                      Service Function Chaining
          Operations, Administration and Maintenance Framework
                  draft-aldrin-sfc-oam-framework-00

Abstract

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

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 must be applied to packets and/or frames selected as a result of
   classification. Service Function Chaining 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. Foundations of the SFC are described in below documents:

   o [I-D.ietf-sfc-problem-statement]: SFC problem statement.

   o Various individual drafts

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

   o In Section 2, an SFC layering model;

   o In Section 3, involved components within the SFC layer;

   o In Section 4, functional requirements for the SFC OAM;

   o In Section 5, an OAM gap analysis.

1.1. Document Scope

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

2. SFC Layering Model

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

   o The service layer, refer to as the "Service Layer" in Figure 1,
      consists of classifiers and service functions, and uses the
      overlay network reach from a classifier to service functions and
      service functions to service functions.

   o The network overlay transport layer, refer to as the "Network",
      "transport" and layers below in Figure 1, extends in between
      various service functions and is mostly transparent to the service
      functions. It leverages various overlay network technologies
      interconnecting service functions and allows establishing of
      service function paths.

   o The link layer, refer to as the "Link" in Figure 1, is dependent
      upon the physical technology used. Ethernet is a popular choice
      for this layer, but other alternatives are deployed (e.g. POS,
      DWDM etc...).

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

   +------+   +---+   +---+   +---+   +---+   +---+   +---+   +---+
   |Classi|---|SF1|---|SF2|---|SF3|---|SF4|---|SF5|---|SF6|---|SF7|
   |fier  |   +---+   +---+   +---+   +---+   +---+   +---+   +---+
   +------+
              o-N/W Elem 1----o    o-N/w Elem 2-o   o-N/W Elem 3-o

   o----------------o-------------------o--------------o  Network

   o----------------o-------------------------------o  Transport

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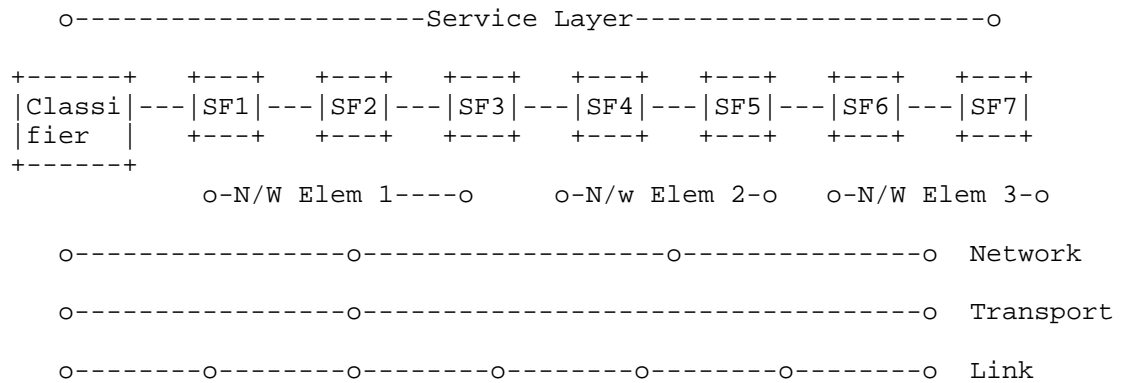
                  Figure 1: SFC Layering Example

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. Service function component: A function providing a specific
       service. OAM solutions for this component are to test the
       service functions from any SFC aware network devices (i.e.
       classifiers, controllers, other service nodes).

   2. Service function chain component: An ordered set of service
       functions. OAM solution for this component are to test the
       service function chains and the service function paths.

   3. Classifier component: A policy that describes the mapping from
       flows to service function chains. OAM solutions for this
       component are to test the validity of the classifiers.

   Below figure 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          \
|              \  /\                                                 \
|     +------+  \/  \ +---+    +---+    +---+    +---+    +---+ \
+----> |Classi|...(+-> ) |SF1|---|SF2|---|SF4|---|SF6|---|SF7|  )
       |fier  |   \  /  +-^-+    +---+    +-|-+    +-^-+    +---+ /
       +----|-+    \/_____|_____|_____|_____ /
            |          |               +-SF_OAM+
       +----SF_OAM----+         +---+    +---+
                      +SF_OAM>|SF3|    |SF5|
                      |       +-^-+    +-^-+
            +------|---+       |        |
            |Controller|     +-SF_OAM+
            +----------+
              Service Function OAM (SF_OAM)
```
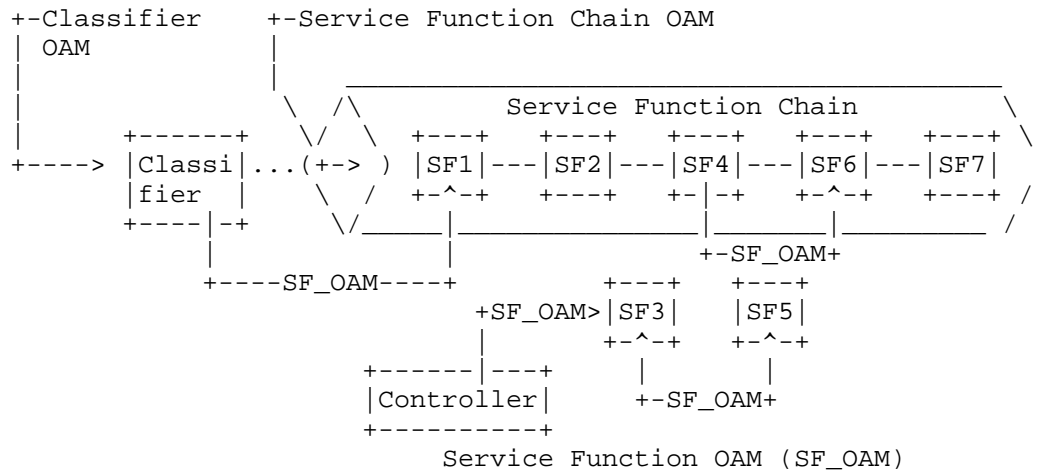
Figure 2: SFC OAM for Three Components

It is expected that multiple SFC OAM solutions will be defined, many
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 service function component, the
service function chain component and the classifier component.

3.1. Service Function Component

3.1.1. Service Function Availability

   One SFC OAM requirement for the service function component is to
   allow an SFC aware network device to check the availability to a
   specific service function, located on the same or different network
   devices. Service function availability is an aspect which raises an
   interesting question. How does one determine that a service function
   is available? On one end of the spectrum, one might argue that a
   service function is sufficiently available if the service node
   (physical or virtual) hosting the service function is available and
   is functional. On the other end of the spectrum, one might argue
   that the service function availability can only be concluded if the
   packet, after passing through the service function, was examined and
   verified that the packet got expected service applied.

   The former approach will likely not provide sufficient confidence to
   the actual service function availability, i.e. a service node and a
   service function are two different entities. The latter approach is
   capable of providing an extensive verification, but comes with a
   cost. Some service functions make direct modifications to packets,
   while other service functions do not make any modifications to

packets. Additionally, purpose of some service functions is to,
conditionally, drop packets intentionally. In such case, packets
will not be coming out from the service function. The fact is that
there are many flavors of service functions available, and many more
flavors of service functions will likely be introduced in future.
Even a given service function may introduce a new functionality
within a service function (ex: a new signature in a firewall). The
cost of this approach is that verifier functions will need to be
continuously modified to "keep up" with new services coming out: lack
of extendibility.

This framework document provides a RECOMMENDED architectural model
where generalized approach is taken to verify that a service function
is sufficiently available. TBD - details will be provided in a later
revision.

3.1.2. Service Function Performance Measurement

Second SFC OAM requirement for the service function component is to
allow an SFC aware network device to check the loss and delay of a
specific service function, located on the same or different network
devices. TBD - details will be provided in a later revision.

3.2. Service Function Chain Component

3.2.1. Service Function Chain Availability

Verifying an SFC is a complicated process as the SFC could be
comprised of varying SF's. Thus, SFC requires the OAM layer to
perform validation and verification of SF's within an SFC Path, as
well as connectivity and fault isolation.

In order to perform service connectivity verification of an SFC, the
OAM could be initiated from any SFC aware network devices for end-to-
end paths or partial path terminating on a specific SF within the
SFC. This OAM function is to ensure the SF's chained together has
connectivity as it is intended to when SFC was established. Necessary
return code should be defined to be sent back in the response to OAM
packet, in order to qualify the verification.

When ECMP exists at the service layer on a given SFC, there must be
an ability to discover and traverse all available paths.

TBD - further details will be provided in a later revision.

3.2.2. Service Function Chain Performance Measurement

The ingress of the service function chain or an SFC aware network

device must have an ability to perform loss and delay measurements
over the service function chain as a unit (i.e. end-to-end) or to a
specific service function through the SFC.

3.3. Classifier Component

A classifier defines a flow and maps incoming traffic to a specific
SFC, and it is vital that the classifier is correctly defined and
functioning. The SFC OAM must be able to test the definition of
flows and the mapping functionality to expected SFCs.

4. SFC OAM Functions

Section 3 described SFC OAM operations required on each SFC
component. This section explores the same from the OAM functionality
point of view, which many will be applicable to multiple SFC
components.

Various SFC OAM requirements provides the need for various OAM
functions at different layers. Many of the OAM functions at
different layers are already defined and in existence. In order to
support SFC and SF's, these functions have to be enhanced to operate
a single SF to multiple SF's in an SFC and also multiple SFC's.

4.1. Connectivity Functions

Connectivity is mainly an on-demand function to verify that the
connectivity exists between network elements and the availability
exists to service functions. Ping is a common tool used to perform
this function. OAM messages should be encapsulated with necessary
SFC header and with OAM markings when testing the service function
chain component. OAM messages MAY be encapsulated with necessary SFC
header and with OAM markings when testing the service function
component. Some of the OAM functions performed by connectivity
functions are as follows:

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

o Verify the packet re-ordering and corruption.

o Verify the policy of an SFC or SF using OAM packet.

o Verification and validating 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 or through a given
   SFC. This allows monitor network device to quickly detect failures
   like link failures, network failures, service function outages or
   service function chain outages. BFD is one such function which helps
   in detecting failures quickly. OAM functions supported by continuity
   check are as follows:

   o Ability to provision continuity check to a given SF or through a
      given SFC.

   o Notifying the failure upon failure detection for other OAM
      functions to take appropriate action.

4.3. Trace Functions

   Tracing is an important OAM function that allows the operation to
   trigger an action (ex: response generation) from every transit device
   on the tested layer. This function is typically useful to gather
   information from every transit devices or to isolate the failure
   point towards an SF or through an SFC. Some of the OAM functions
   supported by trace functions are:

   o Ability to trigger action from every transit device on the tested
      layer towards an SF or through an SFC, using TTL or other means.

   o Ability to trigger every transit device to generate response with
      OAM code(s) on the tested layer towards an SF or through an SFC,
      using TTL or other means.

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

   o Ability to skip un-supported SF's while tracing SF's in an SFC.

4.4. Performance Measurement Function

   Performance management functions involve measuring of packet loss,
   delay, delay variance, etc. These measurements could be measured
   pro-actively and on-demand.

   SFC OAM framework should provide the ability to perform packet loss
   for an SFC. In an SFC, there are various SF's chained together.
   Measuring packet loss is very important function. Using on-demand
   function, the packet loss could be measured using statistical means.
   Using OAM packets, the approximation of packet loss for a given SFC
   could be measured.

Delay within an SFC could be measured from the time it takes for a packet to traverse the SFC from ingress SF to egress SF. As the SFC's are generally unidirectional in nature, measurement of one-way delay is important. In order to measure one-way delay, the clocks have to be synchronized using NTP, GPS, etc.

Delay variance could also be measured by sending OAM packets and measuring the jitter between the packets passing through the SFC.

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

o Ability to measure the packet processing delay of a service function or a service function path along an SFC.

o Ability to measure the packet loss of a service function or a service function path along an SFC.

5. Gap Analysis

This Section identifies various OAM functions available at different levels. It will also identify various gaps, if not all, existing within the existing toolset, to perform OAM function on an SFC.

5.1. Existing OAM Functions

There are various OAM tool sets available to perform OAM function and network layer, protocol layers and link layers. These OAM functions could validate some of the network overlay transport. Tools like ping and trace are in existence to perform connectivity check and tracing 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 detection of data forwarding failures.

```
+---------------+-------------+------------+--------+-----------+
| Layer         | Connectivity |  Continuity |  Trace | Performance|
+---------------+-------------+------------+--------+-----------+
| N/W Overlay   | Ping        | BFD, NVo3  | Trace  | IPPM      |
+---------------+-------------+------------+--------+-----------+
| SF            | None        | + None     | + None | + None    |
+---------------+-------------+------------+--------+-----------+
| SFC           | None        | + None     | + None | + None    |
+---------------+-------------+------------+--------+-----------+
```
                 Figure 3: OAM Tool GAP Analysis

5.2. Missing OAM Functions

   As shown in Figure 3, OAM functions for SFC are not standardized yet.
   Hence, there are no standard based tools available to verify SF and
   SFC.

5.3. Required OAM Functions

   Primary OAM functions exist for network, transport, link and other
   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.

   For configuration, manageability and orchestration, providing data
   and information models for SFC is very much essential. With
   virtualized SF and SFC, manageability of these functions has to be
   done programmatically.

6. Security Considerations

   SFC and SF OAM must provide mechanisms for:

   o Preventing usage of OAM channel for DDOS attacks.

   o OAM packets meant for a given SFC should not get leaked beyond
      that SFC.

   o Prevent OAM packets to leak the information of an SFC beyond its
      administrative domain.

7. IANA Considerations

   No action is required by IANA for this document.

8. Acknowledgements

   TBD

9. References

9.1. Normative References

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative References

   [I-D.ietf-sfc-problem-statement]
               Quinn, P. and T. Nadeau, "Service Function Chaining
               Problem Statement", draft-ietf-sfc-problem-statement-07
               (work in progress), June 2014.

   [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, June 2011.

Authors' Addresses

   Sam K. Aldrin
   Huawei Technologies

   Email: aldrin.ietf@gmail.com

   Carlos Pignataro
   Cisco Systems

   Email: cpignata@cisco.com

   Nobo Akiya
   Cisco Systems

   Email: nobo@cisco.com