RFC 9451
Operations, Administration, and Maintenance (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 is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9451.

Copyright Notice

Table of Contents

1. Introduction

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

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:

Service Function Chaining (SFC) data plane element:

refs to the SFC-aware Service Function (SF), Service Function Forwarder (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 element that is capable of generating NSH OAM packets. An SFC data plane element may behave as an OAM control element.

SFC 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 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 RFC 8300

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 NSH OAM packet. Such a packet is any NSH-encapsulated packet that exclusively includes SFC OAM data. SFC 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 NSH OAM packet that triggers a response (e.g., a specific SFC-aware SF or the last SFF of an SFP).

The O bit **MUST** be set for NSH 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 NSH OAM packets even if some SFC OAM data (e.g., record route) is also supplied in the packet.

When SFC 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. In order to prevent non-deterministic behaviors, SFC data plane elements **MAY** support a configuration parameter to filter valid Next Protocol values in NSH OAM packets. Absent explicit configuration, 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 NSH OAM packet **MAY** include optional Context Headers (e.g., a subscriber identifier [RFC8979] or a flow identifier [RFC9263]) that are used to influence the processing of the packet by SFC data plane elements.

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

SFC-aware implementations of SF, SFF, SFC Proxy, and Classifier that do not support SFC OAM procedures **SHOULD** discard packets with the O bit set but **MAY** support a configurable parameter to enable forwarding received NSH OAM packets unmodified to the next element in the chain. Forwarding NSH OAM packets unmodified by SFC data plane 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 NSH 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 NSH OAM packets is outside the scope of this specification.

4. IANA Considerations

This document has no IANA actions.

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 NSH OAM packet **SHOULD** be integrity protected [RFC9145].

6. References

6.1. 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>.

6.2. Informative References

[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>.

[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>.

[RFC9263]   Wei, Y., Ed., Elzur, U., Majee, S., Pignataro, C., and D. Eastlake 3rd, "Network Service Header (NSH) Metadata Type 2 Variable-Length Context Headers", RFC 9263, DOI 10.17487/RFC9263, August 2022, <https://www.rfc-editor.org/info/rfc9263>.

Acknowledgments

Author's Address

Mohamed Boucadair
Orange
35000 Rennes
France
Email: mohamed.boucadair@orange.com