case of IOAM, any security threat that is relevant to the profile is also relevant to the full-blown IOAM, as defined in [I-D.ietf-ippm-ioam-data]. Therefore, the current document does not present any new security considerations beyond [I-D.ietf-ippm-ioam-data].

Moreover, in some cases a profile may limit the set of features of IOAM in a way that reduces the set of potential threats compared to a full implementation of IOAM. In fact, a particular IOAM profile can optimize a particular security posture or requirement.

5. Normative References

[I-D.ietf-ippm-ioam-data]
Brockners, F., Bhandari, S., and T. Mizrahi, "Data Fields for In-situ OAM", draft-ietf-ippm-ioam-data-11 (work in progress), November 2020.

[I-D.ietf-ippm-ioam-yang]
Zhou, T., Guichard, J., Brockners, F., and S. Raghavan, "A YANG Data Model for In-Situ OAM", draft-ietf-ippm-ioam-yang-00 (work in progress), January 2021.

[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>.

Appendix A. An IOAM Profile Example

A.1. Overview

This section presents an example of an IOAM profile specification. The profile makes use of the Hop limit, Node ID and Transit delay data fields, and is thus called the HNT profile for short.

A.2. Use Cases

This profile is intended for path tracing and transit delay monitoring, while using compact data with just two data fields per packet. The profile can be useful in networks with a large number of hops.

A.3. IOAM Options

The HNT profile makes use of the Incremental Trace Option. A packet that includes IOAM data according to the current profile includes a single IOAM option - the Incremental Trace Option. Specifically, two data fields are used in this profile: the Hop_Lim and node_id field, and the transit delay field.

A.4. IOAM Option Header Field Values

The IOAM-Trace-Type field in the header of the Incremental Trace Option in this profile has a fixed value; Bit 0 (the most significant bit) and Bit 4 are set, while the rest of the bits are zero, indicating the two data fields that are used in the option.

A.5. Opaque State Snapshot

The opaque state snapshot is never used in this profile. Note that the NodeLen field, as defined in [I-D.ietf-ippm-ioam-data], represents the length of the data excluding the opaque state snapshot. Since this field is not used in the current profile, the NodeLen represents the actual length of the data.

A.6. Profile Coexistence

It is assumed that the current profile is used in a confined administrative domain in which no other IOAM profiles are used. Therefore, it is assumed that the current profile does not coexist with other profiles.

A.7. Validity

An IOAM transit/decapsulating node that receives a packet with IOAM options that do not comply to the current profile should forward/ decapsulate the packet without IOAM processing, if it is able to do

so. If a decapsulating node is not able to decapsulate an IOAM option that is not compliant to the current profile, the packet is discarded.

Authors' Addresses

Tal Mizrahi
Huawei
8-2 Matam
Haifa 3190501
Israel

Email: tal.mizrahi.phd@gmail.com

Frank Brockners
Cisco Systems, Inc.
Hansaallee 249, 3rd Floor
DUESSELDORF, NORDRHEIN-WESTFALEN 40549
Germany

Email: fbrockne@cisco.com

Shwetha Bhandari (editor)
Thoughtspot
3rd Floor, Indiqube Orion, 24th Main Rd, Garden Layout, HSR Layout
Bangalore, KARNATAKA 560 102
India

Email: shwetha.bhandari@thoughtspot.com

Ramesh Sivakolundu
Cisco Systems, Inc.
170 West Tasman Dr.
SAN JOSE, CA 95134
U.S.A.

Email: sramesh@cisco.com

Carlos Pignataro
Cisco Systems, Inc.
7200-11 Kit Creek Road
Research Triangle Park, NC 27709
United States

Email: cpignata@cisco.com

Aviv Kfir
Nvidia

Email: avivk@nvidia.com

Barak Gafni
Nvidia
350 Oakmead Parkway, Suite 100
Sunnyvale, CA 94085
U.S.A.

Email: gbarak@nvidia.com

Mickey Spiegel
Barefoot Networks
4750 Patrick Henry Drive
Santa Clara, CA 95054
US

Email: mspiegel@barefootnetworks.com

Tianran Zhou
Huawei
156 Beiqing Rd.
Beijing 100095
China

Email: zhoutianran@huawei.com

Jennifer Lemon
Broadcom
270 Innovation Drive
San Jose, CA 95134
US

Email: jennifer.lemon@broadcom.com