

Service Function Chaining
Internet-Draft
Intended status: Informational
Expires: February 19, 2018

J. Guichard
Huawei
M. Smith
S. Kumar
Cisco Systems, Inc.
S. Majee
F5 Networks
P. Agarwal
Broadcom
K. Glavin
Riverbed
Y. Laribi
Citrix
T. Mizrahi
Marvell
August 18, 2017

Network Service Header (NSH) MD Type 1: Context Header Allocation (Data
Center)
[draft-guichard-sfc-nsh-dc-allocation-07](#)

Abstract

This document provides a recommended default allocation for the Network Service Header (NSH) MD Type 1 fixed length context header when NSH is used for Service Function Chaining within a data center.

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 February 19, 2018.

Copyright Notice

Copyright (c) 2017 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	2
1.1.	Requirements Language	3
2.	Definition Of Terms	3
3.	Recommended Data Center MD Type 1 Fixed Length Context Allocation	3
3.1.	Data Center Allocation Specifics	3
4.	Context Allocation and Control Plane Considerations	5
5.	Security Considerations	6
6.	Acknowledgments	6
7.	IANA Considerations	6
8.	References	6
8.1.	Normative References	6
8.2.	Informative References	7
	Authors' Addresses	8

[1.](#) Introduction

Network Service Header (NSH) [[I-D.ietf-sfc-nsh](#)] provides a mechanism to carry shared metadata between network devices and service functions, and between service functions. When MD Type 1 is used, such metadata is carried within a fixed length (16-bytes) context header.

This document provides a recommended default allocation of the MD Type 1 context header for Service Function Chaining [[RFC7665](#)] within a data center. The context header may be used to support use cases such as those described in [[I-D.ietf-sfc-dc-use-cases](#)].

The goal of this document is to provide a reference allocation that may be used with or without a control plane. It also serves as a guide to implementers and network operators.

1.1. Requirements Language

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. Definition Of Terms

This document uses the terms as defined in [[RFC7498](#)], [[RFC7665](#)], and [[I-D.ietf-sfc-nsh](#)] .

3. Recommended Data Center MD Type 1 Fixed Length Context Allocation

The following context header allocation provides information used to support SFC operation within a generic data center environment. [[I-D.ietf-sfc-dc-use-cases](#)] provides an overview of data center use cases to support the allocation.

The 16 bytes of Fixed Length Context Header is delivered to service functions that may then use the metadata it carries for local policy enforcement and other functionality.

```

 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|D| F |R|      Source Node ID      |      Source Interface ID      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Reserved      |      Tenant ID      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Destination Class / Reserved |      Source Class      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      Opaque Service Class      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Figure 1: NSH DC Context Allocation

3.1. Data Center Allocation Specifics

The specific 16 byte allocation of the Fixed Length Context Header is as follows:

Flag bits: Bits 0-3 are flag bits. Bits 0-2 are defined in this document and the remaining bit is reserved.

D bit: The D-bit is used to indicate whether the Destination Class field in the 3rd word is used. If D-bit is not set then the field is reserved.

F bits: Two-bit value that indicates the format of the Opaque Service Class in the 4th word.

Source Node ID: An identifier indicating the source device where the original traffic initially entered the Service Function Chain. This identifier is unique within an SFC-enabled domain.

Source Interface ID: An identifier indicating the source interface where the original traffic initially entered the Service Function Chain. This identifier is scoped within the context of the Source Node ID.

Tenant ID: The tenant identifier is used to represent the tenant that the Service Function Chain is being applied to. The Tenant ID is a unique value assigned by a control plane. The distribution of Tenant ID's is outside the scope of this document. As an example application of this field, hardware may insert a VRF ID, VLAN number or VXLAN VNI.

Destination Class: The destination class represents the logical classification of the destination of the traffic. This field is optional and/or the Destination Class may not be known. The D-bit is used to indicate that this field contains a valid Destination Class.

Source Class: represents the logical classification of the source of the traffic. For example, this might represent a source application, a group of like endpoints, or a set of users originating the traffic. This grouping is done for the purposes of applying policy. Policy is applied to groups rather than individual endpoints.

Opaque Service Class: A unique identifier that can carry metadata specific to a Rendered Service Path, the format of which is specified by the value of the F-bits as follows:

00: If the F-bits are not set, then the Opaque Service Class field is not specified and can be used as determined by the control plane.

01 (ServiceTag): a ServiceTag is used to identify a particular flow, transaction or an application message unit. The ServiceTag may be used to augment the source and/or destination class. A ServiceTag is a unique identifier that can be used to enable functionality such as classification bypass, slow path skipping and flow programming. As part of the ServiceTag word, bit 0 is

the A bit and is used, when needed, to indicate acknowledgement of a ServiceTag by a Service Function.

02 (Application ID): contains an application identification as described in [\[RFC6759\]](#), and [\[I-D.penno-sfc-appid\]](#)

03 (Timestamp): indicates the time at which the packet was received by the Classifier.

The Timestamp has two possible formats:

- * A 32-bit nanosecond field (Figure 2), which uses the 32 least significant bits of the IEEE 1588 [\[IEEE1588\]](#) timestamp format.
- * The NTP [\[RFC5905\]](#) 32-bit Timestamp format (Figure 3), which is one of the recommended timestamp formats in [\[I-D.mizrahi-intarea-packet-timestamps\]](#).

It is assumed that in a given administrative domain only one of the formats will be used, and that the control plane determines which timestamp format is used.

The two timestamp formats are illustrated in the following figures.

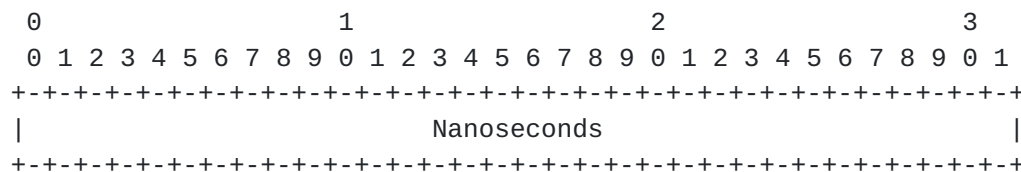


Figure 2: 32-bit Timestamp Format based on PTP [\[IEEE1588\]](#)

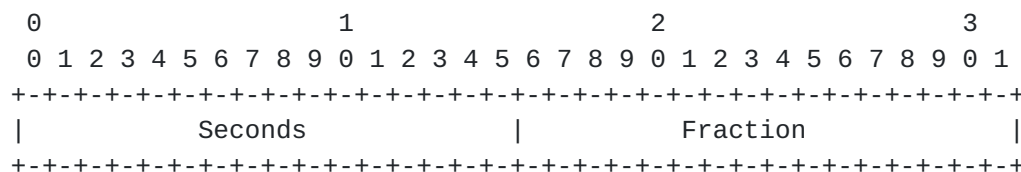


Figure 3: NTP [\[RFC5905\]](#) 32-bit Timestamp Format

[4.](#) Context Allocation and Control Plane Considerations

The context header allocations specified in this document are one of many possible allocation schemes and should be used as a guideline only; that is to say these allocations may vary based upon deployment

specifics and use cases. The suggested allocation is valid with or without a control plane but the semantics of context values MUST be shared amongst participating nodes via some mechanism. The actual method of defining and distributing the allocation scheme is outside of the scope of this document.

5. Security Considerations

This document describes an allocation scheme for the metadata carried within the NSH Fixed Length Context Header. This allocation includes a number of identifiers that must be distributed to participating network elements. While the control plane protocols for distributing these identifiers is outside the scope of this document, any control plane protocol should ensure that these identifiers are securely distributed to the network elements participating in the SFC.

Additionally, many of the fields such as Source and Destination Class described in the metadata directly impact the network policy applied to the traffic flowing through the SFC. There is a risk that these identifiers may be spoofed and proper precautions should be put in place to ensure that these fields can only be updated by trusted entities. Due to the importance of these fields, confidentiality may also be required to ensure that traffic cannot be targeted for attack based on the policy identifiers. This document does not directly address these threats but provides input to the NSH specification as requirements to be considered in securing the contents of the metadata.

6. Acknowledgments

The authors would like to thank Mohamed Boucadair for his helpful review and comments.

7. IANA Considerations

This document includes no request to IANA.

8. References

8.1. Normative References

[I-D.ietf-sfc-nsh]

Quinn, P., Elzur, U., and C. Pignataro, "Network Service Header (NSH)", [draft-ietf-sfc-nsh-19](#) (work in progress), August 2017.

[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.

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

[RFC6759] Claise, B., Aitken, P., and N. Ben-Dvora, "Cisco Systems Export of Application Information in IP Flow Information Export (IPFIX)", [RFC 6759](#), DOI 10.17487/RFC6759, November 2012, <<https://www.rfc-editor.org/info/rfc6759>>.

[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>>.

8.2. Informative References

[I-D.ietf-sfc-dc-use-cases]

Kumar, S., Tufail, M., Majee, S., Captari, C., and S. Homma, "Service Function Chaining Use Cases In Data Centers", [draft-ietf-sfc-dc-use-cases-06](#) (work in progress), February 2017.

[I-D.mizrahi-intarea-packet-timestamps]

Mizrahi, T., Fabini, J., and A. Morton, "Guidelines for Defining Packet Timestamps", [draft-mizrahi-intarea-packet-timestamps-00](#) (work in progress), June 2017.

[IEEE1588]

IEEE, "IEEE 1588 Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems Version 2", 2008.

[RFC5905] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, "Network Time Protocol Version 4: Protocol and Algorithms Specification", [RFC 5905](#), DOI 10.17487/RFC5905, June 2010, <<https://www.rfc-editor.org/info/rfc5905>>.

[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>>.

Authors' Addresses

Jim Guichard
Huawei

Email: james.n.guichard@huawei.com

Michael Smith
Cisco Systems, Inc.

Email: michsmit@cisco.com

Surendra Kumar
Cisco Systems, Inc.

Email: smkumar@cisco.com

Sumandra Majee
F5 Networks
90 Rio Robles
San Jose, CA 95134

Email: S.Majee@f5.com

Puneet Agarwal
Broadcom

Email: pagarwal@broadcom.com

Kevin Glavin
Riverbed

Email: Kevin.Glavin@riverbed.com

Youcef Laribi
Citrix

Email: Youcef.Laribi@citrix.com

Tal Mizrahi
Marvell

Email: talmi@marvell.com