Workgroup: sfc
Internet-Draft: draft-ietf-sfc-oam-packet-00
Updates: 8300 (if approved)
Published: 25 March 2022
Intended Status: Standards Track
Expires: 26 September 2022
Authors: M. Boucadair
Orange

OAM Packet and Behavior in the Network Service Header (NSH)

Abstract

This document clarifies an ambiguity in the Network Service Header (NSH) specification related to the handling of O bit. In particular, this document clarifies the meaning of "OAM packet".

This document updates RFC 8300.

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 26 September 2022.

Table of Contents

1. Introduction
2. Terminology
3. An Update to RFC8300
4. IANA Considerations
5. Security Considerations
6. Acknowledgements
7. References
   7.1. Normative References
   7.2. Informative References

Author's Address

1. Introduction

This document clarifies an ambiguity related to the definition of Operations, Administration, and Maintenance (OAM) packet discussed in [RFC8300].

The processing of the O bit in the Network Service Header (NSH) must follow the updated behavior specified in Section 3.

2. Terminology

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.

This document makes use of the terms defined in [RFC7665] and [RFC8300].

The document defines the following terms:

SFC data plane element: refers to SFC-aware SF, SFF, SFC Proxy, or Classifier as defined in the SFC data plane architecture [RFC7665] and further refined in [RFC8300].

OAM control element: an NSH-aware elements that is capable of generating NSH OAM packets. An SFC data plane element may behave as an OAM control element.

OAM data: refers to an OAM request (e.g., Connectivity Verification and Continuity Checks [RFC7276]), any data that influences how to execute a companion OAM request (e.g., identity of a terminating

Service Function (SF)), the output data of an OAM request, and any combination thereof.

User data: refers to user packets cited in Section 5.7 of [RFC7665].

3. An Update to RFC8300

This document updates Section 2.2 of [RFC8300] as follows:

OLD:

O bit: Setting this bit indicates an OAM packet (see [RFC6291]). The actual format and processing of SFC OAM packets is outside the scope of this specification (for example, see [SFC-OAM-FRAMEWORK] for one approach).

The O bit MUST be set for OAM packets and MUST NOT be set for non-OAM packets. The O bit MUST NOT be modified along the SFP.

SF/SFF/SFC Proxy/Classifier implementations that do not support SFC OAM procedures SHOULD discard packets with O bit set, but MAY support a configurable parameter to enable forwarding received SFC OAM packets unmodified to the next element in the chain. Forwarding OAM packets unmodified by SFC elements that do not support SFC OAM procedures may be acceptable for a subset of OAM functions, but it can result in unexpected outcomes for others; thus, it is recommended to analyze the impact of forwarding an OAM packet for all OAM functions prior to enabling this behavior. The configurable parameter MUST be disabled by default.

NEW:

O bit: Setting this bit indicates an SFC OAM packet. Such a packet is any NSH-encapsulated packet that exclusively includes OAM data. An OAM data can be included in the Fixed-Length Context Header, optional Context Headers, and/or the inner packet.

The O bit is typically set by an OAM controller or a final destination of an SFC OAM packet that triggers a response (e.g., a specific SFC-aware SF, the last SFF of an SFP).

The O bit MUST be set for SFC OAM packets and MUST NOT be set for non-OAM packets. The O bit MUST NOT be modified along the SFP.

NSH-encapsulated packets that include user data are not considered as SFC OAM packets even if some OAM data (e.g., record route) is also supplied in the packet.

When an OAM data is included in the inner packet, the Next Protocol field is set to reflect the structure of that inner OAM packet. The setting and processing of the O bit neither assumes nor expects detailed analysis of the content of any inner IP packet carried by the NSH. As such, SFFs, SFC-aware SFs, and SFC Proxies SHOULD discard any NSH packets with the O bit set and Next Protocol set to something that is not itself an OAM protocol. This includes discarding the packet when the O bit is set and the Next Protocol is set to 0x01 (IPv4), 0x02 (IPv6), 0x03 (MPLS), or 0x05 (Ethernet).

An SFC OAM packet MAY include optional Context Headers (e.g., a subscriber identifier [RFC8979] or a flow identifier [I-D.ietf-sfc-nsh-tlv]) that are used to influence the processing of the packet by SFC data plane elements.

An SFC OAM packet MAY include OAM data in both Context Headers and the inner packet. The processing (including the order) of the OAM data SHOULD be specified in the relevant OAM or Context Header specification.

SFC-aware SF/SFF/SFC Proxy/Classifier implementations that do not support SFC OAM procedures SHOULD discard packets with O bit set, but MAY support a configurable parameter to enable forwarding received SFC OAM packets unmodified to the next element in the chain. Forwarding SFC OAM packets unmodified by SFC elements that do not support SFC OAM procedures may be acceptable for a subset of OAM functions, but it can result in unexpected outcomes for others; thus, it is recommended to analyze the impact of forwarding an SFC OAM packet for all OAM functions prior to enabling this behavior. The configurable parameter MUST be disabled by default.

The actual format and additional processing of SFC OAM packets is outside the scope of this specification.

4. IANA Considerations

This document does not make any request to IANA.

5. Security Considerations

Data plane SFC-related security considerations, including privacy, are discussed in Section 6 of [RFC7665] and Section 8 of [RFC8300]. Additional security considerations related to SFC OAM are discussed in Section 9 of [RFC8924].

Any data included in an SFC OAM packet SHOULD be integrity-protected [RFC9145].

6. Acknowledgements

Thanks to Jim Guichard, Greg Mirsky, Joel Halpern, Christian Jacquenet, Dirk von-Hugo, and Carlos Pignataro for the comments.

7. References

7.1. 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>.

[RFC8300] Quinn, P., Ed., Elzur, U., Ed., and C. Pignataro, Ed., "Network Service Header (NSH)", RFC 8300, DOI 10.17487/RFC8300, January 2018, <https://www.rfc-editor.org/info/rfc8300>.

[RFC9145] Boucadair, M., Reddy.K, T., and D. Wing, "Integrity Protection for the Network Service Header (NSH) and Encryption of Sensitive Context Headers", RFC 9145, DOI 10.17487/RFC9145, December 2021, <https://www.rfc-editor.org/info/rfc9145>.

7.2. Informative References

[I-D.ietf-sfc-nsh-tlv] Wei, Y., Elzur, U., Majee, S., Pignataro, C., and D. E. Eastlake, "Network Service Header Metadata Type 2 Variable-Length Context Headers", Work in Progress, Internet-Draft, draft-ietf-sfc-nsh-tlv-13, 26 January 2022, <https://www.ietf.org/archive/id/draft-ietf-sfc-nsh-tlv-13.txt>.

[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>.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/

RFC7665, October 2015, <https://www.rfc-editor.org/info/rfc7665>.

[RFC8924] Aldrin, S., Pignataro, C., Ed., Kumar, N., Ed., Krishnan, R., and A. Ghanwani, "Service Function Chaining (SFC) Operations, Administration, and Maintenance (OAM) Framework", RFC 8924, DOI 10.17487/RFC8924, October 2020, <https://www.rfc-editor.org/info/rfc8924>.

[RFC8979] Sarikaya, B., von Hugo, D., and M. Boucadair, "Subscriber and Performance Policy Identifier Context Headers in the Network Service Header (NSH)", RFC 8979, DOI 10.17487/RFC8979, February 2021, <https://www.rfc-editor.org/info/rfc8979>.

Author's Address

Mohamed Boucadair
Orange
35000 Rennes
France

Email: mohamed.boucadair@orange.com