Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: February 16, 2016

S. Aldrin
Google
R. Krishnan
Dell
N. Akiya
Big Switch
C. Pignataro
Cisco Systems
A. Ghanwani
Dell

August 17, 2015

Service Function Chaining Operation, Administration and Maintenance Framework draft-ietf-sfc-oam-framework-00

Abstract

This document provides 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", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 16, 2016.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal

Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

Service Function Chaining (SFC) enables the creation of composite services that consist of an ordered set of Service Functions (SF) that are be applied to packets and/or frames selected as a result of classification. 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:

- SFC problem statement [I-D.ietf-sfc-problem-statement]
- SFC architecture [I-D.ietf-sfc-archiecture]

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

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

- In Section 2, an SFC layering model;
- In Section 3, aspects monitored by SFC OAM;
- In Section 4, functional requirements for SFC OAM;
- In Section 5, a gap analysis for SFC OAM.

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.

2. SFC Layering Model

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

- The service layer, refered to as the "Service Layer" in Figure 1, consists of classifiers and SFs, and uses the

transport network, which could be an overlay network, from a classifier to SF and from one SF to the next.

- The network overlay transport layer, refer to as the "Network", "Transport" and layers below in Figure 1, extends between the various SFs and is mostly transparent to the SFs themselves. It can leverage various overlay network technologies interconnecting SFs and allows establishment of service function paths (SFPs).

- 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.).

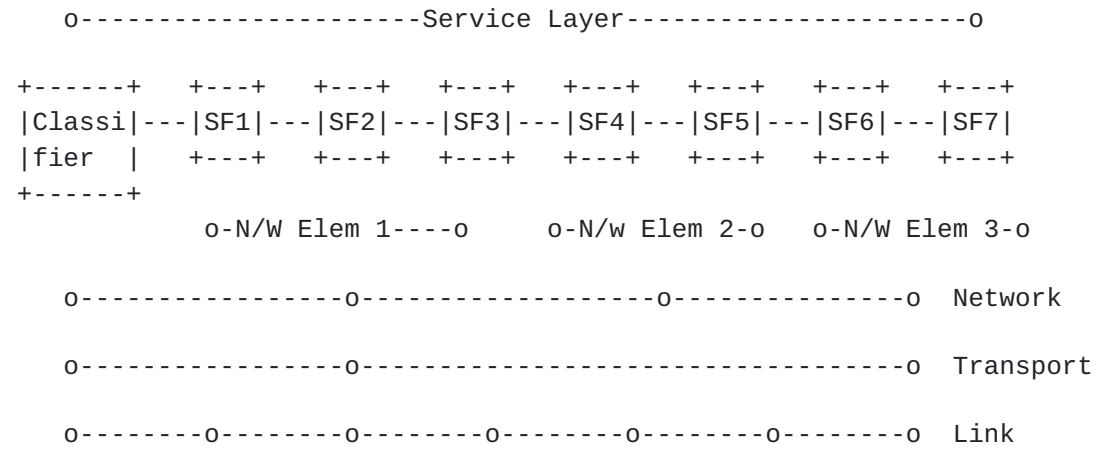


Figure 1: SFC Layering Example

3. Aspects Monitored by SFC OAM?

SFC operates at the service layer. For the purpose of defining the OAM framework, the following aspects of the SFC must be capable of monitored.

1. Service function:

SFs may be SFC-aware or SFC-unaware. An SFC-aware SF is one that understands the SFC encapsulation has the SFF component co-resident with the SF sub-component . An SFC-unware SF is one that does not understand the SFC encapsulation (i.e. a legacy SF) and has to be accessed via an separate SFF and potentially an SFC proxy function.

In both cases, an SF is accessed through an SFF in the SFC architecture. SFC OAM must be able to monitor the SFF associated with a given SF.

2. Service function path:

The SFP comprises a set of SFs that may be ordered or unordered. SFC OAM must be capable of monitoring the SFP and the rendered service path (RSP) that may be used by specific packets.

3. Classifier:

The classifier determines which packets are mapped to an SFP.
SFC OAM must be able to monitor the operation of the classifiers.

The figure below illustrates the various aspects monitored by SFC OAM.

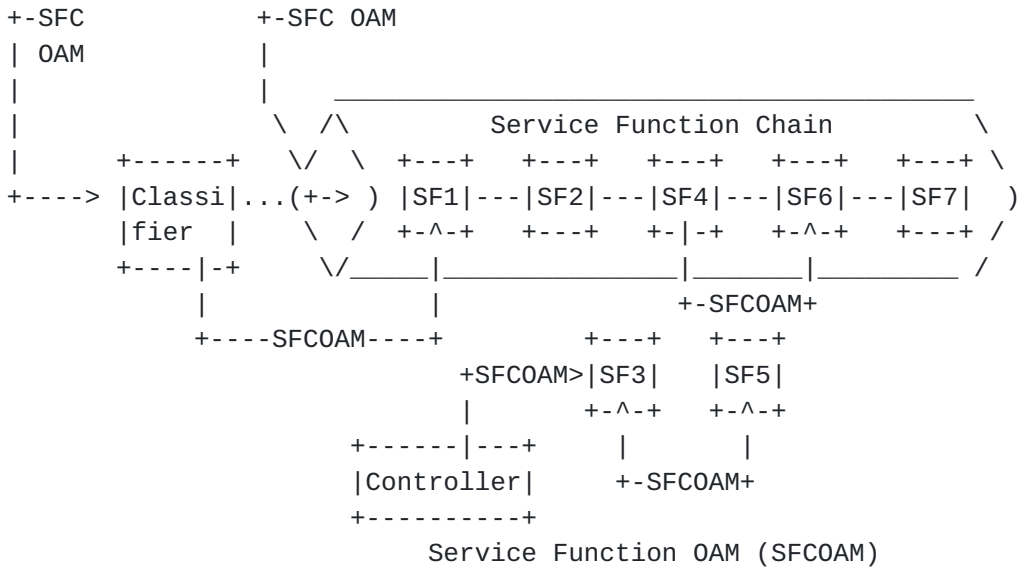


Figure 2: Aspects monitored by SFC OAM

3.1. Operation and Performance of SFs

3.1.1. Monitoring SF Operation

One SFC OAM requirement for the SF component is to
allow an SFC aware network device to monitor a
specific SF. This is accomplished by monitoring the SFF that
the SF is attached to.

A generalized way to monitor the operation of an SF is beyond the scope of SFC OAM, because the functions provided by the SF are not covered by SFC. SFs typically provide their own tools for monitoring.

An optional capability may be provided for an SFF to monitor the operation of its attached SFs and report that on behalf of the SFs.

3.1.2. Service Function Performance Measurement

A second SFC OAM requirement for SF is to
allow an SFC aware network device to check the loss and delay to a
specific SF, located on the same or different network
devices.

3.2. Operation and Performance of SFPs

3.2.1. Monitoring SFP Operation

SFC OAM must be capable of monitoring one or more SFPs or RSPs that are used to realize the SFC and reporting on connectivity and providing fault isolation.

In order to perform service connectivity verification of an SFP, the OAM tools could be initiated from any SFC-aware network device for end-to-end paths, or partial paths terminating on a specific SF, within the SFP. This OAM function is to ensure the SF's chained together has connectivity as it was intended to when SFP was established. Necessary return code(s) 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 (e.g. multiple SFPs, or multiple RSPs), there must be an ability to discover and traverse all available paths.

3.2.2. Service Function Chain Performance Measurement

The ingress of the SFC or an SFC-aware network device must have an ability to perform loss and delay measurements over the SFC as a unit (i.e. end-to-end) or to a specific SF through the SFC.

3.3. Monitoring the Classifier

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. 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 the various aspects monitored by SFC OAM. 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 that the SFs are

operational. 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 SFC component. OAM
messages MAY be encapsulated with necessary SFC

header and with OAM markings when testing the SF component. Some of the OAM functions performed by connectivity functions are as follows:

- 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.

- Verify the packet re-ordering and corruption.

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

- Verification and validating forwarding paths.

- 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 the operator to monitor the network device and to quickly detect failures such as link failures, network failures, SF outages or SFC outages. BFD is one such function which helps in detecting failures quickly. OAM functions supported by continuity check are as follows:

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

- 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. Mechanisms must be provided so that the SFC OAM messages may be sent along the same path that a given data packet would follow. Some of the OAM functions supported by trace functions are:

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

- 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.

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

- 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 should provide the ability to test the 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:

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

- 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 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.

Table 1: OAM Tool GAP Analysis

Layer	Connectivity	Continuity	Trace	Performance
N/W Overlay	Ping	BFD, NVo3	Trace	IPPM
SF	None	+ None	+ None	+ None
SFC	None	+ None	+ None	+ None

5.2. Missing OAM Functions

As shown in Table 1, OAM functions for SFC are not yet standardized. Hence, there are no standards-based tools available to monitor the various components identified in Section 3.

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.

SFC OAM must provide tools that operate through various types of SFs including:

- Transparent SFs: These SFs typically do not make any modifications to the packet. In such cases, the SFF may be able to process OAM messages.

- SFs that modify the packet: These SFs modify packet fields. Certain SFs may modify only the headers corresponding to the network over which it is transported, e.g. the MAC headers or overlay headers. In other cases, the IP header of the application's packet may be modified, e.g. NAT. In yet other cases, the application session itself may be terminated and a new session initiated, e.g. a load balancer that offers HTTPS termination.

6. Open Issues

- Add more details on performance measurement.

- Call out which OAM functions can be achieved by protocol design vs requiring synthetic traffic.

7. Security Considerations

SFC OAM must provide mechanisms for:

- Preventing usage of OAM channel for DDOS attacks.
- Preventing leakage of OAM packets meant for a given SFC beyond that SFC.
- Preventing leakage of information about an sFC beyond its administrative domain.

7. IANA Considerations

No action is required by IANA for this document.

8. Acknowledgements

TBD

9. Contributing Authors

Pedro A. Aranda Gutierrez
Telefonica I+D
Email: pedroa.aranda@tid.es

Diego Lopez
Telefonica I+D
Email: diego@tid.es

Joel Halpern
Ericsson
Email: joel.halpern@ericsson.com

Sriganesh Kini
Ericsson
Email: sriganesh.kini@ericsson.com

Andy Reid
BT
Email: andy.bd.reid@bt.com

10. References

10.1. Normative References

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

[I-D.ietf-sfc-problem-statement]

Quinn, P. and T. Nadeau, "Service Function Chaining
Problem Statement", draft-ietf-sfc-problem-statement-10
(work in progress), August 2014.

[I-D.ietf-sfc-architecture]
Halpern J. and C. Pignataro, "Service Function Chaining (SFC) Architecture", draft-ietf-sfc-architecture-09 (work in progress), June 2015.

10.2. Informative References

[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
Google
Email: aldrin.ietf@gmail.com

Ram Krishnan
Dell
Email: ramkri123@gmail.com

Nobo Akiya
Big Switch
Email: nobo.akiya.dev@gmail.com

Carlos Pignataro
Cisco Systems
Email: cpignata@cisco.com

Anoop Ghanwani
Dell
Email: anoop@alumni.duke.edu