draft-ietf-sfc-serviceid-header-04

Abstract

This document defines Subscriber and Performance Policy Identifiers Network Service Header Variable-Length Context Headers to inform Service Functions about subscriber- and service-related information for the sake of policy enforcement and appropriate service function chaining operations. The structure of each context header is defined, their use and processing instructions by SFC-aware nodes are explained.

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 May 2, 2020.

Copyright Notice

Copyright (c) 2019 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
1. Introduction

This document discusses how to inform Service Functions (SFs, [RFC7665]) 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 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 within the boundaries of a single administrative domain.

Also, the enforcement of SFC-based differentiated traffic policies may be inferred, for example, by QoS (Quality of Service) considerations. Typically, QoS information may serve as an input to 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 performance policy identifier to upstream SFs to appropriately meet the service requirements arises.
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 plane 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 context header in the NSH.

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 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. It is out of scope of this document to include a comprehensive list of deployment contexts which may make use of the context headers defined in the document.

This document does not make any assumption about the structure of subscriber or performance policy identifiers; each such identifier is treated as an opaque value. 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 functions are also discussed in, for example, [I-D.ietf-bess-nsh-bgp-control-plane]. Control plane related considerations are out of scope.

This document assumes 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.

```
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.

The subscriber identifier is used to convey an identifier assigned by the service provider to uniquely identify a subscriber. This subscriber identifier can be used by 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. Typically, a node can be instructed to insert such data following a type/set scheme (e.g., node X should inject subscriber ID type Y). Other schemes may be envisaged.
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 for intermediary SFC-aware nodes 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. When multiple subscriber identifier context TLVs are present and an SF is instructed to strip the subscriber identifier context header, that SF has to remove all subscriber identifier context TLVs.


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). Other policies can be considered when instantiating a service function chain within an SFC-enabled domain. They are conveyed in the Performance Policy Identifier context header.

The performance policy identifier is inserted in an NSH packet so that upstream SFC-aware nodes can make use of the performance information for proper distributed SFC path selection, SF instance selection, or policy selection at SFs.

Thus, the performance policy identifier allows for the distributed enforcement of a per-service policy such as a service function path to only include specific SFs instances. Details of this process are implementation-specific. For illustration purposes, an SFF may retrieve the details of usable SFs based upon the corresponding performance policy identifier. Typical criteria for instantiating specific SFs include location, performance, or proximity considerations. For the particular case of UHR services, the standby operation of back-up capacity or the deployment of multiple SF instances may be requested.

Performance 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 performance 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. It is up to the control plane to ensure that these policies are not conflicting. When such conflict is detected by an SFC-aware node, the default behavior of the node is to discard the packet and send a notification alarm to a Control Element.

```
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   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~                     Performance Policy Identifier             ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Performance Policy Identifier Variable-Length Context Header

The description of the fields is as follows:
o Metadata Class: MUST be set to 0x0 \[RFC8300\].

o Type: TBD2 (See Section 5)

o Performance Policy Identifier: Represents an opaque value pointing to specific performance policy to be enforced. The structure and semantic of this field 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.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD1</td>
<td>Subscriber Identifier</td>
<td>[ThisDocument]</td>
</tr>
<tr>
<td>TBD2</td>
<td>Performance Policy Identifier</td>
<td>[ThisDocument]</td>
</tr>
</tbody>
</table>

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 are out of scope of this document.

A misbehaving node within from the SFC-enabled domain may alter the content of Subscriber and Performance Policy TLVs which may lead to service disruption. Such attach is not unique to the TLVs documents defined in the document; measures discussed in [RFC8300] are to be followed. Also, integrity checks offered by the transport encapsulation can be used to detect anomalies.

An SF maintaining logs for operational reasons MUST NOT log the content of Subscriber and Performance Policy context headers received in NSH packets if the SF does not use the content of that header for its operation.
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, Christian Esteve Rothenberg, and Kyle Larose are thankfully acknowledged.

8. Change Log

Note. This section will be removed after WG last call.

- submitted version -00 as a working group draft after adoption
- submitted version -01 for editorial improvements
- submitted version -02 with these changes: fixed the abbreviated title, corrected typos, editorial improvements, rename policy identifier as performance policy identifier
- 03: As discussed in Prague ([https://datatracker.ietf.org/meeting/104/materials/slides-104-sfc-sfc-chair-slides-01](https://datatracker.ietf.org/meeting/104/materials/slides-104-sfc-sfc-chair-slides-01)), there was a question whether the authors should investigate a solution specific to this I-D to cover integrity protection, but this seems not the good option given that this is a generic concerns for all TLVs. No change is thus added to the document.

9. References

9.1. Normative References


9.2. Informative References

[I-D.ietf-bess-nsh-bgp-control-plane]

[I-D.ietf-sfc-use-case-mobility]


Authors’ Addresses

Behcet Sarikaya
Denpel Informatique
Email: sarikaya@ieee.org

Dirk von Hugo
Deutsche Telekom
T-Online-Allee 1
D-64295 Darmstadt
Germany
Email: Dirk.von-Hugo@telekom.de

Mohamed Boucadair
Orange
Rennes 3500
France
Email: mohamed.boucadair@orange.com