SFC transport consideration
draft-ao-sfc-transport-00

Abstract

A Network Service Header (NSH) is imposed encapsulates a packet or a frame for Service Function Chaining. The resulting packet, in turn, is encapsulate according to transport layer. The NSH contains a Service Path Identifier (SPI) and a Service Index (SI). The SPI is, as per its name, an identifier. The SPI alone cannot be used to forward packets along a service path. Rather, the SPI provides a level of indirection between the service path / topology and the network transport encapsulation. For different transport encapsulations, this document provides the format information with transport and NSH, and gives operational constraints that transport technologies, used by NSH need to meet.

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 https://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 April 23, 2019.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.
1. Introduction

For SFC using NSH, NSH is imposed on original packets/frames. NSH header format is defined in [RFC8300] as Figure 1. NSH is transport encapsulation agnostic, and SFC packet can’t be forwarded or transmitted along without the transport layer support. So how does the different transport technologies bear SFC service traffic is what is discussed in this document.
The NSH is composed of a 4-byte Base Header, a 4-byte Service Path Header, and optional Context Headers, as shown in Figure 2.

In the Base Header part, a Next Protocol field is provided to indicate the protocol type of the payload. The value definition is:

- 0x1: IPv4
- 0x2: IPv6
- 0x3: Ethernet
- 0x4: NSH
- 0x5: MPLS
- 0xFE: Experiment 1
- 0xFF: Experiment 2

This document describes SFC packet over different transport networks, and defines the format for NSH with these different transport networks.
protocol. For some situations, some operational constraints also described.

2. Conventions used in this document

2.1. Terminology

SFC(Service Function Chain): An ordered set of some abstract SFs.

SFF: Service Function Forwarder

SF: Service Function

NVE: Network Virtualization Edge

VXLAN-GPE: VXLAN Generic Protocol Extension

GENEVE: Generic Network Virtualization Encapsulation

GRE: Generic Routing Encapsulation

2.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Ethernet as transport

3.1. Format in encapsulation

In an Ethernet network, Ethernet is as transport for SFC traffic. The format for Ethernet to transport SFC packet should be as Figure 3.
3.2. Operation

1. The Classifier classifies the original packets according to its policies and attach the NSH header. If the network transport is Ethernet, before the Classifier forwards the packet, it adds a L2 Header as the outer header. In the outer L2 header, the source MAC address is the MAC address of the Classifier, and the destination MAC address is the MAC address of the first SFF.

For the VLAN ID in the L2 header, there should be a policy for impose a VLAN ID. If the original packet is IP Packet, the VLAN ID relies on the Service Function Path assigned to the packet which virtual network it belongs.

2. The SFF receives SFC packet from a network interface, checks the SPI and SI in the NSH-to-SF Mapping table, per [RFC8300], to get the locator of SF attached to it, that is MAC address if the transport is Ethernet. SFF modifies the L2 Header to be the destination MAC address is the SF MAC address, and the source MAC address is the MAC address of the SFF, and then forwards the SFC packet to the SF attached to this SFF. After the processing, the SF will decrement SI in the NSH by a value of 1, and will swap the source MAC address with the destination MAC address of the outer L2 Header, and then the SFC packet is forwarded back to the SFF. Once the SFF receives the SFC packet from SF interface, it will check the SPI and SI in the NSH-to-SF Mapping table again to get the locator of next SFF, that is MAC address of the next SFF if the transport is Ethernet. SFF should modify the L2 Header again to be the destination MAC address is the next SFF address, and the source MAC address is the MAC address of the SFF.

3. When the last SFF receive the SFC packet from the SF attaching to it, it will check the SPI and SI in the NSH-to-SF Mapping table, finding it’s the end of the Service Function Path, so it should strip
4. VXLAN-GPE as transport

4.1. Format in encapsulation

In an overlay network, VXLAN-GPE is as transport for SFC traffic. The format for VXLAN-GPE to transport SFC packet should be as Figure 4. Here assuming the overlay networks are built on Ethernet.

```
+----------+------------------------+---------------------+--------------+---------------------+
|L2 header | IP + UDP dst port=4790 | VXLAN-gpe NP=0x4(NSH)| NSH, NP=0x1   | original IPv4 packet |
+----------+------------------------+---------------------+--------------+---------------------+
VXLAN-GPE+ NSH IPv4 packet
```

```
+----------+------------------------+---------------------+--------------+---------------------+
|L2 header | IP + UDP dst port=4790 | VXLAN-gpe NP=0x4(NSH)| NSH, NP=0x3   | original L2 frame   |
+----------+------------------------+---------------------+--------------+---------------------+
VXLAN-GPE+ NSH L2 frame
```

Figure 4: NSH in VXLAN-GPE

4.2. Operation

1. The Classifier classifies the original packets according to the classify its policies and attaches the NSH header. If the network transport is VXLAN-GPE, before the Classifier forward the packet, it should add a VXLAN-GPE header first, and then UDP header and IP header. UDP destination port should be 4790 which means the traffic should send to NVE, which has been specified in [I-D.ietf-nvo3-vxlan-gpe]. The destination IP address should be the IP address of the NVE that the first SFF located. For the VNID in the VXLAN-GPE header, there should be a policy for impose a VNID. If the original frame has VLAN ID, there would be a mapping between VLAN ID and VNID.

2. The SFF receives SFC packet from network interface, remove the outer header and checks the SPI and SI in the NSH-to-SF Mapping table in [RFC8300] to get the locator of SF attaching to it. If the transport between the SFF and the SF attaching to the SFF is Ethernet, the locator of SF in the NSH-to-SF Mapping table should be MAC address. At this time, the SFC packet format from SFF to SF is as the Figure 3 shows. So the destination MAC address of the outer L2 header should be SF MAC address, and the source MAC address of the...
outer L2 header should be MAC address of the SFF. After the process, the SP will decrement SI in the NSH by a value of 1, and exchange the source MAC address and destination MAC address of the outer L2 header, and then the SFC packet is forwarded back to the SFF. Once the SFF receive the SFC packet from SF interface, it will check the SFI and SI in the NSH-to-SF Mapping table again to get the locator of next SFF, that is MAC address of the next SFF if the transport is Ethernet. SFF should modify the L2 Header again to be the destination MAC address is the next SFF address, and the source MAC address is the MAC address of the SFF.

3. When the last SFF receive the SFC packet from the SF attaching to it, it will check the SPI and SI in the NSH-to-SF Mapping table, finding it’s the end of the Service Function Path, so it should strip the outer L2 Header and NSH Header before it send out the original packet.

5. GRE as transport

5.1. Format in encapsulation

In an overlay network, GRE is as transport for SFC traffic. The format for GRE to transport SFC packet should be as Figure 5. Here assuming the overlay networks are built on Ethernet.

| L2 header | IP header, Proto=47 | GRE PT=NSH | NSH, NP=0x1 | original packet |
+-----------+---------------------+------------+-------------+----------------+
GRE+ NSH IPv4 packet

| L2 header | IP header, Proto=47 | GRE PT=NSH | NSH,NP=0x3 | original frame |
+-----------+---------------------+------------+-------------+----------------+
GRE+ NSH L2 frame

Figure 5: NSH in GRE

5.2. Operation

To support the encapsulation, a new value for Protocol Type in GRE is required.

Similar with VXLAN-GPE as transport. Will add later.
6. GENEVE as transport

6.1. Format in encapsulation

In an overlay network, GENEVE is as STANDARD transport technology. GENEVE also can be used as transport for SFC traffic. The format for GENEVE to transport SFC packet should be as Figure 6. Here assuming the overlay networks are built on Ethernet.

|L2 header| IP + UDP dst port=6081 |GENEVE PT=NSH |NSH, NP=0x1 |original packet |
+----------+------------------------+------------------------+--------------+----------------+
GRE+ NSH IPv4 packet

|L2 header| IP + UDP dst port=6081 |GENEVE PT=NSH |NSH,NP=0x3 |original frame |
+----------+------------------------+------------------------+--------------+----------------+
GRE+ NSH L2 frame

Figure 6: NSH in GENEVE

6.2. Operation

To support the encapsulation, a new value for Protocol Type in GENEVE is required.

Similar with operation in VXLAN-GPE transport. Details will be added later.

7. Security Considerations

TBD.

8. IANA Considerations

TBD.

9. Acknowledgements

TBD.

10. References
10.1. Normative References

[I-D.ietf-nvo3-geneve]

[I-D.ietf-nvo3-vxlan-gpe]


10.2. Informational References


Authors’ Addresses
Ting Ao  
ZTE Corporation  
No.889, BiBo Road  
Shanghai  201203  
China  
Phone: +86 21 68897642  
Email: ao.ting@zte.com.cn

Wei Wei  
ZTE Corp.  
No.50, Ruanjian Avenue  
Nanjing  
China  
Email: wei.wei@zte.com.cn

Yan Zheng  
ZTE Corp.  
No.50, Ruanjian Avenue  
Nanjing  
China  
Email: zheng.yan@zte.com.cn