Abstract

This document discusses considerations related to passing service-, host- and subscriber-related information to upstream Service Functions for the sake of policy enforcement and appropriate SFC-inferred forwarding. Once the information is consumed by SFC-aware elements of an SFC-enabled domain, the information is stripped from packets so that privacy-sensitive information is not leaked outside an SFC-enabled domain.

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 January 6, 2017.

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.
1. Introduction

This document focuses on aspects related to passing service-, host- and subscriber-related information to upstream Service Functions (SFs) when required for the sake of policy enforcement. Indeed, subscriber-related information may be needed for upstream SFs when per-subscriber policies are to be enforced upstream in the network while the information conveyed by the original packets does not allow for uniquely identifying a host or a subscriber.

In addition further service- and policy-specific information regarding handling of packet flows according to agreed quality and performance requests - such as denoted by Quality of Service (QoS) or Quality of Experience (QoE) parameters - may be needed, e.g. for prioritization of packet forwarding with respect to latency demands or required high reliability. Such features would ask for preferred assignment of specific network function locations during construction of a constrained service function path (SFP), and for computation of a concrete Rendered Service Path (RSP) i.e. the actual sequence of SFs and SF Forwarders (SFFs), e.g. by a service classification
function according to [RFC7665], which can be executed as described in [I-D.ietf-sfc-control-plane] and [I-D.ietf-sfc-nsh]. SFs and SFFs involved honor their part of the service or slice ID contained assurance contract by being e.g. 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 there might be some value to convey such signal to SFC-aware nodes in data packets to simplify state that would be required to check whether a packet is to be granted a given service.

This document adheres to the architecture defined in [RFC7665]. This document assumes the reader is familiar with [RFC7665] and [I-D.ietf-sfc-control-plane].

Host-related information may be required to implement services such as, but not limited to, traffic policy control, or parental control and traffic offload that are commonly used by operators to enable added value services to their customers in typical network architectures [I-D.liu-sfc-use-cases].

Another typical example is the applicability of service chaining 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 advanced SFs to be invoked are located after a NAT device (that can reside in the Packet Data Network (PDN) Gateway (PGW) or in a distinct operator-specific 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 ease the operation of an SFC-enabled domain. Furthermore, some SFs that are not enabled on the PGW may require a subscriber identifier e.g., International Mobile Subscriber Identity (IMSI), to execute their function. Other use cases that suffer from identification problems further are discussed in [RFC7620].

Because both a host and subscriber identifiers may be required in some scenarios, this document defines two objects that allow carrying this information.

Unless the information contained within such host and subscriber identifiers already allows for deriving service specific requirements (e.g. of services to which the hosts are subscribed to or which the subscribers are expected to consume according to their contract) and which may impact the choice of optimum specific service function locations (placement and service function path constrains) then also additional service or slice identifiers will be required.
Service-related information may be required to ensure specific service quality and performance such as granted low latency or extreme high reliability as, e.g., demanded for future 'tactile internet' applications or eHealth and industry control as typical examples for expected vertical use cases to be deployed in the framework of logically separated network slices. Due to the high variability and broad range of the new services expected for beyond 2020 we do not see that level of complexity covered within a QoS/DSCP (QoS-Class - Identifier AVP) as proposed in [I-D.napper-sfc-nsh-broadband-allocation].

This document does not make any assumption about the structure of host and service identifiers; each information is treated as an opaque value. The meaning and validation of each of these identifiers can be the responsibility of the control plane [I-D.ietf-sfc-control-plane].

Host-related and/or subscriber-related information is stripped from packets exiting an SFC-enabled domain so that privacy-sensitive information is not leaked outside the domain. See Section 8 for more discussion on privacy.

Within this document, only identification issues for the sake of services in a local administrative domain are discussed. Global identification issues are out of scope.

2. Conventions and Terminology

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].

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

3. Problem Space and Sample Use Cases

Enforcing Policies based on an internal IP address:

Because of the address sharing, implicit CPE/UE identification that relies on the source IP address cannot be implemented within the administrative domain because the same IP address is shared among various connected devices (CPE for the fixed case or UE for the mobile case). In the meantime, policies are something provisioned based on the internal IP address assigned to those devices. Means to pass the internal IP address beyond an address sharing device for the sake of per-host or per-subscriber policy enforcement is needed in some SFC deployments.
Also, stable identifiers such as MAC address, IMSI can be passed.

Enforcing Policies based on a subscriber identifier:

In case some deployments may require per-subscriber policies, a means is required to pass subscriber ID to those upstream SFs which are responsible for or rely on policy enforcement.

Enforcing Policies based on a service specific identifier:

In case a specific set of services and applications, e.g. which all are characterized by same QoS/QoE requirements (laid down e.g. in terms of corresponding policies) and the service function chains want to reflect this behavior by assigning a specific SFC (or virtual network slice) to them, deployments may require a per-service/slice identifier and a means to pass such identifier to those upstream SFs which are responsible for or rely on policy enforcement.

Below we present some use cases where problems related to enforcing policies based on subscriber and/or host identities and those based on service and/or slice identifiers currently cannot be achieved in service function chaining. It is important to note that subscriber and host identification due to address and prefix sharing is not specific to the service function chaining. This problem occurs in many other use cases as discussed in [RFC7620].

3.1. Parental Control Use Case

Parental control service function searches each packet for certain content, e.g. destination addresses corresponding to certain URL like www.thisbizarresite.com. Parental control function should keep this information (URL and source IP address) in its cache so that all subsequent packets can be filtered for certain users from the Web server [WT317].

Parental control function receives next packet from the recorded URL. Enforcing the parental control policies may depend on the internal IP address, i.e., the address of the host that is being subject to the parental control. Parental control function must be able to identify incoming traffic to be filtered, e.g. specific URL information. All other traffic is not subject to filtering. Parental control function filters all traffic coming from indicated URL only for the specific hosts identified by the service logic.

For the virtual CPE case, the access node will receive privately-addressed packets. Because private addresses are overlapping between several subscribers, the internal IP address will need to be copied into a dedicated field (Host ID context) so that upstream function
responsible for Parental Control can process the packets appropriately. Furthermore, the subscriber identifier may also be required for authorization purposes.

3.2. Traffic Offload Use Case

Traffic offload service function works on each flow/service originated from mobile terminal and decides if it should be offloaded to the broadband network or sent back to the mobile network. In this use case policy enforcement is based on the subscriber identifier. The broadband network must obtain the subscription profile from the mobile network and decide if the traffic coming from this subscriber needs to be offloaded or not. If offloading is needed, this usually means that the subscriber identifier needs to be known on the SFC-aware forwarders.

3.3. Mobile Network Use Cases

Many SFs can be executed in different combinations in a mobile network [I-D.ietf-sfc-use-case-mobility]. Placement of NAT function plays an important role if it is used.

If NAT function is collocated with P-GW as in [TR23.975] or is located right after the P-GW then all service functions located upstream can only see the translated address as the source address from all User Equipments (UEs). Internal IP address-related part of their policy set won’t be able to execute their service logic. As a consequence, means to pass the internal IP address (i.e., the original one before executing the NAT function) through the service chain may be needed.

Note that the same problem occurs in case IPv6 is being used by UEs but UEs need to communicate with an external legacy server which is IPv4-only. This can be made possible with NAT64 as described in [RFC6146]. NAT64 uses IPv4 address on its outgoing interface which is shared by all UEs. So in the case of NAT64 host identification also becomes an issue in service chaining.

[I-D.ietf-sfc-use-case-mobility] identifies the following information:

- Charging ID
- Subscriber ID
- GGSN or PGW IP address
- Serving Gateway Support Node (SGSN) or SGW IP address
3.4. Extreme Low Latency Service Use Cases

Extreme or ultra-low latency Use Case as foreseen for so-called ‘5G’ system of next generation (not only) mobile networks, e.g. by 3GPP \[TR22.862\] requires specific architectural and protocol characteristics to allow for rapid execution and low transmission delay of packets within services as for example medical, industrial, or vehicular applications. This can be granted by forwarding all packets via the shortest paths only and/or via the service functions granting lowest processing delay.

3.5. High Reliability Applications Use Cases

Another set of use cases within the critical communications family demands for very (or ultra-) high reliability of services as defined by 3GPP in \[TR22.862\] by ‘High Reliable communication services are characterized by the service layer need of committed QoS targets and its possibility to act upon an expected change of the network fulfillment of the QoS targets.’ This can be granted by forwarding all packets via the most reliable and secure paths only.

4. Host and Subscriber Identification SFC Meta Data

Host Identifier and Subscriber Identifier are defined as optional variable length context headers. Their structure is shown in Figure 1 and Figure 2, respectively. Host Identifier context header may convey an internal IP address, VLAN or MAC address.

While the subscriber identifier itself is used to convey an identifier already assigned by the service provider to uniquely identify a subscriber or an information that is required to enforce a per-subscriber policy, the structure of the identifier is deployment-specific. Typically, this header may convey the IMSI, opaque subscriber Identifier, etc.

The classifier and SFC-aware Service Functions MAY be instructed via a control interface to inject or strip a host identifier and/or subscriber identifier context headers. 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 level of sending notification alarms SHOULD be configurable by the control plane.

The control plane SHOULD instruct Ingress Border Nodes about the behavior to follow when receiving Host ID and/or Subscriber ID context headers from external SFC-enabled domain. If no instruction is provided, the default behavior is to strip such context headers when received from external SFC-enabled domain.

The control plane SHOULD instruct Egress Border Nodes about the behavior to follow for processing packets conveying Host ID and/or Subscriber ID context headers. If no instruction is provided, the default behavior is to strip such context headers before sending the packets outside an SFC-enabled domain.

SFC-aware SFs and Proxies that are not acting as SFC border nodes MAY be instructed to strip a host ID and/or subscriber ID from the packet or to pass the data to the next SF in the chain after consuming the content of the 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 functions MAY be instructed via the control plane about the validation checks to follow on the content of these context headers (e.g., accept only some lengths, accept some subtypes) and the behavior to follow. For example, SFC-aware nodes 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 context header, an SFC-aware node ignores that context header. The event SHOULD be logged locally while a notification alarm may be sent to a control element if the SFC-aware node is instructed to do so.

Only one Host Identifier context header MUST be present in the SFC header.

Multiple subscriber Identifier context headers MAY be present in the SFC header each conveying a distinct sub-type.
The description of the fields is as follows:

The fields TLV Class, etc. are defined in [I-D.ietf-sfc-nsh]

Host Identifier: Can be IPv4 or IPv6 address, IPv6 prefix, a subset of IP address/prefix, a MAC address, or any deployment-specific identifier. It could also be in Root NAI format containing arbitrary number of characters [TS23.003].

SubT field of 8 bits indicates the sub-type of the information conveyed in the "Subscriber Identifier" field. The following values are defined:

- 0x00: Opaque value
- 0x01: Charging ID. The structure of this ID is deployment-specific.
- 0x02: Subscriber ID. The structure of this ID is deployment-specific.
Service Identifier: Conveys an opaque subscriber identifier or an identifier that corresponds to the sub-type.

5. Slice and Service Identification SFC Meta Data

Dedicated service- and slice specific performance Identifiers are 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 slice and service identifiers and (among potentially others) are contained and transported within the service Identifier. The service Identifier thus allows for enforcement of a per service policy such as a service classification function to only consider dedicated service functions during service function path construction. Details of this process are implementation specific, for illustration the classifier may retrieve via the corresponding service or slice ID from a data base of the details of usable service functions. Exemplary characteristics of specific service function instantiations may be location or distance from service session endpoints or processing speed in case of ULL. For UHR the stand-by operation of back-up capacity or a redundant deployment of service function instantiations may be requested for all service functions selectable by the classifier when applying for a service denoted by this ID. 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 RSP or insert a pointer to be shared with involved SFFs).

Slice and Service Identifier are defined as optional variable length context headers. Their structure is shown in Figure 3 and Figure 4, respectively. Service/Slice Identifier context header may convey a user or service provider defined unique identity which can be described by an opaque value. Use of IP Address or prefix, VLAN or MAC address here are for further consideration.
The service requirements in terms of e.g. but not limited to parameters as maximum latency or minimum outage probability are to be specified by service providers and not in scope of this document.

General considerations as mentioned above for Host - and Subscriber ID correspondingly apply here (see Section 4).

Only one Slice Identifier context header MUST be present in the SFC header.

Multiple Service Identifier context headers MAY be present in the SFC header each conveying a distinct sub-type.

The description of the fields is as follows:

The fields TLV Class, etc. are defined in [I-D.ietf-sfc-nsh].

Slice Identifier: The structure of the identifier is deployment-specific. This field carries an identifier that uniquely identifies a slice within a network, e.g. it could be an opaque value with an arbitrary number of characters.

[NOTE: The structure of the service ID TLV is to be further discussed, particularly to assess why it is not sufficient to convey an ID rather than a type and an ID.]
The description of the fields is as follows:

The fields TLV Class, etc. are defined in [I-D.ietf-sfc-nsh]

SubT field of 8 bits indicates the sub-type of the information conveyed in the "Service Identifier" field. The following values are defined:

- **0x00**: Opaque value
- **0x01**: Ultra-low latency ID. The structure of this ID is service deployment-specific.
- **0x02**: Ultra-high reliability ID. The structure of this ID is service deployment-specific.
- **0x03**: Slice Identifier. The structure of this ID is service deployment-specific.
- **0x04 - 0x08**: reserved

Service Identifier: Can be any deployment-specific identifier. It could also be an opaque value with an arbitrary number of characters. The Service ID could represent a specific service performance characteristic reflected in the SubT field, but also denote a default basic (best effort) service without specifically defined requirements.

6. IANA Considerations

To be completed.

7. Security Considerations

Data plane SFC-related security considerations are discussed in [RFC7665]. Control plane SFC-related security considerations are discussed in [I-D.ietf-sfc-control-plane].

Security considerations that are related to the host identifier are discussed in [RFC6967].

A misbehaving node can inject host/subscriber Identifiers to disturb the service offered to some host or subscribers. Also, a misbehaving node can inject host/subscriber identifiers as an attempt to be granted access to some services. To prevent such misbehavior, only trusted nodes MUST be able to inject such context headers. Nodes that are involved in a SFC-enabled domain must be trusted. Means to
check that only authorized nodes are solicited when a packet is crossing an SFC-enabled domain.

8. Privacy Considerations

The metadata defined in this document for host and subscriber identifiers may reveal private information about the host and/or the subscriber. Some privacy-related considerations for Internet Protocols are discussed in [RFC6973]. In the light of these privacy considerations, it is important to state that the host and subscriber metadata must not be exposed outside the operator’s domain [I-D.ietf-sfc-control-plane].

The information conveyed in host and/or subscriber identifiers is already known to an administrative entity managing an SFC-enabled domain. Some of that information is already conveyed in the original packets from a host (e.g., internal IP address) while other information is collected from various sources (e.g., GTP tunnel, line identifier, etc.). Conveying such sensitive information in packets may expose subscribers’ sensitive data to entities that are not allowed to receive such information. Misconfiguring SFC egress nodes is a threat that may have negative impacts on privacy (e.g., some operational networks leak the MSISDN outside). Operators must ensure their SFC-enabled domain is appropriately configured so that any privacy-related information is not exposed a domain.

Some use cases that rely upon the solution defined in this document may disclose some additional privacy-related information (e.g., a host identifier of a terminal within a customer premises for the parental control case). It is assumed that this information is provided upon approval from a subscriber. For example, a customer may provide the information as part of its service management interface or as part of explicit subscription form. As a common recommendation for deployment relying on SFC header, a CPE MUST NOT leak non-authorized information to the service provider by means of an SFC header. Note, the use cases discussed in this document assume the service header is used exclusively within the service administrative domain. CPEs are not required to be SFC-aware.

9. Acknowledgements

Comments from Joel Halpern on a previous version are appreciated.

This work has been partially performed in the framework of the EU-funded H2020-ICT-2014-2 project 5G NORMA. Contributions of the project partners are gratefully acknowledged. The project consortium is not liable for any use that may be made of any of the information contained therein.
10. References

10.1. Normative References

[I-D.ietf-sfc-control-plane]

[I-D.ietf-sfc-nsh]


10.2. Informative References

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

[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.napper-sfc-nsh-broadband-allocation]

[I-D.quinn-sfc-nsh-tlv]
Internet-Draft    Service, Subscriber and Hostid in SFC        July 2016

[ RFC6146 ] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful
NAT64: Network Address and Protocol Translation from IPv6
Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146,

[ RFC6967 ] Boucadair, M., Touch, J., Levis, P., and R. Penno,
"Analysis of Potential Solutions for Revealing a Host
Identifier (HOST_ID) in Shared Address Deployments",
RFC 6967, DOI 10.17487/RFC6967, June 2013,

[ RFC6973 ] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J.,
Morris, J., Hansen, M., and R. Smith, "Privacy
Considerations for Internet Protocols", RFC 6973,
DOI 10.17487/RFC6973, July 2013,

[ RFC7620 ] Boucadair, M., Ed., Chatras, B., Reddy, T., Williams, B.,
and B. Sarikaya, "Scenarios with Host Identification
Complications", RFC 7620, DOI 10.17487/RFC7620, August

[ TR22.862 ] "3GPP TR22.862, Feasibility Study on New Markets and
Technology Enablers - Critical Communications; Stage 1
(Release 14)", 2015.


and Terminals; Numbering, addressing and identification",
2015.

[ TS29.212 ] "3GPP TS29.212, Policy and Charging Control (PCC) over Gx/
Sd reference point", December 2011.

2015.

Authors’ Addresses

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

Behcet Sarikaya  
Huawei  
5340 Legacy Dr.  
Plano, TX  75024  
Email: sarikaya@ieee.org