ï»¿

Internet Engineering Task Force (IETF)
Request for Comments: 8924
Category: Informational
ISSN: 2070-1721

S. Aldrin
Google
C. Pignataro, Ed.
N. Kumar, Ed.
Cisco
R. Krishnan
VMware
A. Ghanwani
Dell

October 2020

Service Function Chaining (SFC) Operations, Administration, and Maintenance (OAM) Framework

Abstract

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

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8924.

Table of Contents

1. Introduction
   1.1. Document Scope
   1.2. Acronyms and Terminology
      1.2.1. Acronyms
      1.2.2. Terminology
2. SFC Layering Model
3. SFC OAM Components
   3.1. The SF Component
      3.1.1. SF Availability
      3.1.2. SF Performance Measurement
   3.2. The SFC Component
      3.2.1. SFC Availability
      3.2.2. SFC Performance Measurement

3.3. Classifier Component
3.4. Underlay Network
3.5. Overlay Network
4. SFC OAM Functions
4.1. Connectivity Functions
4.2. Continuity Functions
4.3. Trace Functions
4.4. Performance Measurement Functions
5. Gap Analysis
5.1. Existing OAM Functions
5.2. Missing OAM Functions
5.3. Required OAM Functions
6. Operational Aspects of SFC OAM at the Service Layer
6.1. SFC OAM Packet Marker
6.2. OAM Packet Processing and Forwarding Semantic
6.3. OAM Function Types
7. Candidate SFC OAM Tools
7.1. ICMP
7.2. BFD / Seamless BFD
7.3. In Situ OAM
7.4. SFC Traceroute
8. Manageability Considerations
9. Security Considerations
10. IANA Considerations
11. Informative References
Acknowledgements
Contributors
Authors' Addresses

1. Introduction

Service Function Chaining (SFC) enables the creation of composite services that consist of an ordered set of Service Functions (SFs) that are to be applied to any traffic 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:

* SFC Problem Statement [RFC7498]

* SFC Architecture [RFC7665]

The reader is assumed to be familiar with the material in [RFC7665].

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

* an SFC layering model (Section 2),

* aspects monitored by SFC OAM (Section 3),

* functional requirements for SFC OAM (Section 4),

* a gap analysis for SFC OAM (Section 5),

* operational aspects of SFC OAM at the service layer (Section 6),

* applicability of various OAM tools (Section 7), and

* manageability considerations for SF and SFC (Section 8).

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

OAM controllers are SFC-aware network devices that are capable of generating OAM packets. They should 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

BFD	Bidirectional Forwarding Detection
CLI	Command-Line Interface
DWDM	Dense Wavelength Division Multiplexing
E-OAM	Ethernet OAM
hSFC	Hierarchical Service Function Chaining
IBN	Internal Boundary Node
IPPM	IP Performance Metrics
MPLS	Multiprotocol Label Switching
MPLS_PM	MPLS Performance Measurement
NETCONF	Network Configuration Protocol
NSH	Network Service Header
NVO3	Network Virtualization over Layer 3
OAM	Operations, Administration, and Maintenance
POS	Packet over SONET
RSP	Rendered Service Path
SF	Service Function
SFC	Service Function Chain
SFF	Service Function Forwarder
SFP	Service Function Path
SNMP	Simple Network Management Protocol
TRILL	Transparent Interconnection of Lots of Links
VM	Virtual Machine

1.2.2. Terminology

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

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.).

* The service layer consists of SFC data-plane elements that include classifiers, Service Functions (SFs), Service Function Forwarders (SFF), and SFC Proxies. This layer uses the overlay network layer

for ensuring connectivity between SFC data-plane elements.

* The overlay network layer leverages various overlay network technologies (e.g., Virtual eXtensible Local Area Network (VXLAN)) for interconnecting SFC data-plane elements and allows establishing Service Function Paths (SFPs). This layer is mostly transparent to the SFC data-plane elements, as not all the data-plane elements process the overlay header.

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

* The link layer is tightly coupled with the physical technology used. Ethernet is one such choice for this layer, but other alternatives may be deployed (e.g., POS and DWDM). In a virtual environment, virtualized I/O technologies, such as Single Root I/O Virtualization (SR-IOV) or similar, are also applicable for this layer. The same or distinct link layer technologies may be used in each leg shown in Figure 1.

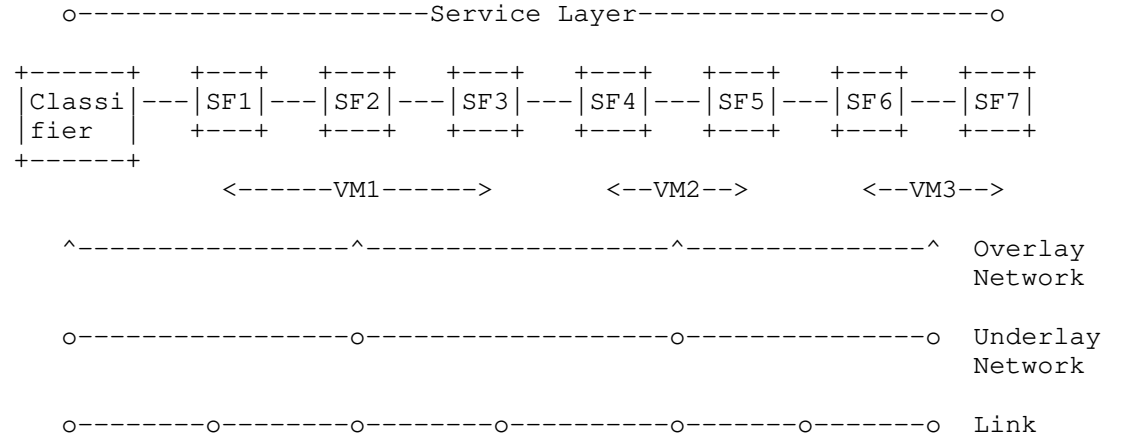

Figure 1: SFC Layering Example

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

While Figure 1 depicts an 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 entities, 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:

SF component:
: OAM functions applicable at this component include testing the SFs from any SFC-aware network device (e.g., classifiers, controllers, and other service nodes). Testing an SF may be more expansive than just checking connectivity to the SF, such as checking if the SF is providing its intended service. Refer to Section 3.1.1 for a more detailed discussion.

SFC component:
: OAM functions applicable at this component include (but are not limited to) testing the SFCs and the SFPs, validation 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.

Classifier component:
OAM functions applicable at this component include testing the validity of the classification rules and detecting any incoherence among the rules installed when more than one classifier is used, as explained in Section 2.2 of [RFC7665].

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

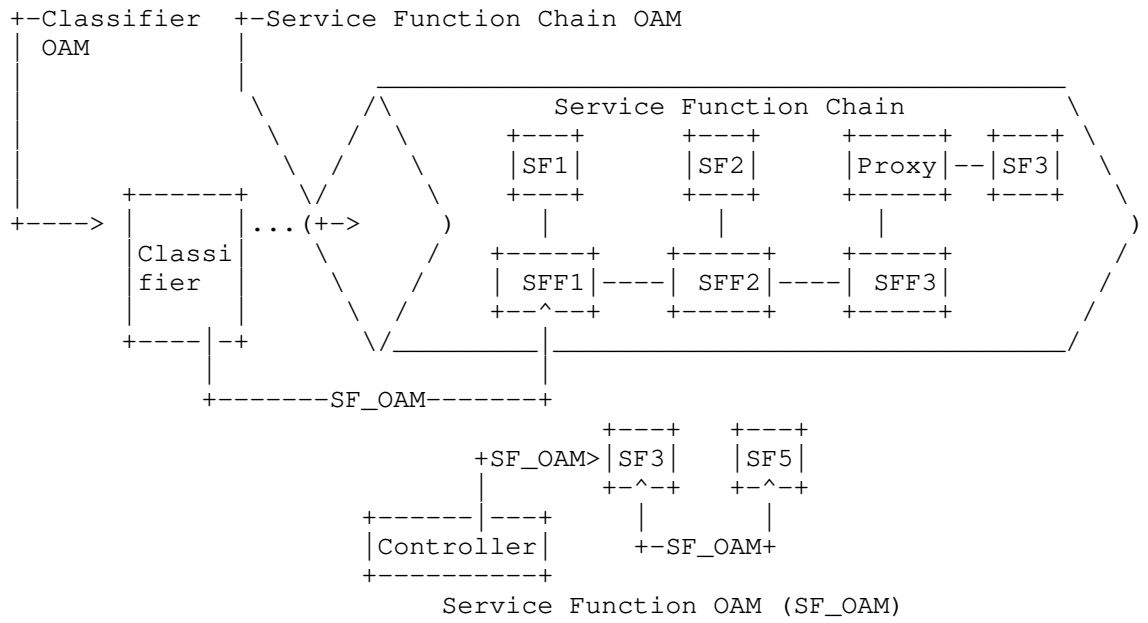

Figure 2: SFC OAM Components

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). For cases where multiple instances of an SF are used to realize a given SF for the purpose of load sharing, SF availability can be performed by checking the availability of any one of those instances, or the availability check may be targeted at a specific instance. SF availability is an aspect that raises an interesting question: How does one determine that an SF is available? At 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. At the other end of the spectrum, one might argue that the SF's availability can only be deduced if the packet, after passing through the SF, was examined and it was verified that the packet did indeed get the expected service.

The former approach will likely not provide sufficient confidence about the actual SF availability, i.e., a service node and an 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 drop certain packets intentionally. In such cases, it is normal behavior that certain packets will not be egressing out from the SF. 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 the 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.

The SF availability check can be performed using a generalized approach, i.e., at an adequate granularity to provide a basic SF service. The task of evaluating the true availability of an SF is a complex activity, currently having no simple, unified solution. There is currently no standard means of doing so. Any such mechanism would be far from a typical OAM function, so it is not explored as part of the analysis in Sections 4 and 5.

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. Performance measurement can be passive by using live traffic, an active measurement by using synthetic probe packets, or a hybrid method that uses a combination of active and passive measurement. More details about this OAM function is explained in Section 4.4.

On the one hand, the performance of any specific SF can be quantified by measuring the loss and delay metrics of the traffic from the 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. For cases where multiple instances of an SF are used to realize a given SF for the purpose of load sharing, SF performance can be quantified by measuring the metrics for any one instance of SF or by measuring the metrics for a specific instance.

The metrics measured to quantify the performance of the SF component are not just limited to loss and delay. Other metrics, such as throughput, also exist and the choice of metrics for performance measurement is outside the scope of this document.

3.2. The SFC Component

3.2.1. SFC Availability

An SFC could comprise 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 device 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 on a specific segment of SFs within the SFC.

3.3. 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 and detect any misclassification. Sample OAM packets can be presented to the classifiers to assess the behavior with regard to a given classification entry.

The classifier availability check may be performed to check the availability of the classifier to apply the rules and classify the traffic flows. Any SFC-aware network device should have the ability to perform availability checking of the classifier component for each SFC.

Any SFC-aware network device should have the ability to perform performance measurement of the classifier component for each SFC. The performance can be quantified by measuring the performance metrics of the traffic from the classifier for each SFC/SFP.

3.4. Underlay Network

The underlay network provides connectivity between the SFC components, so the availability or the performance of the underlay network directly impacts the SFC OAM.

Any SFC-aware network device may have the ability to perform an availability check or performance measurement of the underlay network using any existing OAM functions listed in Section 5.1.

3.5. Overlay Network

The overlay network provides connectivity for the service plane between the SFC components and is mostly transparent to the SFC data-plane elements.

Any SFC-aware network device may have the ability to perform an availability check or performance measurement of the overlay network using any existing OAM functions listed in Section 5.1.

4. SFC OAM Functions

Section 3 described SFC OAM components and the associated OAM operations on each of them. This section explores SFC OAM functions that are applicable for more than one SFC component.

The various SFC OAM requirements listed in Section 3 highlight the need for various OAM functions at the service layer. 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 on a single SF/SFF or multiple SFs/SFFs spanning across one or more SFCs.

4.1. Connectivity Functions

Connectivity is mainly an on-demand function to verify that connectivity exists between certain network elements and that the SFs are available. For example, Label Switched Path (LSP) Ping [RFC8029] is a common tool used to perform this function for an MPLS network. Some of the OAM functions performed by connectivity functions are as follows:

* 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.

* Detect any packet reordering and corruption.

* Verify that an SFC or SF is applying the expected policy.

* Verify and validate 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 of 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 protocol that helps in detecting failures quickly. OAM functions supported by continuity functions are as follows:

* Provision a continuity check to a given SF within an SFC or for the entire SFC.

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

* Notifying other OAM functions or applications of the detected failures so they can 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, and SFC Proxy) on the tested layer. This function is typically useful for gathering information from every transit device 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:

* the ability to trigger an action from every transit device at the SFC layer, using TTL or other means,

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

* the ability to discover and traverse ECMP paths within an SFC, and

* the ability to skip SFs that do not support OAM while tracing SFs in an SFC.

4.4. Performance Measurement Functions

Performance measurement functions involve measuring of packet loss, delay, delay variance, etc. These performance metrics may be measured proactively 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. To ensure accurate estimations, one needs to ensure that OAM packets are treated the same and also share the same fate as regular data traffic.

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. Measurement protocols, such as the One-Way Active Measurement Protocol (OWAMP) [RFC4656] and the Two-Way Active Measurement

Protocol (TWAMP) [RFC5357], can be used to measure delay characteristics. 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, GPS, Precision Time Protocol (PTP), etc.

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

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

* the 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, and

* the 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 layers 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 toolsets 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 checks and trace intermediate hops in a network. These tools support different network types, like IP, MPLS, TRILL, etc. Ethernet OAM (E-OAM) [Y.1731] [EFM] and Connectivity Fault Management (CFM) [DOT1Q] offer OAM mechanisms, such as a continuity check for Ethernet links. There is an effort around NVO3 OAM to provide connectivity and continuity checks for networks that use NVO3. BFD is used for the detection of data-plane forwarding failures. The IPPM framework [RFC2330] offers tools such as OWAMP [RFC4656] and TWAMP [RFC5357] (collectively referred to as IPPM in this section) to measure various performance metrics. MPLS Packet Loss Measurement (LM) and Packet Delay Measurement (DM) (collectively referred to as MPLS_PM in this section) [RFC6374] offer the ability to measure performance metrics in MPLS networks. There is also an effort to extend the toolset to provide connectivity and continuity checks within overlay networks. BFD is another tool that helps in detecting data forwarding failures. Table 1 below is not exhaustive.

Layer	Connectivity	Continuity	Trace	Performance
Underlay network	Ping	E-OAM, BFD	Trace	IPPM, MPLS_PM
Overlay network	Ping	BFD, NVO3 OAM	Trace	IPPM
Classifier	Ping	BFD	Trace	None
SF	None	None	None	None
SFC	None	None	None	None

Table 1: OAM Tool Gap Analysis

5.2. Missing OAM Functions

As shown in Table 1, there are no standards-based tools available at the time of this writing that can be used natively (i.e., without enhancement) 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.

As depicted in Table 1, toolsets and solutions are required to perform the OAM functions at the service layer.

6. Operational Aspects of SFC OAM at the Service Layer

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

SFC OAM messages should be encapsulated with the necessary SFC header and with OAM markings when testing the SFC component. SFC OAM messages may be encapsulated with the necessary SFC header and with OAM markings when testing the SF component.

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 OAM packets 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 at the service layer must have a way to mark the packet as an OAM packet.

6.2. OAM Packet Processing and Forwarding Semantic

Upon receiving an OAM packet, an SFC-aware SF may choose to discard the packet if it does not support OAM functionality or if the local policy prevents it 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 to not forward the OAM packet to an SF if the SF does not support OAM or if the policy does not allow the forwarding of OAM packets to that SF. The SFF may choose to skip the SF, modify the packet's header, and forward the packet to the next SFC node in the chain. It should be noted that skipping an SF might have implications 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 toolset 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 an OAM packet, it is not sufficient to indicate what OAM function the packet is intended for. The Next Protocol field in the NSH header may be used to indicate what OAM function is intended or what toolset is used. Any other overlay encapsulations used at the service layer must have a similar way to indicate the intended OAM function.

7. Candidate SFC OAM Tools

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

7.1. ICMP

[RFC0792] and [RFC4443] describe the use of ICMP in IPv4 and IPv6 networks 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 functions (defined in Section 4.1) to verify the availability of an SF or SFC. The initiator can generate an ICMP echo request message and control the service-layer encapsulation header to get the response from the relevant node. For example, a classifier initiating OAM can generate an ICMP echo request message, set the TTL field in the NSH header [RFC8300] to 63 to get the response from the last SFF, and thereby test the SFC availability. Alternatively, the initiator can set the TTL to some other value to get the response from a specific SF and thereby partially test SFC availability, or the initiator could send OAM packets with sequentially incrementing TTL in the NSH to trace the SFP.

It could be observed that ICMP as currently defined may not be able to perform all required SFC OAM functions, but as explained above, it can be used for some of the connectivity functions.

7.2. BFD / Seamless BFD

[RFC5880] defines the Bidirectional Forwarding Detection (BFD) mechanism for failure detection. [RFC5881] and [RFC5884] define 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 networks.

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

7.3. In Situ OAM

[IOAM-NSH] defines how In situ OAM data fields [IPPM-IOAM-DATA] are transported using the NSH header. [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), IOAM Option-Types, such as IOAM Trace Option-Types, can also be used to perform other SFC OAM functions, such as SFC tracing.

In situ OAM could be leveraged to perform SF availability and SFC availability or performance measurement. For example, if SFC is realized using NSH, the O bit in the NSH header could be set to indicate the OAM traffic, as defined in Section 4.2 of [IOAM-NSH].

7.4. SFC Traceroute

[SFC-TRACE] defines a protocol that checks for path liveliness and traces the service hops in any SFP. Section 3 of [SFC-TRACE] defines the SFC trace packet format, while Sections 4 and 5 of [SFC-TRACE] define the behavior of SF and SFF respectively. While [SFC-TRACE] has expired, the proposal is implemented in Open Daylight and is available.

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

8. Manageability Considerations

This document does not define any new manageability tools but consolidates the manageability tool gap analysis for SF and SFC. Table 2 below is not exhaustive.

Layer	Configuration	Orchestration	Topology	Notification
Underlay network	CLI, NETCONF	CLI, NETCONF	SNMP	SNMP, Syslog, NETCONF
Overlay network	CLI, NETCONF	CLI, NETCONF	SNMP	SNMP, Syslog, NETCONF
Classifier	CLI, NETCONF	CLI, NETCONF	None	None
SF	CLI, NETCONF	CLI, NETCONF	None	None
SFC	CLI, NETCONF	CLI, NETCONF	None	None

Table 2: OAM Tool Gap Analysis

Configuration, orchestration, and other manageability tasks of SF and SFC could be performed using CLI, NETCONF [RFC6241], etc.

While the NETCONF capabilities are readily available, as depicted in Table 2, the information and data models are needed for configuration, manageability, and orchestration for SFC. With virtualized SF and SFC, manageability needs to be done programmatically.

9. Security Considerations

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

The OAM information from the 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 the 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 SFs 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 a Denial of Service (DoS) attack by overloading any specific SF using rogue OAM traffic.

To address the above concerns, SFC and SF OAM should provide mechanisms for mitigating:

* misuse of the OAM channel for denial of services,

* leakage of OAM packets across SFC instances, and

* leakage of SFC information beyond the SFC domain.

The documents proposing the OAM solution for SF components should provide rate-limiting the OAM probes at a frequency guided by the implementation choice. Rate-limiting may be applied at the classifier, 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. To mitigate any attacks that leverage OAM packets, future documents proposing OAM solutions should describe the use of any technique to detect and mitigate anomalies and various security attacks.

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

10. IANA Considerations

This document has no IANA actions.

11. Informative References

[DOT1Q] IEEE, "IEEE Standard for Local and metropolitan area networks--Bridges and Bridged Networks", IEEE 802.1Q-2014, DOI 10.1109/IEEESTD.2014.6991462, November 2014, <https://doi.org/10.1109/IEEESTD.2014.6991462>.

[EFM] IEEE, "IEEE Standard for Ethernet", IEEE 802.3-2018, DOI 10.1109/IEEESTD.2018.8457469, June 2018, <https://doi.org/10.1109/IEEESTD.2018.8457469>.

[IOAM-NSH] Brockners, F. and S. Bhandari, "Network Service Header (NSH) Encapsulation for In-situ OAM (IOAM) Data", Work in Progress, Internet-Draft, draft-ietf-sfc-ioam-nsh-04, 16 June 2020, <https://tools.ietf.org/html/draft-ietf-sfc-ioam-nsh-04>.

[IPPM-IOAM-DATA] Brockners, F., Bhandari, S., and T. Mizrahi, "Data Fields for In-situ OAM", Work in Progress, Internet-Draft, draft-ietf-ippm-ioam-data-10, 13 July 2020, <https://tools.ietf.org/html/draft-ietf-ippm-ioam-data-10>.

[PROOF-OF-TRANSIT] Brockners, F., Bhandari, S., Mizrahi, T., Dara, S., and S. Youell, "Proof of Transit", Work in Progress, Internet-Draft, draft-ietf-sfc-proof-of-transit-06, 16 June 2020, <https://tools.ietf.org/html/draft-ietf-sfc-proof-of-transit-06>.

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

[RFC2330] Paxson, V., Almes, G., Mahdavi, J., and M. Mathis, "Framework for IP Performance Metrics", RFC 2330,

DOI 10.17487/RFC2330, May 1998,
<https://www.rfc-editor.org/info/rfc2330>.

[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>.

[RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, DOI 10.17487/RFC4656, September 2006, <https://www.rfc-editor.org/info/rfc4656>.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, DOI 10.17487/RFC5357, October 2008, <https://www.rfc-editor.org/info/rfc5357>.

[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>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[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>.

[RFC6374] Frost, D. and S. Bryant, "Packet Loss and Delay Measurement for MPLS Networks", RFC 6374, DOI 10.17487/RFC6374, September 2011, <https://www.rfc-editor.org/info/rfc6374>.

[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>.

[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>.

[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>.

[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>.

[SFC-TRACE] Penno, R., Quinn, P., Pignataro, C., and D. Zhou, "Services Function Chaining Traceroute", Work in Progress, Internet-Draft, draft-penno-sfc-trace-03, 30 September 2015, <https://tools.ietf.org/html/draft-penno-sfc-trace-03>.

[Y.1731] ITU-T, "G.8013: Operations, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks", August 2015, <https://www.itu.int/rec/T-REC-G.8013-201508-I/en>.

Acknowledgements

We would like to thank Mohamed Boucadair, Adrian Farrel, Greg Mirsky, Tal Mizrahi, Martin Vigoureux, Tirumaleswar Reddy, Carlos Bernados, Martin Duke, Barry Leiba, Ã\211ric Vyncke, Roman Danyliw, Erik Kline, Benjamin Kaduk, Robert Wilton, Frank Brockner, Alvaro Retana, Murray Kucherawy, and Alissa Cooper for their review and comments.

Contributors

Nobo Akiya
Ericsson

Email: nobo.akiya.dev@gmail.com

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