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
Copyright (c) 2023 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions
with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction
2. Terminology
3. An Update to RFC 8300
4. IANA Considerations
5. Security Considerations
6. References
   6.1. Normative References
   6.2. Informative References
Acknowledgments
Author's Address

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:
refers 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.
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


6.2. Informative References


Acknowledgments

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

Thanks to Barry Leiba for the art directorate review and Russ Housley for the security directorate review.

Thanks to Alvaro Retana and Robert Wilton for their IESG reviews.

Author's Address

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