SFC WG G. Mirsky

Internet-Draft ZTE Corp.

Updates: 8300 (if approved) W. Meng

Intended status: Standards Track ZTE Corporation

Expires: 3 December 2021 B. Khasnabish

C. Wang

Individual contributor

1 June 2021

Active OAM for Network Service Header (NSH) based Service Function Chaining

draft-ietf-sfc-multi-layer-oam-12

Abstract

A set of requirements for active Operation, Administration, and

Maintenance (OAM) of Service Function Chains (SFCs) in a network is

presented in this document. Based on these requirements, an

encapsulation of active OAM messages in SFC and a mechanism to detect

and localize defects are described.

This document updates RFC 8300. Particularly, it updates the

definition of O (OAM) bit in the Network Service Header (NSH) and

defines how an active OAM message is identified in the NSH.

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 3 December 2021.

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the

document authors. All rights reserved.

Mirsky, et al. Expires 3 December 2021 [Page 1]

Internet-Draft Active OAM for SFC June 2021

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 Simplified BSD License text

as described in Section 4.e of the Trust Legal Provisions and are

provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . 2

2. Terminology and Conventions . . . . . . . . . . . . . . . . . 4

2.1. Requirements Language . . . . . . . . . . . . . . . . . . 4

2.2. Acronyms . . . . . . . . . . . . . . . . . . . . . . . . 4

3. Requirements for Active OAM in SFC Network . . . . . . . . . 4

4. Active OAM Identification in the NSH . . . . . . . . . . . . 6

5. Echo Request/Echo Reply for SFC . . . . . . . . . . . . . . . 8

5.1. Return Codes . . . . . . . . . . . . . . . . . . . . . . 10

5.2. Authentication in Echo Request/Reply . . . . . . . . . . 11

5.3. SFC Echo Request Transmission . . . . . . . . . . . . . . 11

5.4. SFC Echo Request Reception . . . . . . . . . . . . . . . 12

5.4.1. Errored TLVs TLV . . . . . . . . . . . . . . . . . . 12

5.5. SFC Echo Reply Transmission . . . . . . . . . . . . . . . 13

5.6. SFC Echo Reply Reception . . . . . . . . . . . . . . . . 14

5.7. Tracing an SFP . . . . . . . . . . . . . . . . . . . . . 15

6. Security Considerations . . . . . . . . . . . . . . . . . . . 15

7. Acknowledgments . . . . . . . . . . . . . . . . . . . . . . . 16

8. IANA Considerations . . . . . . . . . . . . . . . . . . . . . 16

8.1. SFC Active OAM Protocol . . . . . . . . . . . . . . . . . 16

8.2. SFC Active OAM Message Type . . . . . . . . . . . . . . . 16

8.3. SFC Echo Request/Echo Reply Parameters . . . . . . . . . 17

8.4. SFC Echo Request/Echo Reply Message Types . . . . . . . . 17

8.5. SFC Echo Reply Modes . . . . . . . . . . . . . . . . . . 18

8.6. SFC Echo Return Codes . . . . . . . . . . . . . . . . . . 20

8.7. SFC TLV Type . . . . . . . . . . . . . . . . . . . . . . 21

8.8. SFC OAM UDP Port . . . . . . . . . . . . . . . . . . . . 21

9. References . . . . . . . . . . . . . . . . . . . . . . . . . 22

9.1. Normative References . . . . . . . . . . . . . . . . . . 22

9.2. Informative References . . . . . . . . . . . . . . . . . 22

Authors' Addresses . . . . . . . . . . . . . . . . . . . . . . . 24

1. Introduction

[RFC7665] defines data plane elements necessary to implement a

Service Function Chaining (SFC). These include:

Mirsky, et al. Expires 3 December 2021 [Page 2]

Internet-Draft Active OAM for SFC June 2021

1. Classifiers that perform the classification of incoming packets.

Such classification may result in associating a received packet

to a service function chain.

2. Service Function Forwarders (SFFs) that are responsible for

forwarding traffic to one or more connected Service Functions

(SFs) according to the information carried in the SFC

encapsulation and handling traffic coming back from the SFs and

forwarding it to the next SFF.

3. SFs that are responsible for executing specific service treatment

on received packets.

There are different views from different levels of the SFC. One is

the service function chain, an entirely abstract view, which defines

an ordered set of SFs that must be applied to packets selected based

on classification rules. But service function chain doesn't specify

the exact mapping between SFFs and SFs. Thus, another logical

construct used in SFC is a Service Function Path (SFP). According to

[RFC7665], SFP is the instantiation of the SFC in the network and

provides a level of indirection between the entirely abstract SFCs

and a fully specified ordered list of SFFs and SFs identities that

the packet will visit when it traverses the SFC. The latter entity

is referred to as Rendered Service Path (RSP). The main difference

between SFP and RSP is that the former is the logical construct,

while the latter is the realization of the SFP via the sequence of

specific SFC data plane elements.

This document defines how active Operation, Administration and

Maintenance (OAM), per [RFC7799] definition of active OAM, is

identified when Network Service Header (NSH) [RFC8300] is used as the SFC

encapsulation.

Following the analysis of SFC OAM in [RFC8924], this

document applies and, when necessary, extends requirements listed in

Section 4 of [RFC8924] for the use of active OAM in an SFP supporting

fault management and performance monitoring. Active OAM tools,

conformant to the requirements listed in Section 3, improve, for

example, troubleshooting efficiency and defect localization in SFP

because they specifically address architectural principles of NSH.

For that purpose, NSH Echo Request and Echo Reply are specified in

Section 5. This mechanism enables on-demand Continuity Check,

Connectivity Verification among other operations over SFC in

networks, addresses functionalities discussed in Sections 4.1, 4.2,

and 4.3 of [RFC8924]. Also, this document updates Section 2.2 of

[RFC8300] in part of the definition of O bit in the NSH.

Mirsky, et al. Expires 3 December 2021 [Page 3]

Internet-Draft Active OAM for SFC June 2021

2. Terminology and Conventions

The terminology defined in [RFC7665] is used extensively throughout

this document. The reader is expected to be familiar with it.

In this document, SFC OAM refers to an active OAM [RFC7799] in an SFC

architecture.

2.1. Requirements Language

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.

2.2. Acronyms

E2E: End-to-End

FM: Fault Management

NSH: Network Service Header

OAM: Operations, Administration, and Maintenance

RSP: Rendered Service Path

SF: Service Function

SFC: Service Function Chain

SFF: Service Function Forwarder

SFP: Service Function Path

MAC: Message Authentication Code

3. Requirements for Active OAM in SFC

As discussed in [RFC8924], SFC-specific means are needed to perform

the OAM task of fault management (FM) in an SFC architecture,

including failure detection, defect characterization, and

localization. This document defines the set of requirements for

active FM OAM mechanisms to be used in an SFC architecture.

Mirsky, et al. Expires 3 December 2021 [Page 4]

Internet-Draft Active OAM for SFC June 2021

+-----+ +-----+ +-----+ +-----+ +-----+ +-----+

|SFI11| |SFI12| |SFI21| |SFI22| |SFI31| |SFI32|

+-----+ +-----+ +-----+ +-----+ +-----+ +-----+

\ / \ / \ /

+----------+ +----+ +----+ +----+

|Classifier|---|SFF1|---------|SFF2|----------|SFF3|

+----------+ +----+ +----+ +----+

Figure 1: An Example of SFC Data Plane Architecture

In reference to the architecture example depicted in Figure 1, consider a

service function chain that includes three distinct service

functions. In this example, the SFP traverses SFF1, SFF2, and SFF3,

each SFF being connected to two instances of the same service

function. End-to-end (E2E) SFC OAM has the Classifier as the

ingress and SFF3 as its egress. Segment SFC OAM is between two

elements that are part of the same SFP. Following are the

requirements for an FM SFC OAM, whether with the E2E or segment

scope:

REQ#1: Packets of active SFC OAM SHOULD be fate sharing

with the monitored SFC data, in the forward direction from ingress

toward egress endpoint(s) of the OAM test.

The fate sharing, in the SFC environment, is achieved when a test

packet traverses the same path and receives the same treatment in the

transport layer as an SFC-encapsulated packet (e.g., NSH).

REQ#2: SFC OAM MUST support monitoring of the continuity of the

SFP between any of its elements.

A SFC failure might be declared when several consecutive test

packets are not received within a pre-determined time. For example,

in the E2E FM SFC OAM case, the egress, SFF3, in the example in

Figure 1, could be the entity that detects the SFP's failure by

monitoring a flow of periodic test packets. The ingress may be

capable of recovering from the failure, e.g., using redundant SFC

elements. Thus, it is beneficial for the egress to signal the new

defect state to the ingress, which in this example is the Classifier.

Hence the following requirement:

REQ#3: SFC OAM MUST support Remote Defect Indication notification

by the egress to the ingress.

REQ#4: SFC OAM MUST support connectivity verification of the SFP.

Definition of the misconnection defect, entry, and exit criteria

are outside the scope of this document.

Mirsky, et al. Expires 3 December 2021 [Page 5]

Internet-Draft Active OAM for SFC June 2021

Once the SFF1 detects the defect, the objective of the SFC OAM

changes from the detection of a defect to defect characterization and

localization.

REQ#5: SFC OAM MUST support fault localization of the Loss of

Continuity Check within an SFP.

REQ#6: SFC OAM MUST support an SFP tracing to discover the RSP.

In the example presented in Figure 1, two distinct instances of the

same service function share the same SFF. In this example, the SFP

can be realized over several RSPs that use different instances of SF

of the same type. For example, RSP1(SFI11--SFI21--SFI31) and

RSP2(SFI12--SFI22--SFI32). Available RSPs can be discovered using

the trace function discussed in Section 4.3 [RFC8924] or the procedure defined in Section 5.7.

REQ#7: SFC OAM MUST have the ability to discover and exercise all

available RSPs in the network.

The SFC OAM layer model described in [RFC8924] offers an approach for

a defect localization within a service function chain. As the first

step, the SFP's continuity for SFFs that are part of the same SFP

could be verified. After the reachability of SFFs has already been

verified, SFFs that serve an SF may be used as a test packet source.

In such a case, SFF can act as a proxy for another element within the

service function chain.

REQ#8: SFC OAM MUST be able to trigger on-demand FM with responses

being directed towards the initiator of such proxy request.

4. Active OAM Identification in the NSH

The O bit in the NSH is defined in [RFC8300] as follows:

O bit: Setting this bit indicates an OAM packet.

This document updates that definition as follows:

O bit: Setting this bit indicates an OAM command and/or data in

the NSH Context Header or packet payload.

Active SFC OAM is defined as a combination of OAM commands and/or

data included in a message that immediately follows the NSH. To

identify the active OAM message, the ‘Next Protocol’ field MUST

be set to Active SFC OAM (TBA1) (Section 8.1). The rules for

interpreting the values of the O bit and the ‘Next Protocol’ field are

as follows:

Mirsky, et al. Expires 3 December 2021 [Page 6]

Internet-Draft Active OAM for SFC June 2021

\* O bit set and the ‘Next Protocol’ value does not match one of identifying

active or hybrid OAM protocols (per [RFC7799] definitions), e.g.,

defined in this specification Active SFC OAM:

- a Fixed-Length Context Header or Variable-Length Context

Header(s) contain an OAM command or data.

- the type of payload is determined by the Next Protocol field.

\* O bit set and the ‘Next Protocol’ value matches one of identifying active

or hybrid OAM protocols:

- the payload that immediately follows the NSH MUST contain an

OAM command or data.

\* O bit is clear:

- no OAM in a Fixed-Length Context Header or Variable-Length

Context Header(s).

- the payload determined by the ‘Next Protocol’ field

MUST be present.

\* O bit is clear and the ‘Next Protocol’ field identifies

active or hybrid OAM protocol MUST be identified and reported as

an erroneous combination. An implementation MAY have control to

enable processing of the OAM payload.

One conclusion from the above-listed rules of processing the O bit

and the ‘Next Protocol’ field is to avoid the combination of

OAM in an NSH Context Header (Fixed-Length or Variable-Length) and

the payload immediately following the NSH because there is no

unambiguous way to identify such combination using the O bit and the

Next Protocol field.

As demonstrated in Section 4 [RFC8924] and Section 3 of this

document, SFC OAM is required to perform multiple tasks. Several

active OAM protocols could be used to address all the requirements.

When IP/UDP encapsulation of an SFC OAM control message is used,

protocols can be demultiplexed using the destination UDP port number.

But extra IP/UDP headers, especially in an IPv6 network, add

noticeable overhead. This document defines Active OAM Header

(Figure 2) to demultiplex active OAM protocols on an SFC.

Mirsky, et al. Expires 3 December 2021 [Page 7]

Internet-Draft Active OAM for SFC June 2021

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| V | Msg Type | Flags | Length |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

~ NSH Active OAM Control Packet ~

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Figure 2: NSH Active OAM Header

V - two-bit-long field indicates the current version of the NSH

active OAM header. The current value is 0. Future versions may be assigned as per Section 8.1.

Msg Type - six bits long field identifies OAM protocol, e.g., Echo

Request/Reply or Bidirectional Forwarding Detection.

Flags - eight bits long field carries bit flags that define

optional capability and thus processing of the NSH active OAM

control packet, e.g., optional timestamping.

Length - two octets long field that is the length of the NSH

active OAM control packet in octets.

5. Echo Request/Echo Reply for SFC

Echo Request/Reply is a well-known active OAM mechanism that is

extensively used to verify a path's continuity, detect

inconsistencies between a state in control and the data planes, and

localize defects in the data plane. ICMP ([RFC0792] for IPv4 and

[RFC4443] for IPv6 networks respectively) and [RFC8029] are examples

of broadly used active OAM protocols based on Echo Request/Reply

principle. The NSH Echo Request/Reply defined in this document

addresses several requirements listed in Section 3. Specifically, it can be used to check the continuity

of an SFP, trace an SFP, or localize the failure within an SFP. The

NSH Echo Request/Reply control message format is presented in

Figure 3.

Mirsky, et al. Expires 3 December 2021 [Page 8]

Internet-Draft Active OAM for SFC June 2021

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| V | Reserved | Global Flags |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Message Type | Reply mode | Return Code |Return Subcode |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Sender's Handle |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Sequence Number |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

~ TLVs ~

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Figure 3: SFC Echo Request/Reply Format

The interpretation of the fields is as follows:

Version (V) is a two-bit field that indicates the current version

of the SFC Echo Request/Reply. The current value is 0. The

version number is to be incremented whenever a change is made that

affects the ability of an implementation to parse or process

control packet correctly.

Reserved - fourteen-bit field. It MUST be zeroed on transmission

and ignored on receipt.

The Global Flags is a two-octet bit vector field.

The Message Type is a one-octet field that reflects the packet

type. Value TBA3 identifies Echo Request and TBA4 - Echo Reply.

The Reply Mode is a one-octet field. It defines the type of the

return path requested by the sender of the Echo Request.

Return Codes and Subcodes are one-octet fields each. These can be

used to inform the sender about the result of processing its

request. Initial Return Code values are provided in Table 1.

For all Return Code values defined in this document, the value of

the Return Subcode field MUST be set to zero.

The Sender's Handle is a four-octet field. It MUST filled in by the

sender of the Echo Request and returned unchanged by the Echo

Reply sender (if needed). The sender of the Echo Request SHOULD use a pseudo-

random number generator to set the value of the Sender's Handle

field.

Mirsky, et al. Expires 3 December 2021 [Page 9]

Internet-Draft Active OAM for SFC June 2021

The Sequence Number is a four-octet field. It is assigned by the

sender and can be, for example, used to detect missed replies.

The initial Sequence Number MUST randomly generated and then SHOULD be monotonically

increasing in the course of a test session.

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Type | Reserved | Length |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

~ Value ~

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Figure 4: NSH Echo Request/Reply TLV Format

TLV is a variable-length field. Multiple TLVs MAY be placed in an

NSH Echo Request/Reply packet. Additional TLVs may be enclosed

within a given TLV, subject to the semantics of the (outer) TLV in

question. If more than one TLV is to be included, the value of the

Type field of the outmost outer TLV MUST be set to “Multiple TLVs Used"

(TBA12), as assigned by IANA according to Section 8.7. Figure 4

presents the format of an NSH Echo Request/Reply TLV, where fields

are defined as follows:

Type - a one-octet-long field that characterizes the

interpretation of the Value field. Type values allocated

according to Section 8.7.

Reserved - one-octet-long field. The value of the Type field

determines its interpretation and encoding.

Length - two-octet-long field equal to the Value field's length in

octets.

Value - a variable-length field. The value of the Type field

determines its interpretation and encoding.

5.1. Return Codes

The value of the Return Code field is set to zero by the sender of an

Echo Request. The receiver of said Echo Request can set it to one of

the values listed in Table 1 in the corresponding Echo Reply that it

generates (if any).

Mirsky, et al. Expires 3 December 2021 [Page 10]

Internet-Draft Active OAM for SFC June 2021

+=======+============================================+

| Value | Description |

+=======+============================================+

| 0 | No Return Code |

+-------+--------------------------------------------+

| 1 | Malformed Echo Request received |

+-------+--------------------------------------------+

| 2 | One or more of the TLVs was not understood |

+-------+--------------------------------------------+

| 3 | Authentication failed |

+-------+--------------------------------------------+

Table 1: NSH Echo Return Codes

5.2. Authentication in Echo Request/Reply

Authentication can be used to protect the integrity of the

information in SFC Echo Request and/or Echo Reply. In the

[I-D.ietf-sfc-nsh-integrity] a variable-length Context Header has

been defined to protect the integrity of the NSH and the payload.

The header can also be used for the optional encryption of the

sensitive metadata. MAC#1 Context Header is more suitable for the

integrity protection of active SFC OAM, particularly of the defined

in this document SFC Echo Request and Echo Reply. On the other hand,

using MAC#2 Context Header allows the detection of mishandling of the

O-bit by a transient SFC element.

5.3. NSH Echo Request Transmission

SFC Echo Request control packet MUST use the appropriate transport

encapsulation of the monitored SFP. If the NSH is used, Echo Request

MUST set O bit, as defined in [RFC8300]. NSH MUST be immediately

followed by the SFC Active OAM Header defined in Section 4. The

Message Type field's value in the NSH Active OAM Header MUST be set

to NSH Echo Request/Echo Reply value (TBA2) per Section 8.2.

Value of the Reply Mode field MAY be set to:

\* Do Not Reply (TBA5) if one-way monitoring is desired. If the Echo

Request is used to measure synthetic packet loss; the receiver may

report loss measurement results to a remote node. Note that ways

of learning the identity of that node is outside the scope of this

specification.

\* Reply via an IPv4/IPv6 UDP Packet (TBA6) value likely will be the

most used.

Mirsky, et al. Expires 3 December 2021 [Page 11]

Internet-Draft Active OAM for SFC June 2021

\* Reply via Application Level Control Channel (TBA7) value if the

SFP may have bi-directional paths.

\* Reply via Specified Path (TBA8) value to enforce the use of the

particular return path specified in the included TLV to verify bi-

directional continuity and also increase the robustness of the

monitoring by selecting a more stable path.

[I-D.ao-sfc-oam-return-path-specified] provides an example of

providing an explicit path for the Echo Reply.

5.4. NSH Echo Request Reception

Sending an NSH Echo Request to the control plane is triggered by one

of the following packet processing exceptions: NSH TTL expiration,

NSH Service Index (SI) expiration, or the receiver is the terminal

SFF for an SFP.

Firstly, if the NSH Echo Request is authenticated, the receiving SFF

MUST verify the authentication. If the verification fails, the

receiver SFF MUST send an NSH Echo Reply with the Return Code set to

"Authentication failed" and the Subcode set to zero. Then, the SFF

that has received an NSH Echo Request verifies the received packet's

general sanity. If the packet is not well-formed, the receiver SFF

SHOULD send an NSH Echo Reply with the Return Code set to "Malformed

Echo Request received" and the Subcode set to zero. If there are any

TLVs that the SFF does not understand, the SFF MUST send an NSH Echo

Reply with the Return Code set to 2 ("One or more TLVs was not

understood") and set the Subcode to zero. In the latter case, the

SFF MAY include an “Errored TLVs” TLV (Section 5.4.1) that, as sub-

TLVs, contains only the TLVs that it was unable to parse/process. The header field's

Sender's Handle and Sequence Number are not examined but are included in

the NSH Echo Reply message. If the sanity check of the received Echo

Request succeeded, then the SFF at the end of the SFP MUST set the

Return Code value to 5 ("End of the SFP") and the Subcode set to

zero. If the SFF is not at the end of the SFP and the TTL value is 1,

the value of the Return Code MUST be set to 4 ("TTL Exceeded") and

the Subcode set to zero.

5.4.1. “Errored TLVs” TLV

If the Return Code for the Echo Reply is determined as 2 ("One or

more TLVs was not understood"), then the “Errored TLVs” TLV may be

included in an Echo Reply. The use of this TLV is meant to inform the

sender of an Echo Request of mandatory TLVs either not supported by

an implementation or parsed and found to be in error.

Mirsky, et al. Expires 3 December 2021 [Page 12]

Internet-Draft Active OAM for SFC June 2021

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Errored TLVs | Reserved | Length |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Value |

. .

. .

. .

| |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Figure 5: Errored TLVs TLV

where

The Errored TLVs Type MUST be set to TBA14 Section 8.7.

Reserved - one-octet-long field.

Length - two-octet-long field equal to the length of the Value

field in octets.

The Value field contains the TLVs, encoded as sub-TLVs, that were

not understood or failed to be parsed correctly.

5.5. NSH Echo Reply Transmission

The ‘Reply Mode’ field directs whether and how the Echo Reply message

should be sent. The sender of the Echo Request MAY use TLVs to

request that the corresponding Echo Reply is transmitted over the

specified path. [I-D.ao-sfc-oam-return-path-specified] provides an

example of a TLV that can be used to specify the return path of the Echo

Reply. Value TBA3 is referred to as the "Do not reply" mode and

suppresses the Echo Reply packet transmission. The default value

(TBA6) for the Reply mode field requests the responder to send the

Echo Reply packet out-of-band as IPv4 or IPv6 UDP packet.

Responder to the NSH Echo Request encapsulates the Echo Reply in an IP/UDP packet

if the Reply mode is Reply via an IPv4/IPv6 UDP Packet.

Because the NSH does not identify the ingress node that generated the

Echo Request, the source ID MUST be included in the message and used

as the IP destination address for IP/UDP encapsulation of the NSH

Echo Reply. The sender of the NSH Echo Request MUST include a SFC

Source TLV (Figure 6).

Mirsky, et al. Expires 3 December 2021 [Page 13]

Internet-Draft Active OAM for SFC June 2021

0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Source ID | Reserved | Length |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

| Value |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Figure 6: SFC Source TLV

where

Source ID Type is a one-octet-long field and has the value of

TBA13 Section 8.7.

Reserved - one-octet-long field.

Length is a two-octets-long field, and the value equals the length

of the Value field in octets.

Value field contains the IP address of the sender of the SFC OAM

control message, IPv4 or IPv6.

The UDP destination port for SFC Echo Reply TBA15 will be allocated

by IANA Section 8.8.

5.6. NSH Echo Reply Reception

An SFF SHOULD NOT accept an NSH Echo Reply unless the received reply passes

the following checks:

\* the received NSH Echo Reply is well-formed;

\* it has an outstanding NSH Echo Request sent from the UDP port that

matches destination UDP port number of the received packet;

\* if the matching to the Echo Request found, the value of the

Sender's Handle in the Echo Request sent is equal to the value of

Sender's Handle in the Echo Reply received;

\* if all checks passed, the SFF checks if the Sequence Number in the

Echo Request sent matches to the Sequence Number in the received Echo Reply

.

Mirsky, et al. Expires 3 December 2021 [Page 14]

Internet-Draft Active OAM for SFC June 2021

5.7. Tracing an SFP

NSH Echo Request/Reply can be used to isolate a defect detected in

the SFP and trace an RSP. As for ICMP echo request/reply [RFC0792]

and MPLS echo request/reply [RFC8029], this mode is referred to as

"traceroute". In the traceroute mode, the sender transmits a

sequence of SFC Echo Request messages starting with the NSH TTL value

set to 1 and is incremented by 1 in each next Echo Request packet.

The sender stops transmitting SFC Echo Request packets when the

Return Code in the received Echo Reply equals 5 ("End of the SFP").

Suppose a specialized information element (e.g., IPv6 Flow Label

[RFC6437] or Flow ID [I-D.ietf-sfc-nsh-tlv]) is used for distributing

the load across Equal Cost Multi-Path or Link Aggregation Group

paths. In that case, such an element MAY also be used for the SFC

OAM traffic. Doing so is meant to control whether the SFC Echo

Request follows the same RSP as the monitored flow.

6. Security Considerations

When the integrity protection for SFC active OAM, and NSH Echo

Request/Reply in particular, is required, it is RECOMMENDED to use

one of Context Headers defined in [I-D.ietf-sfc-nsh-integrity].

MAC#1 (Message Authentication Code) Context Header could be more

suitable for active SFC OAM because it does not require re-

calculation of the MAC when the value of the NSH Base Header's TTL

field is changed. The integrity protection for SFC active OAM can

also be achieved using mechanisms in the underlay data plane. For

example, if the underlay is an IPv6 network, IP Authentication Header

[RFC4302] or IP Encapsulating Security Payload Header [RFC4303] can

be used to provide integrity protection. Confidentiality for the SFC

Echo Request/Reply exchanges can be achieved using the IP

Encapsulating Security Payload Header [RFC4303]. Also, the security

needs for SFC Echo Request/Reply are similar to those of ICMP ping

[RFC0792], [RFC4443] and MPLS LSP ping [RFC8029].

There are at least three approaches to attacking a node in the

overlay network using the mechanisms defined in the document. One is

a Denial-of-Service attack, sending an SFC Echo Request to overload

an element of the SFC. The second may use spoofing, hijacking,

replying, or otherwise tampering with SFC Echo Requests and/or

replies to misrepresent, alter the operator's view of the state of

the SFC. The third is an unauthorized source using an SFC Echo

Request/Reply to obtain information about the SFC and/or its

elements, e.g., SFF or SF.

Mirsky, et al. Expires 3 December 2021 [Page 15]

Internet-Draft Active OAM for SFC June 2021

It is RECOMMENDED that implementations throttle the SFC ping traffic

going to the control plane to mitigate potential Denial-of-Service

attacks.

Reply and spoofing attacks involving faking or replying to SFC Echo

Reply messages would have to match the Sender's Handle and Sequence

Number of an outstanding SFC Echo Request message, which is highly

unlikely. Thus the non-matching reply would be discarded.

To protect against unauthorized sources trying to obtain information

about the overlay and/or underlay, an implementation MAY check that

the source of the Echo Request is indeed part of the SFP.

7. Acknowledgments

Authors greatly appreciate thorough review and the most helpful

comments from Dan Wing, Dirk von Hugo, and Mohamed Boucadair.

8. IANA Considerations

8.x. NSH OAM Versions

IANA is requested to create a new registry entitled “NSH Active OAM Versions”.

New values are assigned via Standards Action [[RFC8126](https://datatracker.ietf.org/doc/html/rfc8126" \o ")].

The registry is populated as follows:

+-------------+---------------------------------+-----------+

| Version | Description | Reference |

+-------------+---------------------------------+-----------+

| Version 00b | Version 0 | [RFCXXXX](https://datatracker.ietf.org/doc/html/rfc8300) |

| Version 01b | Unassigned | |

| Version 10b | Unassigned | |

| Version 11b | Unassigned | |

+-------------+---------------------------------+-----------+

8.x. NSH Active OAM Protocol

IANA is requested to assign a new type from the SFC Next Protocol

registry as follows:

+=======+================+===============+

| Value | Description | Reference |

+=======+================+===============+

| TBA1 | SFC Active OAM | This document |

+-------+----------------+---------------+

Table 2: SFC Active OAM Protocol

8.2. SFC Active OAM Message Type

IANA is requested to create a new registry called "NSH Active OAM

Message Type". All code points in the range 1 through 32767 in this

registry shall be allocated according to the "IETF Review" procedure

specified in [RFC8126]. The remaining code points to be allocated

according to Table 3:

Mirsky, et al. Expires 3 December 2021 [Page 16]

Internet-Draft Active OAM for SFC June 2021

+===============+=============+=========================+

| Value | Description | Reference |

+===============+=============+=========================+

| 0 | Reserved | |

+---------------+-------------+-------------------------+

| 1 - 32767 | Reserved | IETF Consensus |

+---------------+-------------+-------------------------+

| 32768 - 65530 | Reserved | First Come First Served |

+---------------+-------------+-------------------------+

| 65531 - 65534 | Reserved | Private Use |

+---------------+-------------+-------------------------+

| 65535 | Reserved | |

+---------------+-------------+-------------------------+

Table 3: NSH Active OAM Message Type

IANA is requested to assign a new type from the NSH Active OAM

Message Type registry as follows:

+=======+=============================+===============+

| Value | Description | Reference |

+=======+=============================+===============+

| TBA2 | NSH Echo Request/Echo Reply | This document |

+-------+-----------------------------+---------------+

Table 4: SFC Echo Request/Echo Reply Type

8.3. NSH Echo Request/Echo Reply Parameters

IANA is requested to create a new NSH Echo Request/Echo Reply

Parameters registry.

8.4. NSH Echo Request/Echo Reply Message Types

IANA is requested to create in the NSH Echo Request/Echo Reply

Parameters registry the new sub-registry Message Types. All code

points in the range 1 through 175 in this registry shall be allocated

according to the "IETF Review" procedure specified in [RFC8126].

Code points in the range 176 through 239 in this registry shall be

allocated according to the "First Come First Served" procedure

specified in [RFC8126]. The remaining code points are allocated

according to Table 5: as specified in Table 5.

Mirsky, et al. Expires 3 December 2021 [Page 17]

Internet-Draft Active OAM for SFC June 2021

+===========+==============+===============+

| Value | Description | Reference |

+===========+==============+===============+

| 0 | Reserved | This document |

+-----------+--------------+---------------+

| 1- 175 | Unassigned | This document |

+-----------+--------------+---------------+

| 176 - 239 | Unassigned | This document |

+-----------+--------------+---------------+

| 240 - 251 | Experimental | This document |

+-----------+--------------+---------------+

| 252 - 254 | Private Use | This document |

+-----------+--------------+---------------+

| 255 | Reserved | This document |

+-----------+--------------+---------------+

Table 5: SFC Echo Request/Echo Reply

Message Types

IANA is requested to assign values as listed in Table 6.

+=======+==================+===============+

| Value | Description | Reference |

+=======+==================+===============+

| TBA3 | NSH Echo Request | This document |

+-------+------------------+---------------+

| TBA4 | NSH Echo Reply | This document |

+-------+------------------+---------------+

Table 6: NSH Echo Request/Echo Reply

Message Types Values

8.5. NSH Echo Reply Modes

IANA is requested to create in the NSH Echo Request/Echo Reply

Parameters registry the new sub-registry Reply Mode. All code points

in the range 1 through 175 in this registry shall be allocated

according to the "IETF Review" procedure specified in [RFC8126].

Code points in the range 176 through 239 in this registry shall be

allocated according to the "First Come First Served" procedure

specified in [RFC8126]. The remaining code points are allocated

according to Table 7:

Mirsky, et al. Expires 3 December 2021 [Page 18]

Internet-Draft Active OAM for SFC June 2021

+===========+==============+===============+

| Value | Description | Reference |

+===========+==============+===============+

| 0 | Reserved | This document |

+-----------+--------------+---------------+

| 1- 175 | Unassigned | This document |

+-----------+--------------+---------------+

| 176 - 239 | Unassigned | This document |

+-----------+--------------+---------------+

| 240 - 251 | Experimental | This document |

+-----------+--------------+---------------+

| 252 - 254 | Private Use | This document |

+-----------+--------------+---------------+

| 255 | Reserved | This document |

+-----------+--------------+---------------+

Table 7: SFC Echo Reply Mode

All code points in the range 1 through 191 in this registry shall be

allocated according to the "IETF Review" procedure specified in

[RFC8126] and assign values as listed in Table 8.

+=======+====================================+===============+

| Value | Description | Reference |

+=======+====================================+===============+

| 0 | Reserved | |

+-------+------------------------------------+---------------+

| TBA5 | Do Not Reply | This document |

+-------+------------------------------------+---------------+

| TBA6 | Reply via an IPv4/IPv6 UDP Packet | This document |

+-------+------------------------------------+---------------+

| TBA7 | Reply via Application Level | This document |

| | Control Channel | |

+-------+------------------------------------+---------------+

| TBA8 | Reply via Specified Path | This document |

+-------+------------------------------------+---------------+

| TBA9 | Reply via an IPv4/IPv6 UDP Packet | This document |

| | with the data integrity protection | |

+-------+------------------------------------+---------------+

| TBA10 | Reply via Application Level | This document |

| | Control Channel with the data | |

| | integrity protection | |

+-------+------------------------------------+---------------+

| TBA11 | Reply via Specified Path with the | This document |

| | data integrity protection | |

+-------+------------------------------------+---------------+

Table 8: SFC Echo Reply Mode Values

Mirsky, et al. Expires 3 December 2021 [Page 19]

Internet-Draft Active OAM for SFC June 2021

8.6. NSH Echo Return Codes

IANA is requested to create in the NSH Echo Request/Echo Reply

Parameters registry the new sub-registry Return Codes as described in

Table 9.

+=========+=============+=========================+

| Value | Description | Reference |

+=========+=============+=========================+

| 0-191 | Unassigned | IETF Review |

+---------+-------------+-------------------------+

| 192-251 | Unassigned | First Come First Served |

+---------+-------------+-------------------------+

| 252-254 | Unassigned | Private Use |

+---------+-------------+-------------------------+

| 255 | Reserved | |

+---------+-------------+-------------------------+

Table 9: NSH Echo Return Codes

Values defined for the Return Codes sub-registry are listed in

Table 10.

+=======+=================================+===============+

| Value | Description | Reference |

+=======+=================================+===============+

| 0 | No Return Code | This document |

+-------+---------------------------------+---------------+

| 1 | Malformed Echo Request received | This document |

+-------+---------------------------------+---------------+

| 2 | One or more of the TLVs was not | This document |

| | understood | |

+-------+---------------------------------+---------------+

| 3 | Authentication failed | This document |

+-------+---------------------------------+---------------+

| 4 | TTL Exceeded | This document |

+-------+---------------------------------+---------------+

| 5 | End of the SFP | This document |

+-------+---------------------------------+---------------+

Table 10: NSH Echo Return Codes Values

Mirsky, et al. Expires 3 December 2021 [Page 20]

Internet-Draft Active OAM for SFC June 2021

8.7. NSH TLV Type

IANA is requested to create the NSH OAM TLV Type registry. All code

points in the range 1 through 175 in this registry shall be allocated

according to the "IETF Review" procedure specified in [RFC8126].

Code points in the range 176 through 239 in this registry shall be

allocated according to the "First Come First Served" procedure

specified in [RFC8126]. The remaining code points are allocated

according to Table 11:

+===========+==============+===============+

| Value | Description | Reference |

+===========+==============+===============+

| 0 | Reserved | This document |

+-----------+--------------+---------------+

| 1- 175 | Unassigned | This document |

+-----------+--------------+---------------+

| 176 - 239 | Unassigned | This document |

+-----------+--------------+---------------+

| 240 - 251 | Experimental | This document |

+-----------+--------------+---------------+

| 252 - 254 | Private Use | This document |

+-----------+--------------+---------------+

| 255 | Reserved | This document |

+-----------+--------------+---------------+

Table 11: NSH OAM TLV Type Registry

This document defines the following new values in NSH OAM TLV Type

registry:

+=======+====================+===============+

| Value | Description | Reference |

+=======+====================+===============+

| TBA12 | Multiple TLVs Used | This document |

+-------+--------------------+---------------+

| TBA13 | Source ID TLV | This document |

+-------+--------------------+---------------+

| TBA14 | Errored TLVs | This document |

+-------+--------------------+---------------+

Table 12: SFC OAM Type Values

8.8. SFC OAM UDP Port

IANA is requested to allocate UDP port number according to

Mirsky, et al. Expires 3 December 2021 [Page 21]

Internet-Draft Active OAM for SFC June 2021

+=============+============+===================+============+=====================+=============+

|Service Name |Port Number |Transport Protocol |Description |Semantics Definition |Reference |

+=============+============+===================+============+=====================+=============+

|SFC OAM |TBA15 |UDP |SFC OAM Echo|Section 5.5 |This document|

| | | |Reply | | |

+-------------+------------+-------------------+------------+---------------------+-------------+

Table 13: SFC OAM Port

9. References

9.1. 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>.

9.2. Informative References

[I-D.ao-sfc-oam-return-path-specified]

Mirsky, G., Ao, T., Chen, Z., and G. Mishra, "Controlled

Return Path for Service Function Chain (SFC) OAM", Work in

Progress, Internet-Draft, draft-ao-sfc-oam-return-path-

specified-09, 30 March 2021, <https://tools.ietf.org/html/

draft-ao-sfc-oam-return-path-specified-09>.

[I-D.ietf-sfc-nsh-integrity]

Boucadair, M., Reddy, T., and D. Wing, "Integrity

Protection for the Network Service Header (NSH) and

Encryption of Sensitive Context Headers", Work in

Progress, Internet-Draft, draft-ietf-sfc-nsh-integrity-05,

23 March 2021, <https://tools.ietf.org/html/draft-ietf-

sfc-nsh-integrity-05>.

Mirsky, et al. Expires 3 December 2021 [Page 22]

Internet-Draft Active OAM for SFC June 2021

[I-D.ietf-sfc-nsh-tlv]

Wei, Y. (., Elzur, U., Majee, S., and C. Pignataro,

"Network Service Header Metadata Type 2 Variable-Length

Context Headers", Work in Progress, Internet-Draft, draft-

ietf-sfc-nsh-tlv-06, 12 May 2021,

<https://tools.ietf.org/html/draft-ietf-sfc-nsh-tlv-06>.

[RFC0792] Postel, J., "Internet Control Message Protocol", STD 5,

RFC 792, DOI 10.17487/RFC0792, September 1981,

<https://www.rfc-editor.org/info/rfc792>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302,

DOI 10.17487/RFC4302, December 2005,

<https://www.rfc-editor.org/info/rfc4302>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)",

RFC 4303, DOI 10.17487/RFC4303, December 2005,

<https://www.rfc-editor.org/info/rfc4303>.

[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>.

[RFC6437] Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme,

"IPv6 Flow Label Specification", RFC 6437,

DOI 10.17487/RFC6437, November 2011,

<https://www.rfc-editor.org/info/rfc6437>.

[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>.

[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>.

[RFC8029] Kompella, K., Swallow, G., Pignataro, C., Ed., Kumar, N.,

Aldrin, S., and M. Chen, "Detecting Multiprotocol Label

Switched (MPLS) Data-Plane Failures", RFC 8029,

DOI 10.17487/RFC8029, March 2017,

<https://www.rfc-editor.org/info/rfc8029>.

Mirsky, et al. Expires 3 December 2021 [Page 23]

Internet-Draft Active OAM for SFC June 2021

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for

Writing an IANA Considerations Section in RFCs", BCP 26,

RFC 8126, DOI 10.17487/RFC8126, June 2017,

<https://www.rfc-editor.org/info/rfc8126>.

[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>.

Authors' Addresses

Greg Mirsky

ZTE Corp.

Email: gregimirsky@gmail.com, gregory.mirsky@ztetx.com

Wei Meng

ZTE Corporation

No.50 Software Avenue, Yuhuatai District

Nanjing,

China

Email: meng.wei2@zte.com.cn

Bhumip Khasnabish

Individual contributor

Email: vumip1@gmail.com

Cui Wang

Individual contributor

Email: lindawangjoy@gmail.com

Mirsky, et al. Expires 3 December 2021 [Page 24]