Workgroup: SFC WG
Internet-Draft:
draft-ietf-sfc-multi-layer-oam-10
Updates: 8300 (if approved)
Published: 30 March 2021
Intended Status: Standards Track
Expires: 1 October 2021
Authors: G. Mirsky, ZTE Corp.; W. Meng, ZTE Corporation; B. Khasnabish, Individual contributor; C. Wang, Individual contributor

Active OAM for Service Function Chaining

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 in 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

Copyright Notice

Table of Contents

1. Introduction

[RFC7665] defines components necessary to implement a Service Function Chain (SFC). These include:

1. a classifier that performs the classification of incoming packets

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 service encapsulation and handling traffic coming back from the SF and forwarding it to the next SFF.

3. SFs that are responsible for the executing specific service treatment on received packets.

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

This document defines how active Operation, Administration and Maintenance (OAM), per [RFC7799] definition of active OAM, is identified in Network Service Header (NSH) SFC. Following the analysis of SFC OAM in [RFC8924], this document lists requirements to improve troubleshooting efficiency and defect localization in SFP. For that purpose, SFC Echo Request and Echo Reply are specified in the document. This mechanism enables on-demand Continuity Check, Connectivity Verification among other operations over SFC in networks, thus providing one of the most common SFC OAM functions identified in [RFC8924]. Also, this document updates Section 2.2 of [RFC8300] in part of the definition of O bit in the (NSH).

2. Terminology and Conventions

The terminology defined in [RFC7665] is used extensively throughout this document. A reader is expected to be familiar with it.

In this document, SFC OAM refers to an active OAM, as defined in [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

PRNG: Pseudorandom number generator

RDI: Remote Defect Indication

RSP: Rendered Service Path

SMI Structure of Management Information

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 Network

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.

```
                +----+ +----+  +----+ +----+ +----+ +----+
                |SF1|  |SF2|   |SF3|  |SF4|  |SF5|  |SF6|
                +----+ +----+  +----+ +----+ +----+ +----+
                   \    /         \  /         \  /
+----------+       +-----+        +-----+       +-----+
|Classifier|-------|SFF1|---------|SFF2|--------|SFF3|
+----------+       +-----+        +-----+       +-----+
```

Figure 1: SFC Data Plane Reference Model

Regarding the reference model 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, in this example, has the Classifier as the ingress of the SFC OAM domain, and SFF3 - as its egress. Segment SFC OAM is always within the E2E SFC OAM domain 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 in SFC 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 NSH packet.

REQ#2: SFC OAM MUST support pro-active monitoring of the continuity of the SFP between any of its elements.

A network failure might be declared when several consecutive test packets are not received within a pre-determined time. For example, in the E2E SFC OAM FM 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 (RDI) 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.

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, for instance, RSP1(SF1--SF3--SF5) and RSP2(SF2--SF4--SF6). Available RSPs can be discovered using the trace function discussed in Section 4.3 [RFC8924].

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 efficient 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 SFC NSH

The O bit in the NSH header 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's value MUST be set to Active SFC OAM (TBA1) (Section 8.1). The rules for interpreting the values of O bit and the Next Protocol field are as follows:

- O bit set and the Next Protocol value is not one of identifying active or hybrid OAM protocol (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 is one of identifying active or hybrid OAM protocol:

- the payload that immediately follows SFC 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's value MUST be present.

*O bit is clear and the Next Protocol field's value identifies active or hybrid OAM protocol MUST be identified and reported as the erroneous combination. An implementation MAY have control to enable processing of the OAM payload.

One conclusion from the above-listed rules of processing O bit and the Next Protocol field's value is to avoid the combination of OAM in an NSH Context Header (Fixed-Length or Variable-Length) and the payload immediately following the SFC 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.

```
 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              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~              SFC Active OAM Control Packet                    ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: SFC Active OAM Header

V - two-bit-long field indicates the current version of the SFC active OAM header. The current value is 0.

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 SFC active OAM control packet, e.g., optional timestamping.

Length - two octets long field that is the length of the SFC 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 SFC NSH Echo Request/Reply control message format is presented in Figure 3.

```
 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 according to 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 is filled in by the sender of the Echo Request and returned unchanged by the Echo Reply sender. The sender of the Echo Request MAY use a pseudo-random number generator (PRNG) to set the value of the Sender's Handle field.

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 value of the Sequence Number field SHOULD be monotonically increasing in the course of the 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: SFC Echo Request/Reply TLV Format

TLV is a variable-length field. Multiple TLVs MAY be placed in an SFC 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 SFC Echo Request/Reply TLV, where fields are defined as the following:

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.

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: SFC 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. SFC Echo Request Transmission

SFC Echo Request control packet MUST use the appropriate encapsulation of the monitored SFP. If the NSH is used, Echo Request MUST set O bit, as defined in [RFC8300]. SFC NSH MUST be immediately followed by the SFC Active OAM Header defined in Section 4. The Message Type field's value in the SFC Active OAM Header MUST be set to SFC 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.

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

* 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.

5.4. SFC Echo Request Reception

Sending an SFC 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 SFC Echo Request is authenticated, the receiving SFF MUST verify the authentication. If the verification fails, the receiver SFF MUST send an SFC Echo Reply with the Return Code set to "Authentication failed" and the Subcode set to zero. Then, the SFF that has received an SFC Echo Request verifies the received packet's general sanity. If the packet is not well-formed, the receiver SFF SHOULD send an SFC Echo Reply with the Return Code set to "Malformed Echo Request received" and the Subcode set to zero. If there are any TLVs that SFF does not understand, the SFF MUST send an SFC 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 misunderstood TLVs. The header field's Sender's Handle, Sequence Number are not examined but are included in the SFC Echo Reply message.

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 allows informing the sender of an Echo Request of mandatory TLVs either not supported by an implementation or parsed and found to be in error.

```
     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. SFC 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. 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 SFC Echo Request sends the Echo Reply over IP network if the Reply mode is Reply via an IPv4/IPv6 UDP Packet. Because SFC NSH does not identify the ingress of the SFP, 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 SFC Echo Reply. The sender of the SFC Echo Request MUST include SFC Source TLV Figure 6.

```
 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. SFC Echo Reply Reception

An SFF SHOULD NOT accept SFC Echo Reply unless the received passes the following checks:

* the received SFC Echo Reply is well-formed;

* it has an outstanding SFC 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 n 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 Echo Reply received.

6. Security Considerations

When the integrity protection for SFC active OAM, and SFC 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.

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

8.1. SFC 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 "SFC 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:

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: SFC Active OAM Message Type

IANA is requested to assign a new type from the SFC Active OAM Message Type registry as follows:

Value	Description	Reference
TBA2	SFC Echo Request/Echo Reply	This document

Table 4: SFC Echo Request/Echo Reply Type

8.3. SFC Echo Request/Echo Reply Parameters

IANA is requested to create a new SFC Echo Request/Echo Reply Parameters registry.

8.4. SFC Echo Request/Echo Reply Message Types

IANA is requested to create in the SFC 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.

Value	Description	Reference
0	Reserved	This document
1- 175	Unassigned	This document

Value	Description	Reference
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	SFC Echo Request	This document
TBA4	SFC Echo Reply	This document

Table 6: SFC Echo Request/Echo Reply Message Types Values

8.5. SFC Echo Reply Modes

IANA is requested to create in the SFC 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: as specified in Table 7.

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 Control Channel	This document

Value	Description	Reference
TBA8	Reply via Specified Path	This document
TBA9	Reply via an IPv4/IPv6 UDP Packet with the data integrity protection	This document
TBA10	Reply via Application Level Control Channel with the data integrity protection	This document
TBA11	Reply via Specified Path with the data integrity protection	This document

Table 8: SFC Echo Reply Mode Values

8.6. SFC Echo Return Codes

IANA is requested to create in the SFC 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: SFC 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 understood	This document
3	Authentication failed	This document

Table 10: SFC Echo Return Codes Values

8.7. SFC TLV Type

IANA is requested to create the SFC 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

Value	Description	Reference
176 - 239	Unassigned	This document
240 - 251	Experimental	This document
252 - 254	Private Use	This document
255	Reserved	This document

Table 11: SFC OAM TLV Type Registry

This document defines the following new values in SFC 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

Service Name	Port Number	Transport Protocol	Description	Semantics Definition	Refe
SFC OAM	TBA15	UDP	SFC OAM Echo Reply	Section 5.5	This

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.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>.

[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>.

[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>.

[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