Network Service Header TLVs
draft-quinn-sfc-nsh-tlv-01.txt

Abstract

This draft describes Network Service Header (NSH) MD-Type 2 metadata TLVs that can be used within a service function path.

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 October 17, 2016.

Copyright Notice

Copyright (c) 2016 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 ................................................. 3
2. NSH Type 2 Format ........................................... 4
3. NSH Type 2 TLVs ............................................... 5
4. Security Considerations ................................. 10
5. Acknowledgments ............................................. 11
6. IANA Considerations ........................................ 12
7. References ..................................................... 13
   7.1. Normative References ................................. 13
   7.2. Informative References ............................... 13
Authors’ Addresses ............................................ 14
1. Introduction

Network Service Header NSH [NSH] is the SFC encapsulation protocol used to create Service Function Chains. As such, NSH provides two key elements:

1. Service Function Path identification

2. Metadata

NSH further defines two metadata formats (MD Types): 1 and 2. MD Type 1 defines fixed length, 16 byte metadata, whereas MD Type 2 defines a variable-length TLV format for metadata. This draft defines some common TLVs for use with NSH MD Type 2.

This draft does not address metadata usage, updating/chaining of metadata or other SFP functions. Those topics are described in NSH.
2. NSH Type 2 Format

A NSH is composed of a 4-byte Base Header, a 4-byte Service Path Header and Context Headers. The Base Header identifies the MD-Type in use:

```
+---------------------------------+   Length  |    MD Type    | Next Protocol |
+---------------------------------+            |              |               |
```

Figure 1: NSH Base Header

Please refer to NSH [NSH] for a detailed header description.

When the base header specifies MD Type= 0x2, zero or more Variable Length Context Headers MAY be added, immediately following the Service Path Header. Therefore, Length = 0x2, indicates that only the Base Header followed by the Service Path Header are present. The number, indicated in the length field, of optional Variable Length Context Headers MUST be of an integer indicating length in 4-bytes words Figure 3 below depicts the format the context header.

```
+---------------------------------+          |    Type     |R|R|   Len   |
+---------------------------------+            |              |            |
|                      Variable Metadata                        |
+---------------------------------+          |              |            |
```

Figure 2: NSH TLV Format
3. NSH Type 2 TLVs

As per NSH, TLV Class 0-7 are reserved for standards use. In this draft we use TLV Class 0 for the following Types:

```
+----------------+-----------------+-----------------+-----------------+-----------------+-----------------+
| TLV Class = 0x0 | C |    Type   | R | R | R |   Len  |
|----------------+-----------------+-----------------+-----------------+-----------------+
| Variable Metadata |
|-----------------+
```

Figure 3: NSH TLV Class=0x0

1. Forwarding Context

This TLV carries network-centric forwarding context, used for segregation and forwarding scope. Forwarding context can take several forms depending on the network environment. Commonly used data includes VXLAN/VXLAN- GPE VNID, MPLS VPN label values or VLAN.

```
+----------------+-----------------+-----------------+-----------------+-----------------+-----------------+
| TLV Class = 0x0 | C |    Type   | R | R | R |   Len  |
|----------------+-----------------+-----------------+-----------------+-----------------+-----------------+
| Context Type (CT), 4 bits: |
| 0x0: 24 bit VXLAN/LISP virtual network identifier (VNI) |
| 0x1: 32 bit MPLS VPN label |
| 0x2: VLAN |
```

Figure 4: Forwarding Context

2. Subscriber/user Information

Subscriber information varies in both format and source depending on network environment. A commonly used example is PCRF information in mobile deployments. Considerations for usage of this TLV are addressed in [subhost].
3. Host Identifier

Host Identifier (ID) varies based on the type of host ID being conveyed. A common example is a host IP address. Guidelines for host ID usage in a network are discussed in [subhost].

4. Tenant

Tenant identification is often used for segregation within a multi-tenant environment. Orchestration system generated tenant IDs are an example of such data.
Tenant Type (TT), 4 bits:
0x0: 32 bit
0x1: 64 bit

Figure 7: Tenant Identifier

5. Application ID

Application identification may be used for SF policy enforcement. [NSH AppID] provides guidelines and examples of such data.

Figure 8: Application ID

6. Content Type

Provides explicit information about the content being carried, for example, type of video or content value for billing purposes

Figure 9: Content Type

7. Ingress Network Information

This data identifies ingress network node, and, if required,
ingress interface.

Figure 10: Ingress Network Info

8. Flow ID

Flow ID provides a representation of flow. Akin, but not identical to the usage described in [RFC6437]

Figure 11: Flow ID

9. Source and/or Destination Groups

Intent-based systems can use this data to express the logical grouping of source and/or destination objects. [GROUPBASEDPOLICY] and [GROUPPOLICY] provide examples of such a system.

Figure 12: End Point Group

Group type (4):
0x1: Group Based Policy (GBP) end point group (EPG)
10. Universal Resource Identifier (URI)

URI type (4):
0x1: URI in standard string format as defined in RFC 3986
0x2: URI represented in a compacted hash format

Figure 13: URI
4. Security Considerations

NSH describes the requisite security considerations for protecting NSH metadata.
5. Acknowledgments

The authors would like to thank Behcet Sarikaya, Dirk von Hugo and Mohamed Boucadair for their work regarding usage of subscriber and host information TLVs.
6. IANA Considerations

IANA is requested to create a new "Network Service Header (NSH) TLV Type" registry. TLV types 0-127 are specified in this document. New values are assigned via Standards Action [RFC5226].
7. References

7.1. Normative References

7.2. Informative References

[GROUPBASEDPOLICY]
OpenStack, "Group Based Policy", 2014.

[GROUPPOLICY]

[NSH]

[NSH AppID]

[RFC5226]

[RFC6437]

[subhost]
Authors’ Addresses

Paul Quinn
Cisco Systems, Inc.

Email: paulq@cisco.com

Uri Elzur
Intel

Email: uri.elzur@intel.com

Sumandra Majee
F5

Email: S.Majee@F5.com

Joel Halpern
Ericsson

Email: joel.halpern@ericsson.com