Network Working Group B. Sarikaya
Internet-Draft Huawei
Intended status: Informational M. Boucadair
Expires: July 16, 2017 Orange
D. von Hugo
Telekom Innovation Laboratories
January 12, 2017

Service Function Chaining Metadata Type 1 and Type 2
draft-sarikaya-sfc-metadatat1t2-02.txt

Abstract

With the definition of service function chain data plane protocol there comes the need to define the context data needed in the service function chain use cases. This document gives an account of all context data defined so far as Network Service Header metadata Type 1 and Type 2 context headers. Next, the document discusses the various options that can be taken in standardizing service function chain metadata.

Table of Contents

1. Introduction

Network Service Header (NSH) [I-D.ietf-sfc-nsh] is the Service Function Chaining (SFC) data plane protocol. The SFC architecture is defined in [RFC7665].

NSH has the function of carrying context data in the form of context header. NSH metadata Type 1 is composed of a 4-byte base header, 4-byte service path header. It contains four mandatory Context Headers, 4-byte each which can be combined into one context header of 16 octets in the latest version. For additional metadata that needs to be carried, NSH metadata type 2 is defined. Type 2 metadata is composed of a 4-byte base header carrying Type value of 0x02, 4-byte service path header followed by variable length context headers in the form of metadata class type-length-value or TLV.

Optional variable length metadata definition includes 16-bit metadata class and 7-bit type fields. It is an issue if such a long metadata class field is needed and whether the type field length should be increased.

Many context headers were proposed by many documents. In this document we survey existing drafts that propose new context metadata and then discuss different options that can be taken to standardize this work.

The reader should be familiar with the terms defined in [RFC7665] and [I-D.ietf-sfc-nsh].

2. Context Metadata Definitions

[I-D.guichard-sfc-nsh-dc-allocation] addresses metadata allocation that seems to be relevant when NSH is used for SFC within a data center. The use cases that demonstrate the applicability of SFC within a data center environment are described in [I-D.ietf-sfc-dc-use-cases].

This document defines meta data Type 1 for several IDs of Source Node, Source Interface and Tenant. It defines destination and source class to classify the destination and source of the traffic for the purposes of applying policy. It defines Opaque Service Class in the 4th word.

[I-D.napper-sfc-nsh-broadband-allocation] supports use cases in [I-D.ietf-sfc-use-case-mobility].

This document defines meta data Type 1 with endpoint ID, e.g. for IMSI or MSISDN or wireline subscriber ID with 64-bit length. It also defines ServiceTag to identify that the Service Information field contains information related to the Access Network (AN) for the subscriber. Service information could contain IP-CAN type, QoS class, congestion level, etc. for a 3GPP Radio Access Network (RAN). Context ID field allows the subscriber/endpoint ID field to be scoped. Context ID contains the incoming VRF, VxLAN VNID, VLAN, or policy identifier within which the Subscriber/Endpoint ID field is defined.

In addition, the document defines a meta data Type 2 TLV to be associated with 3GPP registry. The intent here is to offer this TLV for the use of 3GPP to extend the meta data to meet the needs of 3GPP use cases. However, it was not stated if 3GPP requested such an allocation.

[I-D.wang-sfc-nsh-ns-allocation] addresses the use cases for network security defined in [I-D.wang-sfc-ns-use-cases].

It defines a recommended security context allocation as a meta data Type 1 TLV. It is intended to define session ID, tenant ID, destination/ source class for the logical classification of the destination/ source of the traffic, destination/ source score which contains security classification results for communicating immediate actions and accumulated verdicts to downstream Service Functions.

[I-D.wang-sfc-nsh-ns-allocation] also mentions that the security context allocation, although defined as Type 1, it may also form a MD-Type 2 metadata TLV, possibly implying that the sizes of data such as session/ tenant ID, etc. may need to become longer. As a result,

they may need to become variable length data as in Type 2 meta data TLVs. This document defines network security allocation specifics, basically explaining the semantics of the metadata they define in the document.

[I-D.meng-sfc-nsh-broadband-allocation] defines Type 1 metadata called Broadband Context Allocation support service function chaining in a broadband service provider network. It defines Source Node, Source Interface, User and VLAN IDs.

[I-D.sarikaya-sfc-hostid-serviceheader] addresses use cases that require revealing host and/ or subscriber related information to upstream SFs as well as extreme low latency service and ultra-high reliability applications use cases.

From the analysed use cases, there comes the need to come up with definition of host, subscriber, slice identifier and service identifier SFC meta data Type 2 TLVs. Apart from defining these TLVs, the document gives details of post processing in various nodes such as ingress/egress border nodes, SFC-aware Service Functions and Proxies. Such post processing is defined as normative behavior. Since host and subscriber identifiers may reveal private information about the host and/or the subscriber, the document also defines normative behavior needed to protect the privacy of the hosts and subscribers in an operator network.

[I-D.sarikaya-sfc-hostid-serviceheader] is unique among the documents discussed in this document because it defines the post processing normative behavior related to the host and subscriber identifier meta data Type 2 TLVs. Also the use cases are defined in the same document not as a separate document as in the other cases.

[I-D.browne-sfc-nsh-kpi-stamp] addresses monitoring and debugging service chains in terms of application latency and QoS configuration of the flows within a service chain. For that purpose, it introduces key performance indicator (KPI) stamping architecture and several metadata Type 2 meta data.

Different from other documents maybe except [I-D.quinn-sfc-nsh-tlv], this document makes full use of metadata Type 2 with Metadata Class and Type fields as in [I-D.ietf-sfc-nsh]. One new MD Class called KPI General Monitoring, stamping types and QoS types, in short KPI is introduced. With this, the document introduces many new Types such as KPI stamping detection, or TSD mode, generic KPI encapsulation or KPI mode, timestamping encapsulation or TS mode, Quality of Service configuration encapsulation or QoS mode. QoS mode encapsulation enables definition of one or more QoS stamps containing QoS Type (QT)

and QoS value fields and an E bit to indicate the last egress QoS stamp for a given SF.

The new MD Class is used in defining several new metadata Type 2 in the document: Generic NSH KPI Encapsulation (Detection Mode), Generic KPI Encapsulation (Extended Mode), NSH Timestamp Encapsulation (Extended Mode), NSH QoS Configuration Encapsulation (Extended Mode). TSD is proposed to use for KPI anomaly detection. KPI is proposed to use for performance monitoring of service chain issues with respect to QoS configuration and latency. The type TS is proposed for timestamping. The type QoS is proposed for QoS stamping.

[I-D.penno-sfc-packet] addresses the problem of sending packets in the reverse direction to the source of the current in-process packet/ flow. It defines SF Reverse Packet Request as Type 1 metadata. This is defined as Version 1 (as opposed to Version 0 of NSH MD-type 1 in [I-D.ietf-sfc-nsh]) with OAM Protocol replacing the next protocol field and with Reverse Packet Request added to the end of mandatory context header octets for SFC as an additional 4-octet for OAM.

This document also proposes 5 new metadata on service-path invariants, service-path default, bidirectional clonable, unidirectional clonable and service-function-mastered metadata. Their structure specifics are not specified.

[I-D.penno-sfc-packet] gives a detailed explaination of the use of the metadata defined, all the semantic information, pre and post processing details at various nodes.

[I-D.quinn-sfc-nsh-tlv] defines NSH metadata Type 2 TLVs such as forwarding context, subscriber/user info, tenant, application ID, content type, ingress network information, flow ID, source and/or destination groups, universal resource identifier (URI). This document defines Metadata Class value of 0x0. Also each TLV defined is given a Type value starting with 0x1.

Some of these TLVs are defined in other documents, like App ID, Context ID in [I-D.napper-sfc-nsh-broadband-allocation]. Also for Application ID, even though the document references [I-D.penno-sfc-appid], [I-D.penno-sfc-appid] seems to mean Classification Engine ID and Selector ID for the Application ID.

The purpose of [I-D.quinn-sfc-nsh-tlv] is to document syntactic structure of the TLVs for the purpose of setting up a registry of Type 2 metadata. No other additional information about the metadata processing is within the scope of this document. The document mentions no use cases in which the TLVs defined are needed. An implementer will need to refer to other documents to understand the

exact behavior for handling those contexts. This document does not define the normative behavior for processing the defined TLVs. This is key for interoperability.

[I-D.vallamkonda-sfc-metadata-model] does not define any Type 1 or Type 2 meta data TLVs, viewing such meta data as conveying preprocessing information about the packet, this document attempts to formally define the post processing information. To that end, it defines a vocabulary and information model for metadata. The document gives metadata information model example definitions for routing domain, IP endpoint, flow and traffic policy indication.

3. Processing Metadata Type 1 and Type 2

Some options are discussed below for processing NSH meta data:

1. List the structure of meta data in one single document as a registry. The document is not supposed to contain any post processing information. [I-D.quinn-sfc-nsh-tlv] attempts this choice for some Type 2 meta data. Currently there is no such document for Type 1 meta data. Note that in the case of keeping a registry document, it is not clear how the post processing behavior (normative or optional) will be specified for the meta data. One option is to keep such information in separate document(s). If such a strategy is adopted then the advantages obtained from documenting all TLVs in one document disappear because the implementers would need to consult many documents instead of only one.

2. All documents defining new meta data Type 1 and Type 2 meta data are treated individually for standardization. This approach has the advantage of keeping all meta data Type 1 and Type 2 meta data in separate and dedicated documents together with all the information that the implementers may need. This could be a strong positive especially if we consider the fact that the meta data are being defined for very many use cases and scenarios. It is unlikely that one implementer would need to implement a large number of these TLVs, thereby defeating the need for combining them in a single document.

3. Together with choice 1 above, while combining all meta data in one document, it could be possible to keep post processing information related to the meta data in separate documents which can be considered individually for standardization.

4. Together with choice 2 above, Type 1 meta data can be combined in one document but all Type 2 meta data can be considered individually in separate dedicated documents.

A document intended to keep a registry of all meta data can be an informational document. Companion documents defining semantics of Type 1 and Type 2 metadata needs to be standard track in order to take the recommendations on processing the data into effect.

Another issue is the importance of Type 1 metadata and Type 2 metadata. It seems to be difficult to argue that Type 1 metadata is more important. The metadata defined in [I-D.wang-sfc-nsh-ns-allocation] is a good example as it can be defined either as Type 1 or Type 2. The same considerations could possibly be made for other documents.

It is recommended that the metadata defined be given serious consideration as to the merit of the use case that needs the metadata to the Service Function Chaining rather than syntactic considerations of Type 1 or Type 2.

4. IANA Considerations

None.

5. Security Considerations

This document does not introduce any security issues.

6. Acknowledgements

TBD.

7. References

7.1. Normative References

[I-D.ietf-sfc-nsh]
Quinn, P. and U. Elzur, "Network Service Header", draft-ietf-sfc-nsh-10 (work in progress), September 2016.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <http://www.rfc-editor.org/info/rfc7665>.

7.2. Informative References

[I-D.browne-sfc-nsh-kpi-stamp]
Browne, R., Chilikin, A., and T. Mizrahi, "Network Service Header KPI Stamping", draft-browne-sfc-nsh-kpi-stamp-00 (work in progress), October 2016.

[I-D.guichard-sfc-nsh-dc-allocation]
Guichard, J., Smith, M., Surendra, S., Majee, S., Agarwal, P., Glavin, K., and Y. Laribi, "Network Service Header (NSH) Context Header Allocation (Data Center)", draft-guichard-sfc-nsh-dc-allocation-05 (work in progress), August 2016.

[I-D.ietf-sfc-dc-use-cases]
Surendra, S., Tufail, M., Majee, S., Captari, C., and S. Homma, "Service Function Chaining Use Cases In Data Centers", draft-ietf-sfc-dc-use-cases-05 (work in progress), August 2016.

[I-D.ietf-sfc-use-case-mobility]
Haeffner, W., Napper, J., Stiemerling, M., Lopez, D., and J. Uttaro, "Service Function Chaining Use Cases in Mobile Networks", draft-ietf-sfc-use-case-mobility-07 (work in progress), October 2016.

[I-D.liu-sfc-use-cases]
Will, W., Li, H., Huang, O., Boucadair, M., Leymann, N., Qiao, F., Qiong, Q., Pham, C., Huang, C., Zhu, J., and P. He, "Service Function Chaining (SFC) General Use Cases", draft-liu-sfc-use-cases-08 (work in progress), September 2014.

[I-D.meng-sfc-nsh-broadband-allocation]
Meng, W. and C. Wang, "NSH Context Header - Broadband", draft-meng-sfc-nsh-broadband-allocation-01 (work in progress), May 2016.

[I-D.napper-sfc-nsh-broadband-allocation]
Napper, J., Surendra, S., Muley, P., and W. Henderickx, "NSH Context Header Allocation -- Broadband", draft-napper-sfc-nsh-broadband-allocation-01 (work in progress), October 2016.

[I-D.penno-sfc-appid]
Penno, R., Claise, B., Pignataro, C., and C. Fontaine, "Using Application Identification in Services Function Chaining Metadata", draft-penno-sfc-appid-05 (work in progress), August 2016.

[I-D.penno-sfc-packet]
Penno, R., Pignataro, C., Yen, C., Wang, E., Leung, K., and D. Dolson, "Packet Generation in Service Function Chains", draft-penno-sfc-packet-03 (work in progress), April 2016.

[I-D.quinn-sfc-nsh-tlv]
Quinn, P., Elzur, U., Majee, S., and J. Halpern, "Network Service Header TLVs", draft-quinn-sfc-nsh-tlv-02 (work in progress), October 2016.

[I-D.sarikaya-sfc-hostid-serviceheader]
Boucadair, M., Hugo, D., and B. Sarikaya, "Service Function Chaining Service, Subscriber and Host Identification Use Cases and Metadata", draft-sarikaya-sfc-hostid-serviceheader-03 (work in progress), July 2016.

[I-D.vallamkonda-sfc-metadata-model]
sunilvk@f5.com, s., Dunbar, L., and D. Dolson, "A Framework for SFC Metadata", draft-vallamkonda-sfc-metadata-model-01 (work in progress), July 2016.

[I-D.wang-sfc-ns-use-cases]
Wang, E., Leung, K., Felix, J., and J. Iyer, "Service Function Chaining Use Cases for Network Security", draft-wang-sfc-ns-use-cases-02 (work in progress), October 2016.

[I-D.wang-sfc-nsh-ns-allocation]
Wang, E., Leung, K., and A. Ossipov, "Network Service Header (NSH) Context Header Allocation (Network Security)", draft-wang-sfc-nsh-ns-allocation-02 (work in progress), November 2016.

Authors' Addresses

Behcet Sarikaya
Huawei
5340 Legacy Dr.
Plano, TX 75024

Email: sarikaya@ieee.org

Mohamed Boucadair
Orange
Rennes 3500, France

Email: mohamed.boucadair@orange.com

Dirk von Hugo
Telekom Innovation Laboratories
Deutsche-Telekom-Allee 7
D-64295 Darmstadt
Germany

Email: Dirk.von-Hugo@telekom.de