Internet Engineering Task Force   S. Aldrin
Internet-Draft   Google
Intended status: Informational   C. Pignataro, Ed.
Expires: December 29, 2019   N. Kumar, Ed.
                                                              Cisco
                                                        R. Krishnan
                                                             VMware
                                                        A. Ghanwani
                                                               Dell
                                                      June 27, 2019

Service Function Chaining (SFC)
Operations, Administration and Maintenance (OAM) Framework
draft-ietf-sfc-oam-framework-09

Abstract

   This document provides a reference framework for Operations,
   Administration and Maintenance (OAM) for Service Function Chaining
   (SFC).

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 RFC
   2119 [RFC2119] RFC 8174 [RFC8174] when and only when, they appear in
   all capitals, as shown here.

Table of Contents

1. Introduction

   Service Function Chaining (SFC) enables the creation of composite
   services that consist of an ordered set of Service Functions (SF)
   that are to be applied to packets and/or frames selected as a result
   of classification [RFC7665]. SFC is a concept that provides for more
   than just the application of an ordered set of SFs to selected
   traffic; rather, it describes a method for deploying SFs in a way
   that enables dynamic ordering and topological independence of those
   SFs as well as the exchange of metadata between participating
   entities. The foundations of SFC are described in the following
   documents:

   o SFC Problem Statement [RFC7498]

   o SFC Architecture [RFC7665]

   The reader is assumed to be familiar with the material in these
   documents.

   This document provides a reference framework for Operations,
   Administration and Maintenance (OAM, [RFC6291]) of SFC.
   Specifically, this document provides:

   o In Section 2, an SFC layering model;

   o In Section 3, aspects monitored by SFC OAM;

   o In Section 4, functional requirements for SFC OAM;

   o In Section 5, a gap analysis for SFC OAM.

   SFC OAM solution documents should refer to this document to indicate
   the SFC OAM component and the functionality they target.

   OAM controllers are assumed to be within the same administrative
   domain as the target SFC enabled domain.

1.1. Document Scope

The focus of this document is to provide an architectural framework
for SFC OAM, particularly focused on the aspect of the Operations
component within OAM. Actual solutions and mechanisms are outside
the scope of this document.

1.2. Acronyms and Terminology

1.2.1. Acronyms

SFC: Service Function Chain

SFF: Service Function Forwarder

SF: Service Function

SFP: Service Function Path

RSP: Rendered Service Path

NSH: Network Service Header

VM: Virtual Machines

OAM: Operations, Administration and Maintenance

IPPM: IP Performance Metrics

BFD: Bidirectional Forwarding Detection

NVo3: Network Virtualization over Layer3

SNMP: Simple Network Management Protocol

NETCONF: Network Configuration Protocol

1.2.2. Terminology

This document uses the terminologies defined in [RFC7665], [RFC8300],
and so the readers are expected to be familiar with the same.

2. SFC Layering Model

Multiple layers come into play for implementing the SFC. These
include the service layer and the underlying layers (Network Layer,
Link Layer, etc.).

o The service layer, which consists of SFC data plane elements that
   includes classifiers, Service Functions (SF), Service Function
   Forwarders (SFF), and SFC Proxies. This layer uses the overlay
   network for ensuring connectivity between SFC data plane elements.

o The overlay network layer, which leverages various overlay network
   technologies interconnecting SFC data plane elements and allows
   establishing Service Function Paths (SFPs). This layer is mostly
   transparent to the SFC data plane elements.

o The underlay network layer, which is dictated by the networking
   technology deployed within a network (e.g., IP, MPLS)

o The link layer, which is dependent upon the physical technology
   used. Ethernet is a popular choice for this layer, but other
   alternatives are deployed (e.g. POS, DWDM). The same or distinct
   link layer technologies may be used in each leg shown in Figure 1.

```
   o----------------------Service Layer----------------------o

+------+    +---+    +---+    +---+    +---+    +---+    +---+    +---+
|Classi|---|SF1|---|SF2|---|SF3|---|SF4|---|SF5|---|SF6|---|SF7|
|fier  |    +---+    +---+    +---+    +---+    +---+    +---+    +---+
+------+
              <------VM1------>        <--VM2-->        <--VM3-->

   ^----------------^-------------------^---------------^  Overlay N/W

   o----------------o-------------------o---------------o  Underlay N/W

   o--------o--------o--------o--------o--------o--------o  Link
```
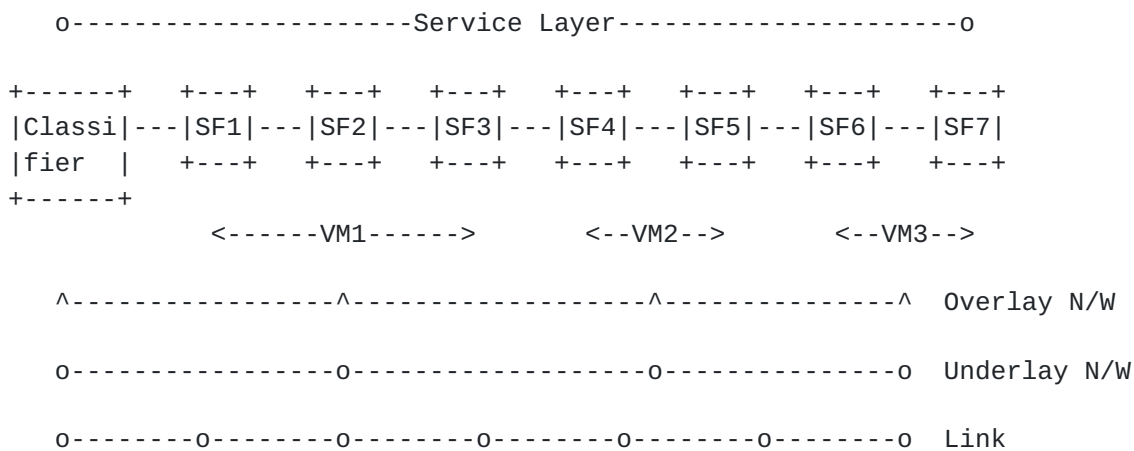
                 Figure 1: SFC Layering Example

In Figure 1, the service layer element such as classifier and SF are
depicted as virtual machines that are interconnected using an overlay
network. The underlay network may comprise of multiple intermediate
nodes but not shown in the figure that provides underlay connectivity
between the service layer elements.

While Figure 1 depicts a sample example where SFs are enabled as
virtual entities, the SFC architecture does not make any assumptions
on how the SFC data plane elements are deployed. The SFC
architecture is flexible and accommodates physical or virtual entity
deployment. SFC OAM accounts for this flexibility and accordingly it
is applicable whether SFC data plane elements are deployed directly
on physical hardware, as one or more Virtual Machines, or any
combination thereof.

3. SFC OAM Components

The SFC operates at the service layer. For the purpose of defining
the OAM framework, the service layer is broken up into three distinct
components:

1. SF component: OAM functions applicable at this component includes
    testing the SFs from any SFC-aware network devices (e.g.,
    classifiers, controllers, other service nodes). Testing an SF
    may not be restricted to connectivity to the SF, but also whether
    the SF is providing its intended service. Refer to Section 3.1.1
    for a more detailed discussion.

2. SFC component: OAM functions applicable at this component
    includes (but are not limited to) testing the service function
    chains and the SFPs, validaion of the correlation between an SFC
    and the actual forwarding path followed by a packet matching that
    SFC, i.e. the Rendered Service Path (RSP). Some of the hops of
    an SFC may not be visible when Hierarchical Service Function
    Chaining (hSFC) [RFC8459] is in use. In such schemes, it is the
    responsibility of the Internal Boundary Node (IBN) to glue the
    connectivity between different levels for end-to-end OAM
    functionality.

3. Classifier component: OAM functions applicable at this component
    includes testing the validity of the classification rules and
    detecting any incoherence among the rules installed in different
    classifiers.

Figure 2 illustrates an example where OAM for the three defined
components are used within the SFC environment.

```
 +-Classifier  +-Service Function Chain OAM
 | OAM         |
 |             |     _____
 |             \       /\          Service Function Chain         \
 |              \     /  \      +---+       +---+      +-----+  +---+ \
 |               \   /    \     |SF1|       |SF2|      |Proxy|--|SF3|   \
 |     +------+   \/       \    +---+       +---+      +-----+  +---+    \
 +----> |      |....(+->    )     |           |          |                )
        |Classi|    \      /   +-----+     +-----+     +-----+           /
        |fier  |     \    /    | SFF1|----| SFF2|----| SFF3|          /
        |      |      \  /     +--^--+     +-----+     +-----+         /
        +----|-+       \/_____|_____/
             |             |
          +-------SF_OAM-------+
                             +---+    +---+
                    +SF_OAM>|SF3|    |SF5|
                    |         +-^-+    +-^-+
          +------|---+     |        |
          |Controller|    +-SF_OAM+
          +----------+
                   Service Function OAM (SF_OAM)
```
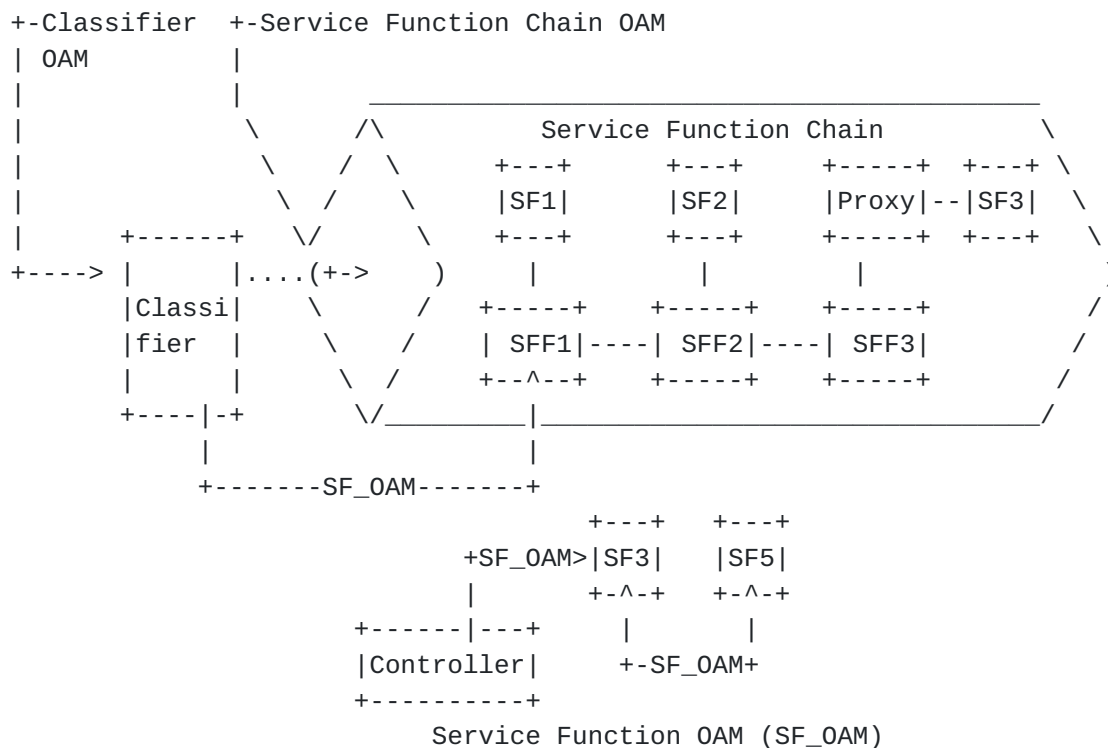
                    Figure 2: SFC OAM Components

   It is expected that multiple SFC OAM solutions will be defined, each
   targeting one specific component of the service layer. However, it
   is critical that SFC OAM solutions together provide the coverage of
   all three SFC OAM components: the SF component, the SFC component,
   and the classifier component.

3.1. The SF Component

3.1.1. SF Availability

   One SFC OAM requirement for the SF component is to allow an SFC-aware
   network device to check the availability of a specific SF (instance),
   located on the same or different network device(s). The SF
   availability may be performed to check the availability of any
   instance of a specific SFn or it can be a specific instance of a SF.
   SF availability is an aspect that raises an interesting question --
   How to determine that a service function is available?. On one end
   of the spectrum, one might argue that an SF is sufficiently available
   if the service node (physical or virtual) hosting the SF is available
   and is functional. On the other end of the spectrum, one might argue
   that the SF's availability can only be concluded if the packet, after
   passing through the SF, was examined and it was verified that the
   packet did indeed get the got expected service.

The former approach will likely not provide sufficient confidence to the actual SF availability, i.e. a service node and a SF are two different entities. The latter approach is capable of providing an extensive verification, but comes at a cost. Some SFs make direct modifications to packets, while others do not. Additionally, the purpose of some SFs may be to, conditionally, drop packets intentionally. In such cases, it is normal behavior that certain packets will not be egressing out from the service function. The OAM mechanism needs to take into account such SF specifics when assessing SF availability. Note that there are many flavors of SFs available, and many more that are likely be introduced in future. Even a given SF may introduce a new functionality (e.g., a new signature in a firewall). The cost of this approach is that the OAM mechanism for some SF will need to be continuously modified in order to "keep up" with new functionality being introduced: lack of extendibility.

This framework document provides a RECOMMENDED framework where a generalized approach is taken to verify that a SF is sufficiently available (i.e., an adequate granularity to provide a basic SF service). More specifics on the mechanism to characterize SF-specific OAM to validate the service offering are outside the scope of this document. Those fine-grained mechanisms are implementation- and deployment-specific.

3.1.2. SF Performance Measurement

The second SFC OAM requirement for the SF component is to allow an SFC-aware network device to check the performance metrics such as loss and delay induced by a specific SF for processing legitimate traffic. The performance can be a passive measurement by using live traffic or can be active measurement by using synthetic probe packets.

On the one hand, the performance of any specific SF can be quantified by measuring the loss and delay metrics of the traffic from SFF to the respective SF, while on the other hand, the performance can be measured by leveraging the loss and delay metrics from the respective SFs. The latter requires SF involvement to perform the measurement while the former does not.

3.2. The SFC Component

3.2.1. SFC Availability

An SFC could be comprised of varying SFs and so the OAM layer is required to perform validation and verification of SFs within an SFP, in addition to connectivity verification and fault isolation.

In order to perform service connectivity verification of an SFC/SFP,
the OAM functions could be initiated from any SFC-aware network
devices of an SFC-enabled domain for end-to-end paths, or partial
paths terminating on a specific SF, within the SFC/SFP. The goal of
this OAM function is to ensure the SFs chained together have
connectivity as was intended at the time when the SFC was
established. The necessary return codes should be defined for
sending back in the response to the OAM packet, in order to complete
the verification.

When ECMP is in use at the service layer for any given SFC, there
MUST be the ability to discover and traverse all available paths.

A detailed explanation of the mechanism is outside the scope of this
document and is expected to be included in the actual solution
document.

3.2.2. SFC Performance Measurement

Any SFC-aware network device SHOULD have the ability to make
performance measurements over the entire SFC (i.e., end-to-end) or to
a specific segment of SFs within the SFC.

3.3. The Classifier Component

A classifier maintains the classification rules that map a flow to a
specific SFC. It is vital that the classifier is correctly
configured with updated classification rules and is functioning as
expected. The SFC OAM must be able to validate the classification
rules by assessing whether a flow is appropriately mapped to the
relevant SFC. Sample OAM packets can be presented to the classifiers
to assess the behavior with regard to a given classification entry.

4. SFC OAM Functions

Section 3 described SFC OAM operations that are required on each SFC
component. This section explores SFC OAM functions that are
applicable for more than one SFC components.

The various SFC OAM requirements listed in Section 3 highlighted the
need for various OAM functions at different layers. As listed in
Section 5.1, various OAM functions are in existence that are defined
to perform OAM functionality at different layers. In order to apply
such OAM functions at the service layer, they need to be enhanced to
operate a single SF/SFF to multiple SFs/SFFs in an SFC and also in
multiple SFCs.

4.1. Connectivity Functions

   Connectivity is mainly an on-demand function to verify that the
   connectivity exists between certain network elements and that the SFs
   are available. For example, LSP Ping [RFC8029] is a common tool used
   to perform this function for an MPLS underlay network. OAM messages
   SHOULD be encapsulated with necessary SFC header and with OAM
   markings when testing the SFC component. OAM messages MAY be
   encapsulated with the necessary SFC header and with OAM markings when
   testing the SF component. Some of the OAM functions performed by
   connectivity functions are as follows:

   o Verify the Path MTU from a source to the destination SF or through
      the SFC. This requires the ability for the OAM packet to be of
      variable length packet size.

   o Verify any packet re-ordering and corruption.

   o Verify the policy of an SFC or SF.

   o Verification and validation of forwarding paths.

   o Proactively test alternate or protected paths to ensure
      reliability of network configurations.

4.2. Continuity Functions

   Continuity is a model where OAM messages are sent periodically to
   validate or verify the reachability to a given SF within an SFC or
   for the entire SFC. This allows a monitoring network device (such as
   the classifier or controller) to quickly detect failures such as link
   failures, network element failures, SF outages, or SFC outages. BFD
   [RFC5880] is one such function which helps in detecting failures
   quickly. OAM functions supported by continuity function are as
   follows:

   o Ability to provision continuity check to a given SF within an SFC
      or for the entire SFC.

   o Notifying the detected failures to other OAM functions or
      applications to take appropriate action.

4.3. Trace Functions

   Tracing is an OAM function that allows the operation to trigger an
   action (e.g. response generation) from every transit device (e.g.
   SFF, SF, SFC Proxy) on the tested layer. This function is typically
   useful for gathering information from every transit devices or for

isolating the failure point to a specific SF within an SFC or for an
entire SFC. Some of the OAM functions supported by trace functions
are:

o Ability to trigger action from every transit device at the SFC
   layer, using TTL or other means.

o Ability to trigger every transit device at the SFC layer to
   generate a response with OAM code(s), using TTL or other means.

o Ability to discover and traverse ECMP paths within an SFC.

o Ability to skip SFs that do not support OAM while tracing SFs in
   an SFC.

4.4. Performance Management Functions

Performance management functions involve measuring of packet loss,
delay, delay variance, etc. These performance metrics may be
measured pro-actively or on-demand.

SFC OAM should provide the ability to measure packet loss for an SFC.
On-demand measurement can be used to estimate packet loss using
statistical methods. Measuring the loss of OAM packets, an
approximation of packet loss for a given SFC can be derived.

Delay within an SFC could be measured based on the time it takes for
a packet to traverse the SFC from the ingress SFC node to the egress
SFF. As SFCs are unidirectional in nature, measurement of one-way
delay [RFC7679] is important. In order to measure one-way delay,
time synchronization MUST be supported by means such as NTP, PTP,
GPS, etc.

One-way delay variation [RFC3393] could also be calculated by sending
OAM packets and measuring the jitter between the packets passing
through an SFC.

Some of the OAM functions supported by the performance measurement
functions are:

o Ability to measure the packet processing delay induced by a single
   SF or the one-way delay to traverse an SFP bound to a given SFC.

o Ability to measure the packet loss [RFC7680] within an SF or an
   SFP bound to a given SFC.

5. Gap Analysis

   This section identifies various OAM functions available at different
   levels introduced in Section 2. It also identifies various gaps that
   exist within the current toolset for performing OAM functions
   required for SFC.

5.1. Existing OAM Functions

   There are various OAM tool sets available to perform OAM functions
   within various layers. These OAM functions may be used to validate
   some of the underlay and overlay networks. Tools like ping and trace
   are in existence to perform connectivity check and tracing of
   intermediate hops in a network. These tools support different
   network types like IP, MPLS, TRILL, etc. There is also an effort to
   extend the tool set to provide connectivity and continuity checks
   within overlay networks. BFD is another tool which helps in
   detecting data forwarding failures. The orchestration tool may be
   used for network and service orchestration function. Tables 3 and 4
   are not exhaustive.

                    Table 3: OAM Tool GAP Analysis

Layer	Connectivity	Continuity	Trace	Performance
Underlay N/w	Ping	E-OAM, BFD	Trace	IPPM, MPLS_PM
Overlay N/w	Ping	BFD, NVo3 OAM	Trace	IPPM
SF	None	+ None	+ None	+ None
SFC	None	+ None	+ None	+ None

Table 4: OAM Tool GAP Analysis (contd.)

Layer	Configuration	Orchestration	Topology	Notification
Underlay N/w	CLI, NETCONF	CLI, NETCONF	SNMP	SNMP, Syslog, NETCONF
Overlay N/w	CLI, NETCONF	CLI, NETCONF	SNMP	SNMP, Syslog NETCONF
SF	CLI, NETCONF	+ CLI, NETCONF	None	None
SFC	CLI, NETCONF	+ CLI, NETCONF	None	None

5.2. Missing OAM Functions

   As shown in Table 3, there are no standards-based tools available for
   the verification of SFs and SFCs.

5.3. Required OAM Functions

   Primary OAM functions exist for underlying layers. Tools like ping,
   trace, BFD, etc. exist in order to perform these OAM functions.

   Configuration, orchestration and manageability of SF and SFC could be
   performed using CLI, NETCONF, etc.

   As depicted in Tables 3 and 4, information and data models are needed
   for configuration, manageability and orchestration for SFC. With
   virtualized SF and SFC, manageability needs to be done
   programmatically.

6. Candidate SFC OAM Tools

   This section describes the operational aspects of SFC OAM at the
   service layer to perform the SFC OAM function defined in Section 4
   and analyzes the applicability of various existing OAM toolsets in
   the service layer.

6.1. SFC OAM Packet Marker

   The SFC OAM function described in Section 4 performed at the service
   layer or overlay network layer must mark the packet as an OAM packet
   so that relevant nodes can differentiate an OAM packet from data
   packets. The base header defined in Section 2.2 of [RFC8300] assigns
   a bit to indicate OAM packets. When NSH encapsulation is used at the

service layer, the O bit must be set to differentiate the OAM packet.
Any other overlay encapsulations used in future must have a way to
mark the packet as OAM packet.

6.2. OAM Packet Processing and Forwarding Semantic

Upon receiving an OAM packet, SFC-aware SFs may choose to discard the
packet if it does not support OAM functionality or if the local
policy prevents them from processing the OAM packet. When an SF
supports OAM functionality, it is desirable to process the packet and
provide an appropriate response to allow end-to-end verification. To
limit performance impact due to OAM, SFC-aware SFs should rate limit
the number of OAM packets processed.

An SFF may choose not to forward the OAM packet to an SF if the SF
does not support OAM or if the policy does not allow to forward OAM
packet to an SF. The SFF may choose to skip the SF, modify the
header and forward to next SFC node in the chain. It should be noted
that skipping an SF might have implication on some OAM functions
(e.g. the delay measurement may not be accurate). The method by
which an SFF detects if the connected SF supports or is allowed to
process OAM packets is outside the scope of this document. It could
be a configuration parameter instructed by the controller or it can
be done by dynamic negotiation between the SF and SFF.

If the SFF receiving the OAM packet bound to a given SFC is the last
SFF in the chain, it must send a relevant response to the initiator
of the OAM packet. Depending on the type of OAM solution and tool
set used, the response could be a simple response (such as ICMP
reply) or could include additional data from the received OAM packet
(like statistical data consolidated along the path). The details are
expected to be covered in the solution documents.

Any SFC-aware node that initiates an OAM packet must set the OAM
marker in the overlay encapsulation.

6.3. OAM Function Types

As described in Section 4, there are different OAM functions that may
require different OAM solutions. While the presence of the OAM
marker in the overlay header (e.g., O bit in the NSH header)
indicates it as OAM packet, it is not sufficient to indicate what OAM
function the packet is intended for. The Next Protocol field in NSH
header may be used to indicate what OAM function is intended to or
what toolset is used.

6.4. OAM Toolset Applicability

   As described in Section 5.1, there are different tool sets available
   to perform OAM functions at different layers. This section describes
   the applicability of some of the available toolsets in the service
   layer.

6.4.1. ICMP

   [RFC0792] and [RFC4443] describes the use of ICMP in IPv4 and IPv6
   network respectively. It explains how ICMP messages can be used to
   test the network reachability between different end points and
   perform basic network diagnostics.

   ICMP could be leveraged for connectivity function (defined in
   Section 4.1) to verify the availability of SF or SFC. The Initiator
   can generate an ICMP echo request message and control the service
   layer encapsulation header to get the response from relevant node.
   For example, a classifier initiating OAM can generate ICMP echo
   request message, can set the TTL field in NSH header to 255 to get
   the response from last SFF and thereby test the SFC availability.
   Alternately, the initiator can set the TTL to some other value to get
   the response from a specific SFs and there by test partial SFC
   availability. Alternately, the initiator could send OAM packets with
   sequentially incrementing the TTL in the NSH to trace the SFP.

   It could be observed that ICMP at its current stage may not be able
   to perform all required SFC OAM functions, but as explained above, it
   can be used for basic OAM functions.

6.4.2. BFD/Seamless-BFD

   [RFC5880] defines Bidirectional Forwarding Detection (BFD) mechanism
   for fast failure detection. [RFC5881] and [RFC5884] defines the
   applicability of BFD in IPv4, IPv6 and MPLS networks. [RFC7880]
   defines Seamless BFD (S-BFD), a simplified mechanism of using BFD.
   [RFC7881] explains its applicability in IPv4, IPv6 and MPLS network.

   BFD or S-BFD could be leveraged to perform SF or SFC availability.
   An initiator could generate a BFD control packet and set the "Your
   Discriminator" value as last SFF in the control packet. Upon
   receiving the control packet, the last SFF in the SFC will reply back
   with relevant DIAG code. The TTL field in the NSH header could be
   used to perform partial SFC availability. For example, the initiator
   can set the "Your Discriminator" value to the SF that is intended to
   be tested and set the TTL field in NSH header in a way that it expire
   at the relevant SF. How the initiator gets the Discriminator value
   of the SF is outside the scope of this document.

6.4.3. In-Situ OAM

[I-D.ietf-sfc-proof-of-transit] defines a mechanism to perform proof
of transit to securely verify if a packet traversed the relevant SFP
or SFC. While the mechanism is defined inband (i.e., it will be
included in data packets), it may be used to perform various SFC OAM
functions as well.

In-Situ OAM could be used with O bit set to perform SF availability
and SFC availability or performance measurement.

6.4.4. SFC Traceroute

[I-D.penno-sfc-trace] defines a protocol that checks for path
liveliness and traces the service hops in any SFP. Section 3 of
[I-D.penno-sfc-trace] defines the SFC trace packet format while
Sections 4 and 5 of [I-D.penno-sfc-trace] defines the behavior of SF
and SFF respectively.

An initiator can control the Service Index Limit (SIL) in SFC trace
packet to perform SF and SFC availability test.

7. Security Considerations

Any security consideration defined in [RFC7665] and [RFC8300] are
applicable for this document.

The OAM information from service layer at different components may
collectively or independently reveal sensitive information. The
information may reveal the type of service functions hosted in the
network, the classification rules and the associated service chains,
specific service function paths etc. The sensitivity of the
information from SFC layer raises a need for careful security
considerations

The mapping and the rules information at the classifier component may
reveal the traffic rules and the traffic mapped to the SFC. The SFC
information collected at an SFC component may reveal the SF
associated within each chain and this information together with
classifier rules may be used to manipulate the header of synthetic
attack packets that may be used to bypass the SFC and trigger any
internal attacks.

The SF information at the SF component may be used by a malicious
user to trigger Denial of Service (DoS) attack by overloading any
specific SF using rogue OAM traffic.

To address the above concerns, SFC and SF OAM may provide mechanism
for:

o Misuse of the OAM channel for denial-of-services,

o Leakage of OAM packets across SFC instances, and

o Leakage of SFC information beyond the SFC domain.

The documents proposing the OAM solution for SF component should
consider rate-limiting the OAM probes at a frequency guided by the
implementation choice. Rate-limiting may be applied at the SFF or
the SF . The OAM initiator may not receive a response for the probes
that are rate-limited resulting in false negatives and the
implementation should be aware of this.

The documents proposing the OAM solution for any service layer
components should consider some form of message filtering to prevent
leaking any internal service layer information outside the
administrative domain.

8. IANA Considerations

No action is required by IANA for this document.

9. Acknowledgements

We would like to thank Mohamed Boucadair, Adrian Farrel, and Greg
Mirsky for their review and comments.

10. Contributing Authors

Nobo Akiya
Ericsson
Email: nobo.akiya.dev@gmail.com

11. References

11.1. 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>.

   [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>.

   [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>.

   [RFC8459] Dolson, D., Homma, S., Lopez, D., and M. Boucadair,
              "Hierarchical Service Function Chaining (hSFC)", RFC 8459,
              DOI 10.17487/RFC8459, September 2018,
              <https://www.rfc-editor.org/info/rfc8459>.

11.2. Informative References

   [I-D.ietf-sfc-proof-of-transit]
              Brockners, F., Bhandari, S., Dara, S., Pignataro, C.,
              Leddy, J., Youell, S., Mozes, D., Mizrahi, T., Aguado, A.,
              and D. Lopez, "Proof of Transit", draft-ietf-sfc-proof-of-
              transit-02 (work in progress), March 2019.

   [I-D.penno-sfc-trace]
              Penno, R., Quinn, P., Pignataro, C., and D. Zhou,
              "Services Function Chaining Traceroute", draft-penno-sfc-
              trace-03 (work in progress), September 2015.

   [RFC0792] Postel, J., "Internet Control Message Protocol", STD 5,
              RFC 792, DOI 10.17487/RFC0792, September 1981,
              <https://www.rfc-editor.org/info/rfc792>.

   [RFC3393] Demichelis, C. and P. Chimento, "IP Packet Delay Variation
              Metric for IP Performance Metrics (IPPM)", RFC 3393,
              DOI 10.17487/RFC3393, November 2002,
              <https://www.rfc-editor.org/info/rfc3393>.

   [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>.

   [RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection
              (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010,
              <https://www.rfc-editor.org/info/rfc5880>.

   [RFC5881] Katz, D. and D. Ward, "Bidirectional Forwarding Detection
              (BFD) for IPv4 and IPv6 (Single Hop)", RFC 5881,
              DOI 10.17487/RFC5881, June 2010,
              <https://www.rfc-editor.org/info/rfc5881>.

   [RFC5884] Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow,
              "Bidirectional Forwarding Detection (BFD) for MPLS Label
              Switched Paths (LSPs)", RFC 5884, DOI 10.17487/RFC5884,
              June 2010, <https://www.rfc-editor.org/info/rfc5884>.

   [RFC6291] Andersson, L., van Helvoort, H., Bonica, R., Romascanu,
              D., and S. Mansfield, "Guidelines for the Use of the "OAM"
              Acronym in the IETF", BCP 161, RFC 6291,
              DOI 10.17487/RFC6291, June 2011,
              <https://www.rfc-editor.org/info/rfc6291>.

   [RFC7498] Quinn, P., Ed. and T. Nadeau, Ed., "Problem Statement for
              Service Function Chaining", RFC 7498,
              DOI 10.17487/RFC7498, April 2015,
              <https://www.rfc-editor.org/info/rfc7498>.

   [RFC7679] Almes, G., Kalidindi, S., Zekauskas, M., and A. Morton,
              Ed., "A One-Way Delay Metric for IP Performance Metrics
              (IPPM)", STD 81, RFC 7679, DOI 10.17487/RFC7679, January
              2016, <https://www.rfc-editor.org/info/rfc7679>.

   [RFC7680] Almes, G., Kalidindi, S., Zekauskas, M., and A. Morton,
              Ed., "A One-Way Loss Metric for IP Performance Metrics
              (IPPM)", STD 82, RFC 7680, DOI 10.17487/RFC7680, January
              2016, <https://www.rfc-editor.org/info/rfc7680>.

   [RFC7880] Pignataro, C., Ward, D., Akiya, N., Bhatia, M., and S.
              Pallagatti, "Seamless Bidirectional Forwarding Detection
              (S-BFD)", RFC 7880, DOI 10.17487/RFC7880, July 2016,
              <https://www.rfc-editor.org/info/rfc7880>.

   [RFC7881] Pignataro, C., Ward, D., and N. Akiya, "Seamless
              Bidirectional Forwarding Detection (S-BFD) for IPv4, IPv6,
              and MPLS", RFC 7881, DOI 10.17487/RFC7881, July 2016,
              <https://www.rfc-editor.org/info/rfc7881>.

   [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>.

Authors' Addresses

   Sam K. Aldrin
   Google

   Email: aldrin.ietf@gmail.com

   Carlos Pignataro (editor)
   Cisco Systems, Inc.

   Email: cpignata@cisco.com

   Nagendra Kumar (editor)
   Cisco Systems, Inc.

   Email: naikumar@cisco.com

   Ram Krishnan
   VMware

   Email: ramkri123@gmail.com

   Anoop Ghanwani
   Dell

   Email: anoop@alumni.duke.edu