SFC
Internet-Draft
Intended status: Standards Track
Expires: April 19, 2019

B. Sarikaya
Denpel Informatique
M. Boucadair
Orange
D. von Hugo
Deutsche Telekom

October 16, 2018

Service Function Chaining: Subscriber and Policy Identification Variable-Length Network Service Header (NSH) Context Headers
draft-sfc-serviceid-header-01

Abstract

This document discusses how to inform Service Functions about subscriber- and service-related information for the sake of policy enforcement and appropriate service function chaining operations.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document discusses how to inform Service Functions (SFs) about subscriber- and service-related information when required for the sake of policy enforcement within a single administrative domain. Particularly, subscriber-related information may be required to enforce subscriber-specific SFC-based traffic forwarding policies. Nevertheless, the information carried in packets may not be sufficient to unambiguously identify a subscriber. This document fills this void by specifying a new Network Service Header (NSH) [RFC8300] context header to convey and disseminate such information.

Also, the enforcement of SFC-based differentiated traffic forwarding policies may be inferred by QoS considerations. Typically, QoS information may serve as an input to classification of the Service Function Path (SFP) for path computation, establishment, and selection. Furthermore, the dynamic structuring of service function chains and their subsequent enforcement may be conditioned by QoS requirements that will affect SF instance identification, location, and sequencing. Hence, the need to supply a policy identifier to upstream SFs to appropriately meet the service requirements.

SFs and SF Forwarders (SFFs) involved in a service chain have to contribute to the respective service policy (QoS, for example) requirements characterized by low transmission delay between each other, by exposing a high availability of resources to process function tasks, or by redundancy provided by stand-by machines for seamless execution continuation in case of failures. These requirements may be satisfied by means of control protocols, but in some contexts, (e.g., in networks where resources are very much constrained), carrying QoS-related information directly in packets

may improve the overall SFC operation instead of relying upon the potential complexity or adding overhead introduced by some SFC control plane features. This information is typically included as metadata in the NSH as the SFC encapsulation to provide the SFP identification.

The context information defined in this document can be applicable in the context of mobile networks (typically, in the 3GPP defined (S)Gi Interface) [I-D.ietf-sfc-use-case-mobility]. Because of the widespread use of private addressing in those networks, if SFs to be invoked are located after a NAT function (that can reside in the Packet Data Network (PDN) Gateway (PGW) or in a distinct node), the identification based on the internal IP address is not anymore possible once the NAT has been crossed. As such, means to allow passing the internal information may optimise packet traversal within an SFC-enabled mobile network domain. Furthermore, some SFs that are not enabled on the PGW may require a subscriber identifier to properly operate.

This document does not make any assumption about the structure of subscriber or policy identifiers; each such identifier is treated as an opaque value by the SFC operations and protocols. The semantics and validation of these identifiers are up to the control plane used for SFC. Expectations to SFC control plane protocols are laid down, e.g., in [RFC8459], but specifications of SFC control plane functionalities are also discussed in, for example, [I-D.ietf-bess-nsh-bgp-control-plane], [I-D.wu-pce-traffic-steering-sfc], or [I-D.maglione-sfc-nsh-radius].

The use cases considered in this document assume the NSH is used exclusively within a single administrative domain.

This document adheres to the architecture defined in [RFC7665]. This document assumes the reader is familiar with [RFC8300].

2. Conventions and Terminology

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.

The reader should be familiar with the terms defined in [RFC7665].

3. Subscriber Identification NSH Variable-Length Context Header

Subscriber Identifier is defined as an optional variable-length NSH context header. Its structure is shown in Figure 1.

The subscriber identifier is used to convey an identifier already assigned by the service provider to uniquely identify a subscriber. This header conveys an opaque subscriber Identifier that can be used by the service functions to enforce per-subscriber policies.

The classifier and SFC-aware SFs MAY be instructed via a control interface to inject or strip a subscriber identifier context header. Also, the data to be injected in such header SHOULD be configured to nodes authorized to inject such headers. Failures to inject such headers SHOULD be logged locally while a notification alarm MAY be sent to a Control Element. The details of sending notification alarms (i.e., the parameters affecting the transmission of the notification alarms depend on the information in the context header such as frequency, thresholds, and content in the alarm (full header, header ID, timestamp), etc.) SHOULD be configurable by the control plane.

This document adheres to the recommendations in [RFC8300] for handling the context headers at both ingress and egress SFC boundary nodes. That is, to strip such context headers. Revealing any personal and subscriber-related information to third parties is avoided by design to prevent privacy breaches in terms of user tracking.

SFC-aware SFs and proxies MAY be instructed to strip a subscriber identifier context header from the packet or to pass the data to the next SF in the service chain after processing the content of the context headers. If no instruction is provided, the default behavior is to maintain such context headers so that the information can be passed to next SFC-aware hops.

SFC-aware SFs MAY be instructed via the control plane about the validation checks to run on the content of these context headers (e.g., accept only some lengths) and the behavior to adopt. For example, SFC-aware SFs may be instructed to ignore the context header, to remove the context header from the packet, etc. Nevertheless, this specification does not require nor preclude such additional validation checks. These validation checks are deployment-specific. If validation checks fail on a subscriber identifier context header, an SFC-aware SF MUST ignore that context header. The event SHOULD be logged locally while a notification alarm MAY be sent to a Control Element if the SFC-aware SF is instructed to do so.

Multiple subscriber Identifier context TLVs MAY be present in the NSH each carrying a distinct opaque value but all pointing to the same subscriber.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          Metadata Class       |      Type     |U|    Length   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   ~                      Subscriber Identifier                    ~
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: Subscriber Identifier Variable-Length Context Header

The description of the fields is as follows:

- Metadata Class: MUST be set to 0x0 [RFC8300].

- Type: TBD1 (See Section 5)

- Subscriber Identifier: Carries an opaque subscriber identifier.

4. Policy Identification NSH Variable-Length Context Headers

Dedicated service-specific performance identifier is defined to differentiate between services requiring specific treatment to exhibit a performance characterized by, e.g., ultra-low latency (ULL) or ultra-high reliability (UHR). These parameters are related to policy identifier, among others. They are contained in the policy identifier context header. The policy identifier thus allows for the enforcement of a per-service policy such as a service classification function to only consider specific SFs instances during service function path establishment. Details of this process are implementation-specific. For illustration purposes, the classifier may retrieve the details of usable SFs based upon the corresponding service identifier. Typical criteria for instantiating specific SFs include location, performance, or proximity considerations. For UHR services, the stand-by operation of back-up capacity or the deployment of multiple SF instances may be requested.

In other words, the classifier uses this kind of information to decide about the set of SFFs to invoke to honor the latency or reliability requirement (e.g., compute an Rendered Service Path (RSP), or insert a pointer to be shared with involved SFFs). Then, the policy identifier is inserted in the packet so that upstream SFC-aware nodes can make use of the information for proper distributed SFC path selection and SF instance selection.

Policy identifier is defined as optional variable length context header. Its structure is shown in Figure 2.

Similar control plane considerations as those discussed in Section 3 are to be followed.

Multiple policy identifier context headers MAY be present in the NSH; each carrying a distinct opaque value but all are pointing to policies that need to be enforced for a flow.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Metadata Class       |      Type     |U|    Length   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                      Policy Identifier                        ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Policy Identifier Variable-Length Context Header

The description of the fields is as follows:

- Metadata Class: MUST be set to 0x0 [RFC8300].

- Type: TBD2 (See Section 5)

- Policy Identifier: Represents an opaque value pointing to specific policy to be enforced. The structure and semantic of this filed is deployment-specific.

5. IANA Considerations

This document requests IANA to assign the following types from the "NSH IETF- Assigned Optional Variable-Length Metadata Types" (0x0000 IETF Base NSH MD Class) registry available at: https://www.iana.org/assignments/nsh/nsh.xhtml#optional-variable-length-metadata-types.

Value	Description	Reference
TBD1	Subscriber Identifier	[ThisDocument]
TBD2	Policy Identifier	[ThisDocument]

6. Security Considerations

Data plane SFC-related security considerations, including privacy, are discussed in [RFC7665] and [RFC8300].

Nodes that are involved in an SFC-enabled domain are assumed to be trusted ([RFC8300]). Means to check that only authorized nodes are solicited when a packet is crossing an SFC-enabled domain.

7. Acknowledgements

Comments from Joel Halpern on a previous version and by Carlos Bernardos are appreciated. Contributions and review by Christian Jacquenet, Danny Lachos, Debashish Purkayastha, and Christian Esteve Rothenberg are thankfully acknowledged.

8. References

8.1. Normative References

[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>.

[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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8300] Quinn, P., Ed., Elzur, U., Ed., and C. Pignataro, Ed., "Network Service Header (NSH)", RFC 8300, DOI 10.17487/RFC8300, January 2018, <https://www.rfc-editor.org/info/rfc8300>.

8.2. Informative References

[I-D.ietf-bess-nsh-bgp-control-plane]
Farrel, A., Drake, J., Rosen, E., Uttaro, J., and L. Jalil, "BGP Control Plane for NSH SFC", draft-ietf-bess-nsh-bgp-control-plane-04 (work in progress), July 2018.

[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-08 (work in progress), May 2018.

[I-D.maglione-sfc-nsh-radius]
Maglione, R., Trueba, G., and C. Pignataro, "RADIUS Attributes for NSH", draft-maglione-sfc-nsh-radius-01 (work in progress), October 2016.

[I-D.wu-pce-traffic-steering-sfc]
Wu, Q., Dhody, D., Boucadair, M., Jacquenet, C., and J. Tantsura, "PCEP Extensions for Service Function Chaining (SFC)", draft-wu-pce-traffic-steering-sfc-12 (work in progress), June 2017.

[RFC8459] Dolson, D., Homma, S., Lopez, D., and M. Boucadair, "Hierarchical Service Function Chaining (hSFC)", RFC 8459, DOI 10.17487/RFC8459, September 2018, <https://www.rfc-editor.org/info/rfc8459>.

Authors' Addresses

Behcet Sarikaya
Denpel Informatique

Email: sarikaya@ieee.org

Mohamed Boucadair
Orange
Rennes 3500
France

Email: mohamed.boucadair@orange.com

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

Email: Dirk.von-Hugo@telekom.de