SFC Working Group
Internet Draft
Category: Informational

R. Krishnan
Brocade
A. Ghanwani
Dell
Pedro A. Aranda Gutierrez
D. R. Lopez
Telefonica I+D
J. Halpern
S. Kini
Ericsson
Andy Reid
BT

Expires: October 2014 July 3, 2014

SFC OAM Requirements and Framework

draft-krishnan-sfc-oam-req-framework-00

Abstract

This document discusses SFC OAM requirements and proposes a SFC OAM Framework to handle these requirements.

This Internet-Draft will expire on April, 2014.

Conventions used in this document

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 [RFC 2119].

Table of Contents

1. Introduction

Operations, administration, and maintenance (OAM) is the general term applied to monitoring both the connectivity and performance in the network [RFC 6291] [RFC 7276]. The goal of SFC OAM then is to monitor these attributes for a service function chain (SFC).

Some clarification is needed regarding the scope of this work. SFC OAM does will not attempt to monitor the actual services. Also, SFC OAM does not replace or obviate the need for transport-level OAM functions such as NVO3 OAM, IEEE 802.1ag, MPLS OAM, or whatever else may be applicable depending on the network technology that the SFC is implemented on.

The following figure depicts the layering of OAM.

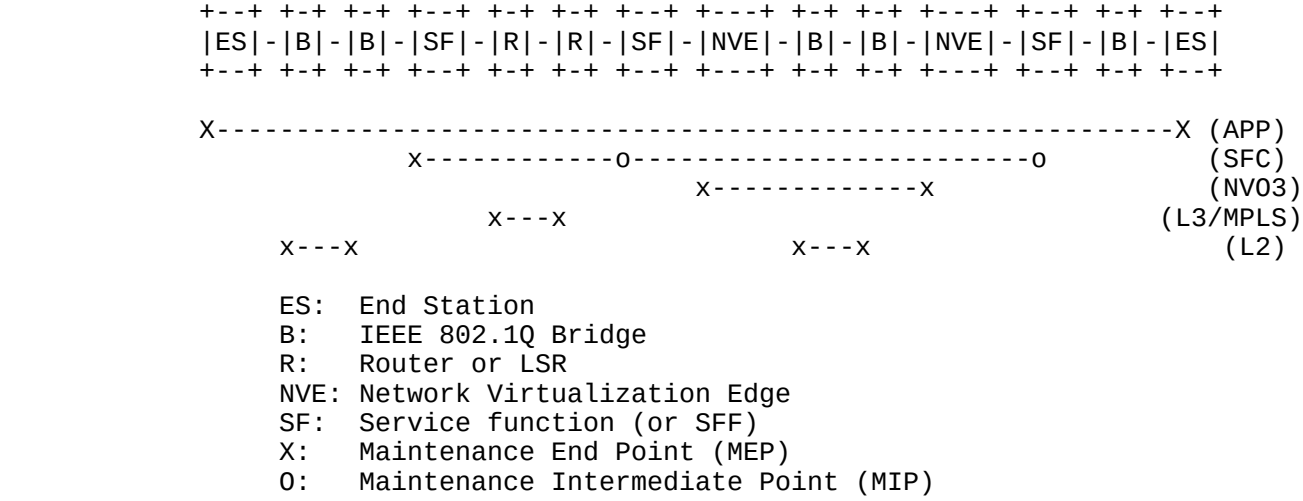

Figure 1: Layered OAM Architecture

The SFC layer resides above the transport layer (where the transport layer can simply be implemented using VLANs or may be done using overlays such as VXLAN or NVGRE), and below the application layer (APP). As mentioned earlier, depending on the underlying network technology, other OAM layers may be present (NVO3 OAM [NVO3 OAM], L3/MPLS OAM [RFC 7276], IEEE 802.1ag CFM [IEEE 802.1ag], etc.). The use of the terms maintenance end point (MEP) and maintenance (MIP) are consistent with IEEE 802.1Q are simply used to denote points where monitoring services are configured.

The systems denoted SF refer to devices in the network that either insert, modify, remove, or access the service chain header (SCH) [SCH draft]. These nodes may implement the actual service function (as would be the case for an SF-aware appliance) or they may be proxy nodes such as SFFs with the service function itself residing in a different device (as would be the case for an SF-unaware appliance).

1.1. Acronyms

DPI: Deep Packet Inspection

MPLS: Multiprotocol Label Switching

NVGRE: Network Virtualization using Generic Routing Encapsulation

OAM: Operations, Administration, and Maintenance

SF: Service Function

SFC: Service Function Chain

SFP: Service Function Path

VXLAN: Virtual Extensible LAN

2. SFC OAM Requirements

2.1. Topologies

Mechanisms must be provided to monitor the entire SFP or just a portion of the SFP.

SFC OAM must also be able to handle various topologies that can be created such a point-to-point or multipoint.

2.2. Connectivity

2.2.1. Connectivity Check

The purpose of the connectivity check tool is to test the liveness of a given service function along a given SFP (service function path).

Mechanisms must be provided so that the SFC OAM messages may be sent along the same path that a given data packet would follow. In other words, it should be possible to construct SFC OAM packets that would be treated by network devices such as bridges and routers as they would handle regular data packets on that SFP from the standpoint of functions such as link aggregation and equal cost multipath.

2.2.2. SFP Trace

The purpose of SFP trace is to provide the list of SFs that comprise the service function chain as defined by the SCH.

Mechanisms must be provided so that the SFC OAM messages may be sent along the same path that a given data packet would follow. In other words, it should be possible to construct SFC OAM packets that would be treated by network devices such as bridges and routers as they would handle regular data packets on that SFP from the standpoint of functions such as link aggregation and equal cost multipath.

2.3. Performance

It must be possible to measure various parameters of a given SFP such as the loss, delay, and delay variation through the service chain.

[Ed Note: Details TBD]

2.4. Leakage of OAM Messages

Mechanisms must be provided to ensure that OAM messages are received only by devices that need to process them. These messages must never be forwarded to devices that would terminate such messages as result of not knowing how to process them.

2.5. Appliance Types

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

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

- Appliances that modify the packet: These appliances modify packet fields. Certain appliances 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.

In general, it should be possible to allow or disallow having a given SF operate on an OAM packet in the same way that it would on a regular data packet, but with the awareness that it is operating on an OAM packet. It is essential to recognize the OAM message so that its status (as an OAM message) can be preserved as it is processed through the normal data path.

3. IANA Considerations

This draft does not have any IANA considerations.

4. Security Considerations

TBD

5. Acknowledgements

6. References

6.1. Normative References

6.2. Informative References

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

[RFC 6291] Andersson, L. et al., "Guidelines for the Use of the "OAM" Acronym in the IETF," June 2011

[RFC 7276] Mizrahi, T. et al., "An Overview of Operations, Administration, and Maintenance (OAM) Tools," June 2014

[NVO3 OAM] Senevirathne, T., "NVO3 Fault Management," https://datatracker.ietf.org/doc/draft-tissa-nvo3-oam-fm/?include_text=1, August 2014

[STEALTH FIREWALL] Brandon Gillespie "Stealth firewalls", http://www.giac.org/paper/gsec/629/stealth-firewalls/101440

[SCH draft] Quinn, P. et al., "Network Service Header," https://datatracker.ietf.org/doc/draft-quinn-sfc-nsh/, February 2014

Authors' Addresses

Ram Krishnan
Brocade Communications
ramk@brocade.com

Anoop Ghanwani
Dell
anoop@alumni.duke.edu

Pedro A. Aranda Gutierrez
Telefonica I+D
Don Ramon de la Cruz, 82
Madrid, 28006, Spain
+34 913 129 041
pedroa.aranda@tid.es

Diego Lopez
Telefonica I+D
Don Ramon de la Cruz, 82
Madrid, 28006, Spain
+34 913 129 041
diego@tid.es

Joel Halpern
Ericsson
joel.halpern@ericsson.com

Sriganesh Kini
Ericsson
Sriganesh.kini@ericsson.com

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