SFC WG G. Mirsky
Internet-Draft ZTE Corp.
Updates: 8300 (if approved) W. Meng
Intended status: Standards Track ZTE Corporation
Expires: June 17, 2021 B. Khasnabish
C. Wang
Individual contributor
December 14, 2020

Active OAM for Service Function Chains in Networks
draft-ietf-sfc-multi-layer-oam-07

Abstract

A set of requirements for active Operation, Administration and Maintenance (OAM) of Service Function Chains (SFCs) in networks is presented. Based on these requirements, an encapsulation of active OAM message in SFC and a mechanism to detect and localize defects described. Also, this document updates RFC 8300 in the definition of O (OAM) bit in the Network Service Header (NSH) and defines how the active OAM message is identified in SFC NSH.

Table of Contents

1. Introduction

[RFC7665] defines components necessary to implement a Service Function Chain (SFC). These include a classifier that performs the classification of incoming packets. A Service Function Forwarder (SFF) is responsible for forwarding traffic to one or more connected Service Functions (SFs) according to the information carried in the SFC encapsulation. SFF also handles traffic coming back from the SF

and transports the data packets to the next SFF. And the SFF serves as a termination element of the Service Function Path (SFP). SF is responsible for the specific treatment of received packets.

Resulting from that SFC is constructed by a number of these components, there are different views from different levels of the SFC. One is the SFC, an entirely abstract entity, which defines an ordered set of SFs that must be applied to packets selected due to classification. But SFC doesn't specify the exact mapping between SFFs and SFs. Thus there exists another semi-abstract entity referred to as SFP. SFP is the instantiation of the SFC in the network and provides a level of indirection between the entirely abstract SFC 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 being referred to as Rendered Service Path (RSP). The main difference between SFP and RSP is that in the former the authority to select the SFF/SF has been delegated to the network.

This document defines how active Operation, Administration and Maintenance (OAM), per [RFC7799] definition of active OAM, identified in Network Service Header (NSH) SFC. The document lists requirements to improve troubleshooting efficiency. It defines SFC Echo Request and Echo reply that enables on-demand Continuity Check, Connectivity Verification among other operations over SFC in networks addressing essential 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. Conventions

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

Unless explicitly specified in this document, active OAM in SFC and SFC OAM are being used interchangeably.

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

3. Requirements for Active OAM in SFC Network

To perform the OAM task of fault management (FM) in an SFC, that includes failure detection, defect characterization and localization, this document defines the set of requirements for active OAM mechanisms to be used on an SFC.

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

Figure 1: SFC reference model

In the example presented in Figure 1, the service SFP1 may be realized through two independent RSPs, RSP1(SF1--SF3--SF5) and RSP2(SF2--SF4--SF5). To perform end-to-end (e2e) FM SFC OAM:

REQ#1: Packets of active OAM in SFC SHOULD be fate sharing with data traffic, i.e., in-band with the monitored traffic follow the same RSP, in the forward direction from ingress toward egress endpoint(s) of the OAM test.

REQ#2: SFC OAM MUST support pro-active monitoring of any element in the SFC availability.

The egress, SFF3, in the example in Figure 1, is the entity that detects the failure of the SFC. It must be able to signal the new defect state to the ingress SFF1. 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. Definition of the misconnection defect, entry and exit criteria are outside the scope of this document.

Once the SFF1 detects the defect objective of OAM switches from failure detection to defect characterization and localization.

REQ#5: SFC OAM MUST support fault localization of Loss of Continuity check in the SFC.

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

It is practical, as presented in Figure 1, that several SFs share the same SFF. In such a case, SFP1 may be realized over two RSPs, RSP1(SF1--SF3--SF5) and RSP2(SF2--SF4--SF6).

REQ#7: SFC OAM MUST have the ability to discover and exercise all available RSPs in the transport network.

In the process of localizing the SFC failure, separating SFC OAM layers is an efficient approach. To achieve that continuity among SFFs that are part of the same SFP should be verified. Once SFFs reachability along the particular SFP has been confirmed, the task of defect localization may focus on SF reachability verification. Because reachability of SFFs has already verified, SFF local to the SF may be used as a source of the test packets.

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 interpretation of the O bit flag in the NSH header is defined in [RFC8300] as:

O bit: Setting this bit indicates an OAM packet.

This document updates the definition of O bit 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 value on the Next Protocol field MUST be set to Active SFC OAM (TBA1) according to Section 8.1. The rules of 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 OAM command or data. and the type of payload 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 contains OAM command or data;

- O bit is clear - no OAM in a Fixed-Length Context Header or Variable-Length Context Header(s) and the payload determined by the value of the Next Protocol field;

- O bit is clear and the Next Protocol value is one of identifying 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.

From the above-listed rules follows the recommendation to avoid combination of OAM in a Fixed-Length Context Header or Variable-Length Context Header(s) and in 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.

Several active OAM protocols will be needed to address all the requirements listed in Section 3. Destination UDP port number may identify protocols if IP/UDP encapsulation is used. But extra IP/UDP headers, especially in the case of IPv6, 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 bits 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 in Networks

Echo Request/Reply is a well-known active OAM mechanism that is extensively used to detect inconsistencies between a state in control and the data planes, localize defects in the data plane. The format of the Echo request/Echo reply control packet is to support ping and traceroute functionality in SFC in networks Figure 3 resembles the format of MPLS LSP Ping [RFC8029] with some exceptions.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Version Number        |         Global Flags          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Message Type  |   Reply mode  |  Return Code  | Return S.code |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Sender's Handle                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Sequence Number                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                              TLVs                             ~
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3: SFC Echo Request/Reply Format

The interpretation of the fields is as follows:

The Version reflects the current version. 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.

The Global Flags is a bit vector field.

The Message Type field reflects the type of the packet. Value TBA3 identifies Echo Request and TBA4 - Echo Reply

The Reply Mode defines the type of the return path requested by the sender of the Echo Request.

Return Codes and Subcodes can be used to inform the sender about the result of processing its request.

The Sender's Handle is filled in by the sender and returned unchanged by the Echo Reply receiver. The sender MAY use a pseudo-random number generator (PRNG) to set the value of the Sender's Handle field. The value of the Sender's Handle field SHOULD NOT be changed in the course of the test session.

The Sequence Number 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. TLVs (Type-Length-Value tuples) have the two octets long Type field, two octets long Length field is the length of the Value field in octets. 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 length of the Value field 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 9 in the corresponding Echo Reply that it generates.

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. This document defines the Authentication TLV to provide the integrity protection for SFC Echo Request/Reply. The format of the Authentication TLV is displayed in Figure 5.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Authentication|   HMAC Type   |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                            Digest                             |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5: Authentication TLV

where fields are defined as follows:

- Authentication Type - is a one-octet-long field, value TBA15 allocated by IANA Section 8.7.

- o HMAC Type - is a one-octet-long field that identifies the type of the HMAC and the length of the digest and the length of the digest according to the HTS HMAC Type sub-registry (see Section 8.9).

- o Length - two-octet-long field, set equal to the length of the HMAC field in octets.

- o Digest - is a variable-length field that carries HMAC digest of the text that includes the encompassing TLV.

This specification defines the use of HMAC-SHA-256 truncated to 128 bits ([RFC4868]) in HTS. Future specifications may define the use in HTS of more advanced cryptographic algorithms or the use of digest of a different length. HMAC is calculated as defined in [RFC2104] over text as the concatenation of the Sequence Number, Sender's Handle fields of the SFC Echo Request/Reply packet (see Figure 3) and, if present, the preceding TLVs. The digest then MUST be truncated to 128 bits and written into the Digest field. HMAC MUST be verified before using any data in the included SFC Echo Request or Reply. If HMAC verification of an SFC Echo Request fails, the system MUST stop processing it and respond with the SFC Echo Reply setting the value of the Return Code field to Authentication failed (see Section 5.1). If HMAC verification of an SFC Echo Reply fails, the system MUST stop processing it and notify the operator. Specification of the notification mechanism is outside the scope of this document.

5.3. SFC Echo Request Transmission

SFC Echo Request control packet MUST use the appropriate encapsulation of the monitored SFP. If Network Service Header (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:

- o 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.

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

- o Reply via Application Level Control Channel (TBA7) value if the SFP may have bi-directional paths.

- o 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 6: 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 transmission of Echo Reply packet. 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 7.

```
 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 7: 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 TBA16 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 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

This document defines the Authentication TLV (Section 5.2) that can be used to protect the integrity of SFC Echo Request/Reply. The integrity protection for SFC Echo Request/Reply 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 and Dirk von Hugo.

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 1: 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]. Remaining code points to be allocated according to Table 2:

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 2: 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 3: 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 4: as specified in Table 4.

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 4: SFC Echo Request/Echo Reply Message Types

IANA is requested to assign values as listed in Table 5.

Value	Description	Reference
TBA3	SFC Echo Request	This document
TBA4	SFC Echo Reply	This document

Table 5: 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 6: as specified in Table 6.

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 6: 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 7.

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
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 7: 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 8.

Value	Description	Reference
0-191	Unassigned	IETF Review
192-251	Unassigned	First Come First Served
252-254	Unassigned	Private Use
255	Reserved	

Table 8: SFC Echo Return Codes

Values defined for the Return Codes sub-registry are listed in Table 9.

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 9: 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 10:

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 10: 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
TBA15	Authentication TLV	This document

Table 11: 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	Reference
SFC OAM	TBA16	UDP	SFC OAM	Section 5.5	This document

Table 12: SFC OAM Port

8.9. HMAC Type Sub-registry

IANA is requested to create the HMAC Type sub-registry as part of the SFC OAM TLV Type registry. All code points in the range 1 through 127 in this registry shall be allocated according to the "IETF Review" procedure specified in [RFC8126]. Code points in the range 128 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 13:

Value	Description	Reference
0	Reserved	This document
1- 127	Unassigned	This document
128 - 239	Unassigned	This document
240 - 249	Experimental	This document
250 - 254	Private Use	This document
255	Reserved	This document

Table 13: HMAC Type Sub-registry

This document defines the following new values in the HMAC Type sub-registry:

Value	Description	Reference
1	HMAC-SHA-256 16 octets long	This document

Table 14: HMAC Types

9. References

9.1. Normative References

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <https://www.rfc-editor.org/info/rfc2104>.

[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

[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>.

[RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, DOI 10.17487/RFC4868, May 2007, <https://www.rfc-editor.org/info/rfc4868>.

[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

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