Network Working Group
INTERNET-DRAFT
Intended Status: standard
Expires: August 08, 2025

J. Dai
CICT and PCL
S. Yu
PCL
W. Cheng
China Mobile
X. Wang
D. Deng
Fiberhome

February 08, 2025

Protocol extension and mechanism for fused service function chain
draft-dai-sfc-fused-protocol-and-procedure-04

Abstract

This document discusses the protocol extension and procedure that are used to implement the fused service function chain. Fused service function chain means that two or more service function chains are fused to become a single service function chain from the view of data plane and control plane. Fused service function chain is a extension for service function chain.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

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

The delivery of end-to-end services often requires various service functions. These include traditional network service functions such as firewalls and traditional IP Network Address Translators (NATs),

as well as application-specific functions. The definition and instantiation of an ordered set of service functions and subsequent "steering" of traffic through them is termed Service Function Chaining (SFC).[RFC7665]. [RFC7498] describes the motive for service function chain.

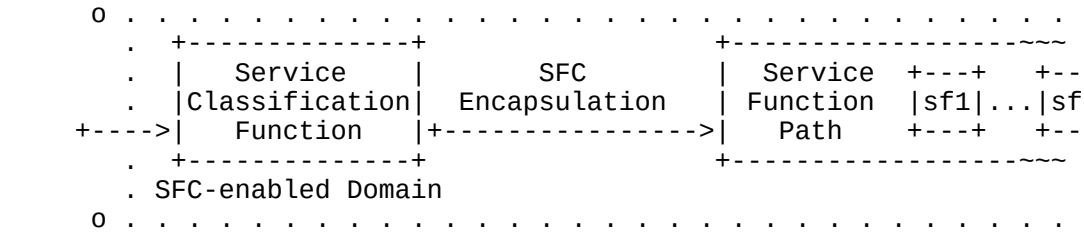


Figure 1: Architecture of service function chain

There are many application scenarios that can use technologies or methods related to service function chain (see RFC 7665). However, some application scenarios have not yet been covered by RFC 7665. For example, RFC 8459 illustrates an application scenario corresponding to large, geographically dispersed network and SFC for that application scenario is called Hierarchical service function chain.

Hierarchical service function chain described in RFC 8459 is only one of the application scenarios that have not been covered by RFC 7665. Many other application scenarios that can be enhanced by service function chain can’t yet be covered by RFC 8459. I_D_fused-architecture-and-scenario has illustrated some of the afore-mentioned. application scenarios.

However, in order to carry out the fused service function chain, extension for the relevant protocol and new methods or procedure are necessary, and it is the target of this draft.

1.1 Terminology

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].

2. Overview of the Architecture of Fused Service Function Chain

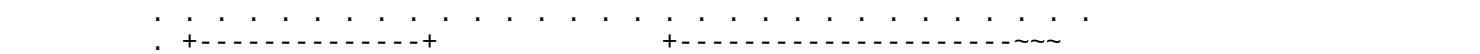
As is described in clause 1, there is a need to fuse two or more service fucntion chain to form a single service chain when service

function chain is applied in some application scenarios. the afore-mentioned single service function chain is called fused service function chain (F-SFC). The detailed description about arthitecture for fused service function chain can be seen in [I-D.ietf-sfc-arch -fused-sfc].The following is brief introdution for the afore-mentioned architecture.

At first, a F-SFC is composed of two or more service function chains that are logically independent each other and possibly seperate physically.

Secondly, a F-SFC can be thought as a single service function chain from the view of data plane and management plane. That is to say, data packet can be steered through all selected SFs within the F-SFC according to preset configuration. moreover, a F-SFC can be managed by a management entity and the management entity can think the F-SFC as an ordinary service function chain.

Thirdly, all service function chains within a F-SFC can still work as an independent service function chain. In other words, if a F-SFC consists of SFC A, SFC B and SFC C, SFCs with the F-SFC such as SFC A can also be used as an independent if it is needed.



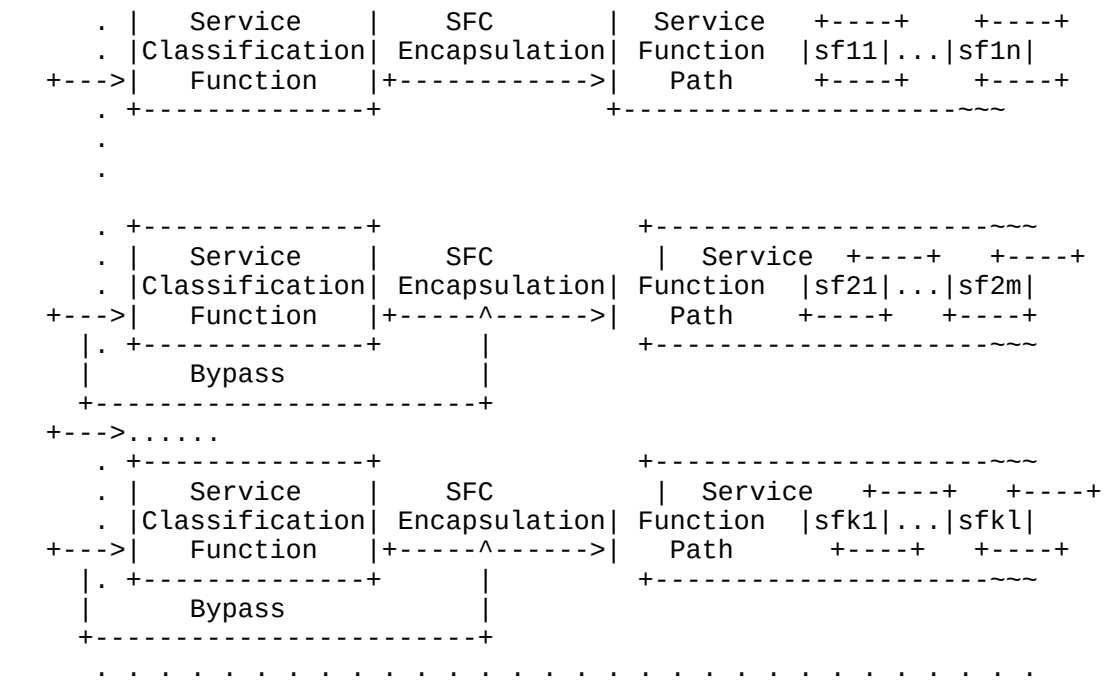


Figure 2: General architecture for fused service function chain

Figure 2 describes a general architecture of F-SFC. From the figure, it can be learned that the F-SFC is composed of SFC1, SFC2 ... and SFCj. SFC1 consists SF11, SF12 ... and SF1n. SFC2 consists SF21, SF22 ... and SF2m. ... SFCk consists SFk1, SFk2 ... and SFkl. This figure can also be seen in [I-D.ietf-sfc-arch-fused-sfc].

All SFs within SFC1, SFC2 ... and SFCj can be used by F-SFC. On the one hand, SFs within SFC(i+1) should be used after SFs within SFC(i) in order to keep the logical order of SFCs. On the other hand, SFs within the same SFC should take action based on logical order of the SFC.

It is noted that all CFs (Classification Function) in SFC2 ... SFCk can be configurated to work in By-pass mode in order that SFC2 ... SFCk can action based on the result of the CF in SFC1. It is sure all CFs can also work in normal mode.

3 Protocol Extention for Network Service Header

3.1 The original formation of Network Service Header

[RFC 8300] specifies the detailed information of Network Service Header (NSH). A typical NSH is composed of the following three parts:

Base Header: Provides information about the service header and the payload protocol.

Service Path Header: Provides path identification and location within a service path.

Context Header: Carries metadata (i.e., context data) along a service path.

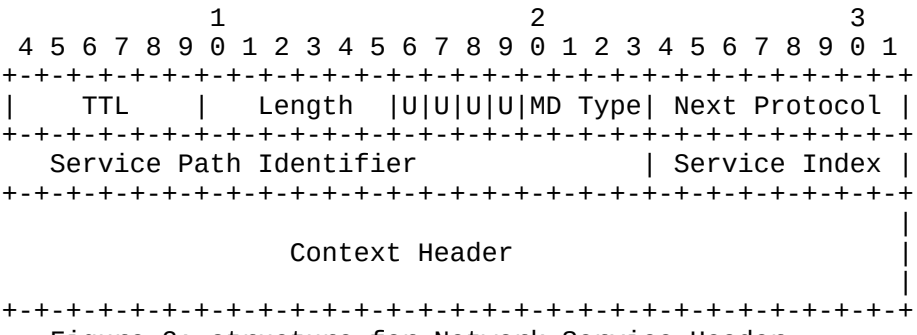


Figure 2: structure for Network Service Header

Figure 2 describes the formation of the NSH. The first Row is used to describe 'Base Header' meanwhie the second row is used to specify 'Service Path Header'. The third row is 'Context Header'. There five bits marked 'U' in the Base Header of NSH are not defined in [RFC 8300].

3.2 Extension for NSH

At first, in order to carry out a fused service function chain, a certain mechanism should be used to tell components within a SFC whether the packet is bound to a common SFC or a fused SFC.

Because all inforamtion related to a SFC is enveloped in the NSH, some modification should be taken on the NSH when it is needed to classify packets of a Fused SFC from packets of a common SFC.

There are the following two solutions to implement the afore-mentioned classification funciton:

.Using one of the five unused bits as the F-SFC bit, and the bit is defined as follows:

0: the packet is related to a common SFC.

1: the packet is related to a fused SFC.

.Encoding 'Service Path Identifier'.

some numbers are used for F-SFC meanwhile other numbers are used to represent common SFCs. For example, the packet is bound to a F-SFC when the most significant bit of 'Service Path Identifier' is set, and the other packets are related to a common SFC.

It is recommended that the first solution should be used to classify the packets of a F-SFC from the packets of a common SFC. And the third bit of the 'Base Header ' is recommended to be used.

3.3 SPI in NSH

When a packet related to a F-SFC is sent out from the classifier of the first SFC that belongs to the F-SFC, a NSH will be inserted into the packet and the SPI is related to the F-SFC rather than a common

SFC within the F-SFC. A common SFC in the F-SFC is called a member SFC of the F-SFC.

On the other hand, every member SFC of the F-SFC also has a corresonding SPI and the SPI of the member SFC is different from SPI of the F-SFC. That will bring some problems to forwarding functions of the SFC components.

Generally, within every member SFC of a F-SFC, the packet forwarding action is based on SPI of the member SFC, though the NSH of the forarded packet envelops the SPI of the F-SFC.

So, it is needed that some mechnism to be used to realize the function to map from SPI of the F-SFC to SPI of the member SFC. The mapping mechanism of SPI is specified in clause 4.

4 Mapping of SPI

4.1 Candidate solutions for information exchanging

If a functional component of SFC wants to map a SPI A to another SPI B, it needs to know the SPI pairs(for example, A and B is a SPI pair) in advance. Then, the functional component can map SPI A to SPI B or map SPI B to SPI A.

There are two solutions for the functional component to get the informaton of SPI pairs:

.Using one central controller to configurate the information about SPI pairs.

.Exchange the information about SPI pairs among functional components based on BGP.

4.2 Central controller based solution

When a central controller can exchange information with all functional components of the SFC that needs the information about the SPI paiirs, it is recommended to exchange information about SPI pairs based on the central controller.

In this mode, the information of SPI pairs can be encoded with other configuarion information and sent to those relevant functional components.

Many management protocol or mechanism such as SNMP and Netconf can be used to dispatch the configuration information.

4.3 BGP based solution

When there is not a proper central controller that can configurate the SPI pairs to all functional components of the SFC that needs the information about the SPI paiirs, it is better to use the BGP based method to exchange information about SPI pairs.

This section specifies how to use BGP extensions to exchange SPI pairs among functional components of the SFC.

One feasible solution is using ’BGP Extended Communities Attribute’ to envelop the inforamtion of SPI pairs. a new type of BGP extended community called SPI-Pairs Extended Community. It is a transitive extended community with type 0x01 and sub-type TBD.

The format of this extended community is shown in Figure 3.

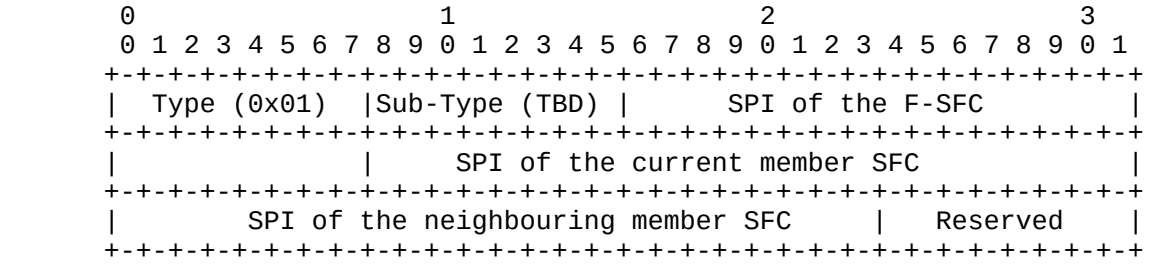


Figure 3. SPI-Pairs Extended Community

5. Actions for SFC components

Because some changes occur to the protocol, the processing actions of the functional components become different from the common SFC.

There are three aspects related to the afore-mentioned change of actions that need to be executed by the functional components. The following are those aspects.

. SPI mapping: two kinds of mapping are as follows:

. Mapping SPI of the F-SFC to SPI of a member SFC when a F-SFC packet enter the member SFC.(A10)

. Mapping SPI of a member SFC to SPI of the F-SFC when a F-SFC packet leave the member SFC and will enter another member SFC.(A11).

. F-SFC bit processing:

. Clearing F-SFC bit when a F-SFC packet enter the member SFC. (A20)

. Setting F-SFC bit when a F-SFC packet leave the member SFC and will enter another member SFC.(A11).(A21)

. SI processing:

. Re-initiate SI when a F-SFC packet enter the member SFC.(A30)

. Restore and re-calculate SI when a F-SFC packet leave the member SFC and will enter another member SFC.(A31)

. Decrementing the SI.(A32)

. Restore and re-calculate SI when a F-SFC packet leave the member SFC and will enter another member SFC.(A31)

. Decrementing the SI.(A32)

Figure 4 illustrates the actions possibly executed by the functional components of the member SFC.

Component	SPI processing	F-SFC bit processing	SI processing
Classifier	A10	A20	A30
Service Function Forwarder (SFF)	A10&A11	A20&A21	A30&A31
Service Function (SF)	-	-	A32
SFC Proxy	-	-	A30

Figure 4. Actions for SFC components related extended field for F-SFC

6. Transport layer envelopment for F-SFC

According to [RFC 8300], an outer transport encapsulation is used to forward the packet with a NSH header. And the service header is independent of the transport encapsulation used.

Because F-SFC is usually applied in cross-domain scenarios, the outer transport layer envelopment should meet the requirement that the packet with the outer transport layer envelopment can be exchange among the domains in which the member SFCs are deployed.

7. Some candidate mechanisms appropriate for fusing member SFCs

7.1 Overview of fusing member SFCs

For F-SFC, it is a critical issue to steering the packet from one member SFC to another member SFC. Because network traffic related to F-SFC needs to be forwarded domain by domain, problems

including security will be brought about when network traffic is transported from a domain to another domain.

Some mature technologies can help to steer network traffic domain by domain and avoid possible problems. the next two sections will introduce two candidate mechanisms that can be used for F-SFC. It is noted that the other feasible methods are also proper for F-SFC.

7.2 VPN

VPN (Virtual Private Network) is a good solution to connect different member SFCs when member SFCs are set up in different network domains. detailed information of VPN can be seen in [RFC 4110] and [RFC 4664].

For example, L2 VPN can provide two fundamentally different kinds of Layer 2 VPN service that a service provider could offer to a customer:

- Virtual Private Wire Service (VPWS).
- Virtual Private LAN Service (VPLS).

A VPWS is a VPN service that supplies an L2 point-to-point service. Then A VPWS is appropriate for F-SFC.

Figure 5 illustrate the scene that two member SFCs are connected by a VPN.

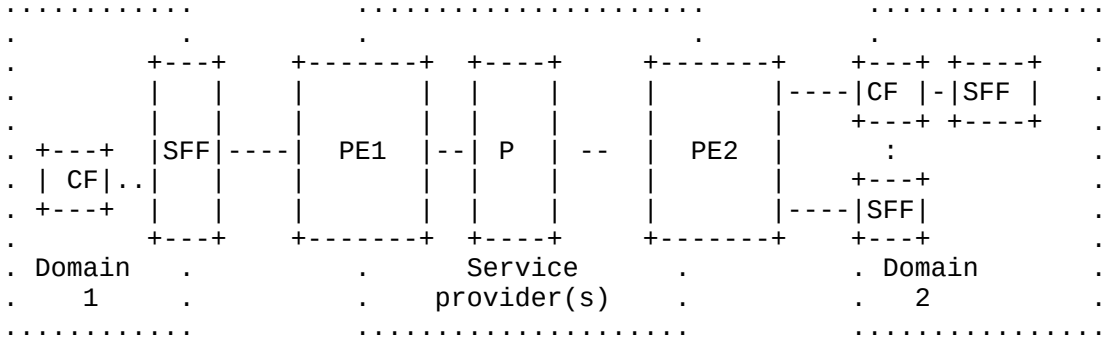


Figure 5. VPN connects two member SFCs

7.3 NVO3

Another example for mechanisms that can be used to connect two independent member SFCs is NVO3. and Figure 6 illustartes such a scene. Detail

description about NVO3 can be seen in [RFC 7365] and [RFC 8014].

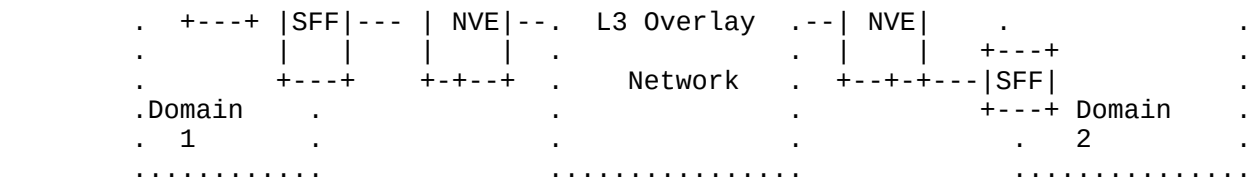


Figure 6. NVO3 connects two member SFCs

8. Extension for management/control plane

Functional components in a F-SFC are possibly deployed in different Domains, then multi-controllers are possibly needed, figure 7 depicts the logical structure for multi-controllers to cooperate in F-SFC context.

There is possibly a need for information to be exchanged among the controllers. It is a feasible solution to use BGP extensions to realize the information exchange functions.

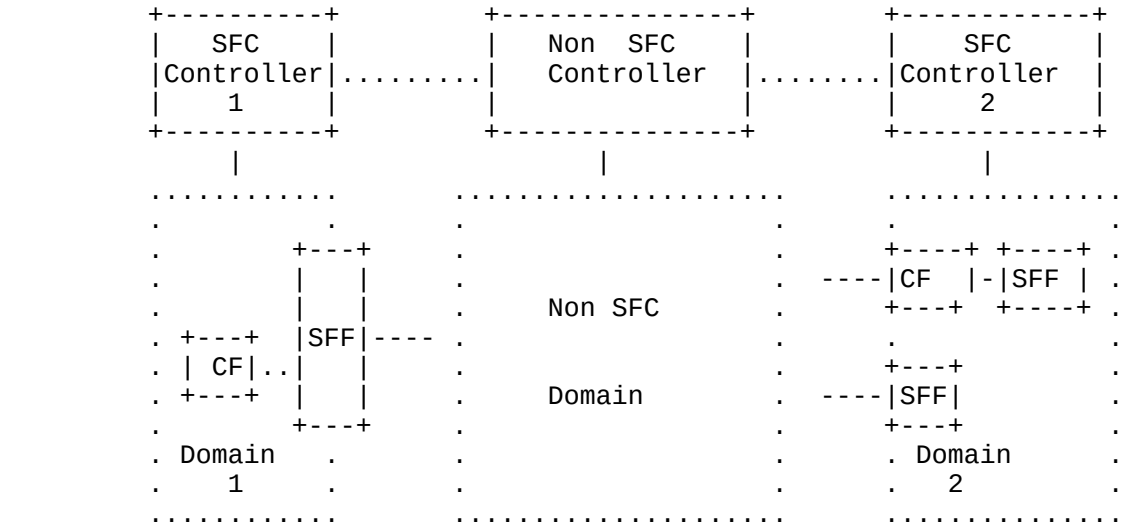


Figure 7. logical structure for multi-controllers in F-SFC

9. Security Considerations

The security considerations described throughout [RFC7665] and [RFC8300] apply here as well.

Additionally, when a data packet is forwarded from SFC(i) to SFC(i+1), the path between SFC(i) to SFC(i+1) should provide mechanism to guarantee security of the data packet.

Moreever, when the CF in SFC(i) is by-passed, it should be assured that the bu-passed path has the same security support as the CF.

10. IANA Considerations

The IANA is requested to make the assignments for SPI-Pairs Extended Community:

Value	Description	Reference
TBA1	IPv4-Address-Specific IFIT Tail Community	This document

11 Acknowledgements

This document is written by referring to [RFC7665] authored by J. Halpern and C, Pignataro and [RFC8924] authored by S. Aldrin, C. Pignataro, N. Kumar, R. Krishnan and A. Ghanwani.

Many thanks to all the afore-mentioned editors and authors.

12 References

12.1 Normative References

[RFC4360] S. Sangli, D. Tappan and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, February 2006.

[RFC4760] T. Bates, R. Chandra, D. Katz and Y. Rekhter, "Multiprotocol Extensions for BGP-4 ", RFC 4760, Jenuary 2007.

[RFC7665] J. Halpern and C. Pignataro, "Service Function Chaining (SFC) Architecture", RFC 7665, October 2015.

[RFC8300] P. Quinn, U. Elzur and C. Pignataro, "Network Service Header (NSH)", RFC 8300, January 2018.

[RFC8459] D. Dolson, S. Homma, D. Lopez and M. Boucadair "Hierarchical Service Function Chaining (hSFC)", RFC 8459, September 2018.

[RFC8924] S. Aldrin, C. Pignataro, N. Kumar, R. Krishnan and A. Ghanwani, "Service Function Chaining (SFC) Operations, Administration, and Maintenance (OAM) Framework", RFC 8924, October 2020.

12.2 Informative References

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

[RFC4110] R. Callon and M. Suzuki, "A Framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs)", RFC 4110, July 2005.

[RFC4664] L. Andersson and E. Rosen, "Framework for Layer 2 Virtual Private Networks (L2VPNs) ", RFC 4664, September 2006.

[RFC7365] M. Lasserre, T. Morin, N. Bitar and Y. Rekhter, "Framework for Data Center (DC) Network Virtualization ", RFC 7365, October 2014.

[RFC7498] P. Quinn and T. Nadeau, "Problem Statement for Service Function Chaining", RFC 7468, April 2015.

[RFC8014] D. Black, J. Hudson, L. Kreeger, M. Lasserre and T. Narten, "An Architecture for Data-Center Network Virtualization over Layer 3 (NVO3) ", RFC 8014, December 2016.

[RFC8393] A. Farrel and J. Drake, "Operating the Network Service Header (NSH) with Next Protocol ‘None’", RFC 8393, May 2018.

[I-D.ietf-sfc-multi-layer-oam] G. Mirsky, W. Meng, B. Khasnabish and C. Wang, "Active OAM for Service Function Chains in Networks", draft-ietf-sfc-multi-layer-oam-07, December 2020.

Authors’ Addresses

Jinyou Dai
China Information Communication Technologies Group.
Gaoxin 4th Road 6#
Wuhan, Hubei 430079
China

Email: djy@fiberhome.com

Shaohua Yu
Shaohua Yu
PCL., Nanshan
Shenzhen
China

Email: yush@cae.cn

Weiqiang Cheng
China Mobile
Email: chengweiqiang@chinamobile.com

Xueshun Wang
China Information Communication Technologies Group.
Gaoxin 4th Road 6#
Wuhan, Hubei 430079
China

Email: xswang@fiberhome.com

Dongping Deng
China Information Communication Technologies Group.
Gaoxin 4th Road 6#
Wuhan, Hubei 430079
China

Email: dzb@fiberhome.com