Service Function Chaining
Internet-Draft
Intended status: Informational
Expires: April 14, 2017

W. Haeffner
Vodafone
J. Napper
Cisco Systems
M. Stiemerling
NEC
D. Lopez
Telefonica I+D
J. Uttaro
AT&T

October 11, 2016

Service Function Chaining Use Cases in Mobile Networks
draft-ietf-sfc-use-case-mobility-07

Abstract

This document provides some exemplary use cases for service function chaining in mobile service provider networks. The objective of this draft is not to cover all conceivable service chains in detail. Rather, the intention is to localize and explain the application domain of service chaining within mobile networks as far as it is required to complement the problem statement [RFC7498] and architecture framework [RFC7665] of the working group.

Service function chains typically reside in a LAN segment which links the mobile access network to the actual application platforms located in the carrier's datacenters or somewhere else in the Internet. Service function chains (SFC) ensure a fair distribution of network resources according to agreed service policies, enhance the performance of service delivery or take care of security and privacy. SFCs may also include Value Added Services (VAS). Commonly, SFCs are typical middle box based services.

General considerations and specific use cases are presented in this document to demonstrate the different technical requirements of these goals for service function chaining in mobile service provider networks.

The specification of service function chaining for mobile networks must take into account an interaction between service function chains and the 3GPP Policy and Charging Control (PCC) environment.

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 [RFC2119].

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 April 14, 2017.

Copyright Notice

Table of Contents

1. Introduction

1.1. Terminology and abbreviations

Much of the terminology used in this document has been defined by the 3rd Generation Partnership Project (3GPP), which defines standards for mobile service provider networks. Although a few terms are defined here for convenience, further terms can be found in [RFC6459].

UE User equipment like tablets or smartphones

eNB enhanced NodeB, radio access part of the LTE system

S-GW Serving Gateway, primary function is user plane mobility

P-GW Packet Gateway, actual service creation point, terminates 3GPP mobile network, interface to Packet Data Networks (PDN)

HSS Home Subscriber Server (control plane element)

MME Mobility Management Entity (control plane element)

GTP GPRS (General Packet Radio Service) Tunnel Protocol

S-IP Source IP address

D-IP Destination IP address

IMSI International Mobile Subscriber Identity that identifies a mobile subscriber

(S)Gi Egress termination point of the mobile network (SGi in case of LTE, Gi in case of UMTS/HSPA). The internal data structure of this interface is not standardized by 3GPP

PCRF 3GPP standardized Policy and Charging Rules Function

PCEF Policy and Charging Enforcement Function

TDF Traffic Detection Function

TSSF Traffic Steering Support Function

IDS Intrusion Detection System

FW Firewall

ACL Access Control List

PEP Performance Enhancement Proxy

IMS IP Multimedia Subsystem

LI Lawful Interception

1.2. General scope of mobile service chains

Mobile access networks terminate at a mobile service creation point (called Packet Gateway) typically located at the edge of an operator IP backbone. From the user equipment (UE) up to the Packet Gateway (P-GW) or, if deployed, the Traffic Detection Function (TDF) everything is fully standardized by the 3rd Generation Partnership Project (3GPP) e.g., in [TS.23.401] and in [TS.23.203]. Within the mobile network, the user payload is encapsulated in 3GPP specific tunnels terminating eventually at the P-GW. In many cases application- specific IP traffic is not directly exchanged between the original mobile network, more specifically the P-GW, and an application platform, but will be forced to pass a set of service

functions. Those application platforms are, for instance, a web server environment, a video platform, a social networking platform or some other multimedia platform. Network operators use these service functions to differentiate their services to their subscribers. Service function chaining is thus integral to the business model of operators.

Important use case classes for service function chains generally include:

- functions to protect the carrier network and the privacy of its users(IDS, FW, ACL, encryption, decryption, etc.),
- functions that ensure the contracted quality of experience using e.g., performance enhancement proxies (PEP) like video optimizers, TCP optimizers or functions guaranteeing fair service delivery built upon policy based QoS mechanisms,
- functions like HTTP header enrichment that may be used to identify and charge subscribers real time,
- functions like Carrier Grade NAT (CG-NAT) and NAPT, which are required solely for technical reasons, and
- functions like parental control or malware detection that may be a cost option of a service offer.

1.3. General structure of end-to-end carrier networks

Although this memo is focused on the Service Function Chaining use cases for mobile carrier networks, such as 3GPP-based ones, a number of other, different carrier networks exists that share similarities in the structure of the access networks and the service functions with mobile networks.

Figure 1 shows a simplified schematic view of 4 different access service networks to indicate similarities with respect to Service Functions and their Chaining.

These service networks consist of access-specific user equipment, a dedicated access network, a related service creation point and finally a (LAN) infrastructure hosting Service Functions which eventually interconnect to application platforms in the Internet or in the carrier's own datacenter (DC). From top to down, there is a 3GPP mobile network terminating at the P-GW (or TDF), an xDSL network with its PPP tunnels terminating at a BNG (Broadband Network Gateway), a FTTH network terminating at an OLT (Optical Line

Terminal) and finally a CATV (cable TV) network terminating at a CMTS (Cable Modem Termination System).

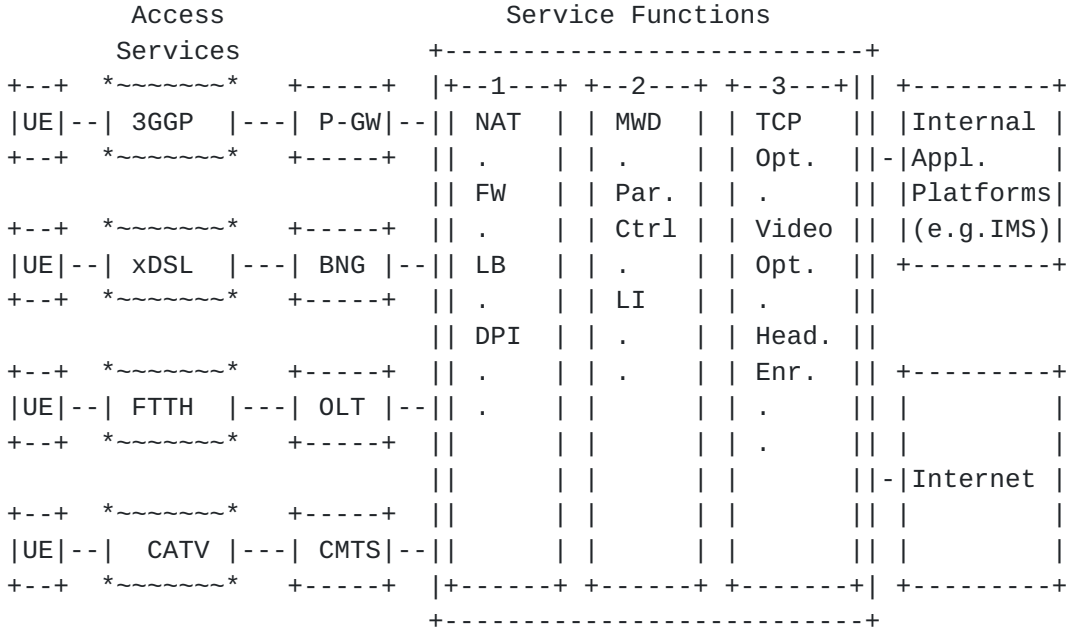

Figure 1: Various end-to-end carrier networks and service functions sorted into categories 1, 2 and 3.

Category 1 of service functions like NAT or DPI may be used by all of these service networks mainly just (but not exclusively) for technical reasons. The same is true for category 2, Value Added Services (VAS) like parental control, malware detection and elimination (MWD) or Lawful Interception (LI). TCP optimization is basically seen in mobile networks only. The same may be true for video optimizers or HTTP header enrichment; i.e., category 3 as a rule mainly belongs to mobile networks only.

In our view, 3GPP-based mobile networks seem to have the largest demand for service functions and service function chains. Service Function Chains used in other access networks are very likely a subset of what one can expect in 3GPP-based mobile networks.

Typical data center use cases are described in [ietf-sfc-dc-use-cases].

2. Mobile network overview

For simplicity we only describe service function chaining in the context of LTE (Long Term Evolution) networks. But indeed our service chaining model also applies to earlier generations of mobile networks, such as purely UMTS-based mobile networks.

2.1. Building blocks of 3GPP mobile LTE networks

The major functional components of an LTE network are shown in Figure 2 and include user equipment (UE) like smartphones or tablets, the LTE radio unit named enhanced NodeB (eNB), the serving gateway (S-GW) which together with the mobility management entity (MME) takes care of mobility and the packet gateway (P-GW), which finally terminates the actual mobile service. These elements are described in detail in [TS.23.401]. Other important components are the home subscriber system (HSS), the Policy and Charging Rule Function (PCRF) and the optional components: the Traffic Detection Function (TDF) and the Traffic Support Steering Function (TSSF), which are described in [TS.23.203]. The P-GW interface towards the SGi-LAN is called the SGi-interface, which is described in [TS.29.061]. The TDF resides on this interface. Finally, the SGi-LAN is the home of service function chains (SFC), which are not standardized by 3GPP.

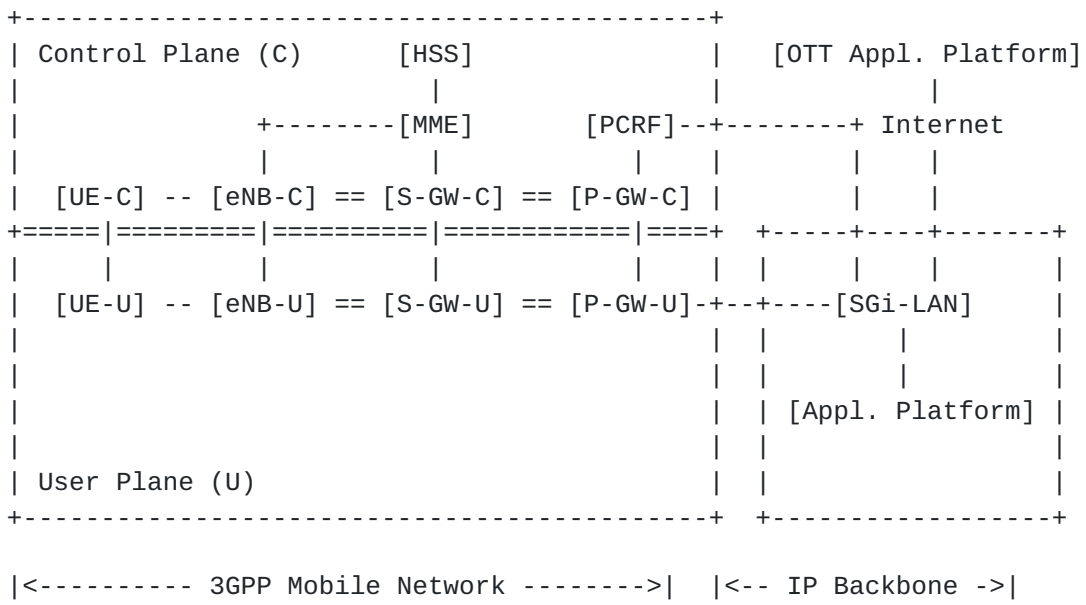

Figure 2: End to end context including all major components of an LTE network. The actual 3GPP mobile network includes the elements from the user equipment [UE] to the packet gateway [P-GW]. Labels ending with -C denote control plane functionality and ending with -U user plane functionality, respectively. Separation of control and user plane is presented for a logical view and is not currently standardized by 3GPP.

The radio-based IP traffic between the UE and the eNB is encrypted according to 3GPP standards. Between eNB, S-GW and P-GW user IP packets are encapsulated in 3GPP-specific tunnels. In some mobile carrier networks the 3GPP-specific tunnels between eNB and S-GW are even additionally IPSec-encrypted. More precisely, IPSec originates/

terminates at the eNB and on the other side at an IPSec-GW often placed just in front of the S-GW. For more details see [TS.29.281], [TS.29.274] and [TS.33.210].

Service function chains act on user plane IP traffic only. But the way these act on user traffic may depend on subscriber, service or network specific control plane metadata (see Section 2.4 for a discussion of metadata in the context of this document).

2.2. Overview of mobile service chains

The original user IP packet, including the Source-IP-Address (S-IP) of the UE and the Destination-IP-Address (D-IP) of the addressed application platform (or any host in the Internet in general), leaves the Packet Gateway from the mobile network via the so-called Gi-interface (3G service, e.g., UMTS), respectively SGi-interface (4G service, e.g., LTE). Between this (S)Gi-interface and the actual application platform the user generated upstream IP packets and the corresponding downstream IP packets are typically forced to pass an ordered set of service functions, loosely called a Service Function Chain (SFC).

The set of all available service functions (physical or virtualized) which can be used to establish different Service Function Chains for different services is often called a Gi-LAN for 2G/3G services and SGi-LAN for 4G services.

The (S)Gi-interface towards the (S)Gi-LAN itself is discussed in [TS.29.061], and service function chaining classification or traffic steering is discussed in [TS.23.203].

The (S)Gi-LAN service functions can use subscriber and service related metadata delivered from the mobile control plane, such as the PCRF, or from the user plane, e.g., via HTTP Header Enrichment to process the flows according to service related policies. Some service functions may even use network performance data describing the actual momentary state of a network segment.

If a network operator utilizes HTTP Header Enrichment, care must be taken that privacy is ensured by some mechanism especially when IP service flows leave the operator's network towards a third party (see Section 3.3.3).

In short, the (S)Gi-LAN service area is presently used by mobile service providers to differentiate their services to their subscribers and reflect the business model of mobile operators.

For different applications (e.g., Appl. 1,2,3) upstream and downstream user plane IP flows will be forced to pass a sequence of service functions which is called a Service Function Chain specific to a given application. In the simple example sketched in Figure 3, the service chains for applications 1, 2 and 3 may be just classified by a unique interface-ID of the egress P-GW interfaces or TDF where the service chains for application 1, 2 and 3 are attached.

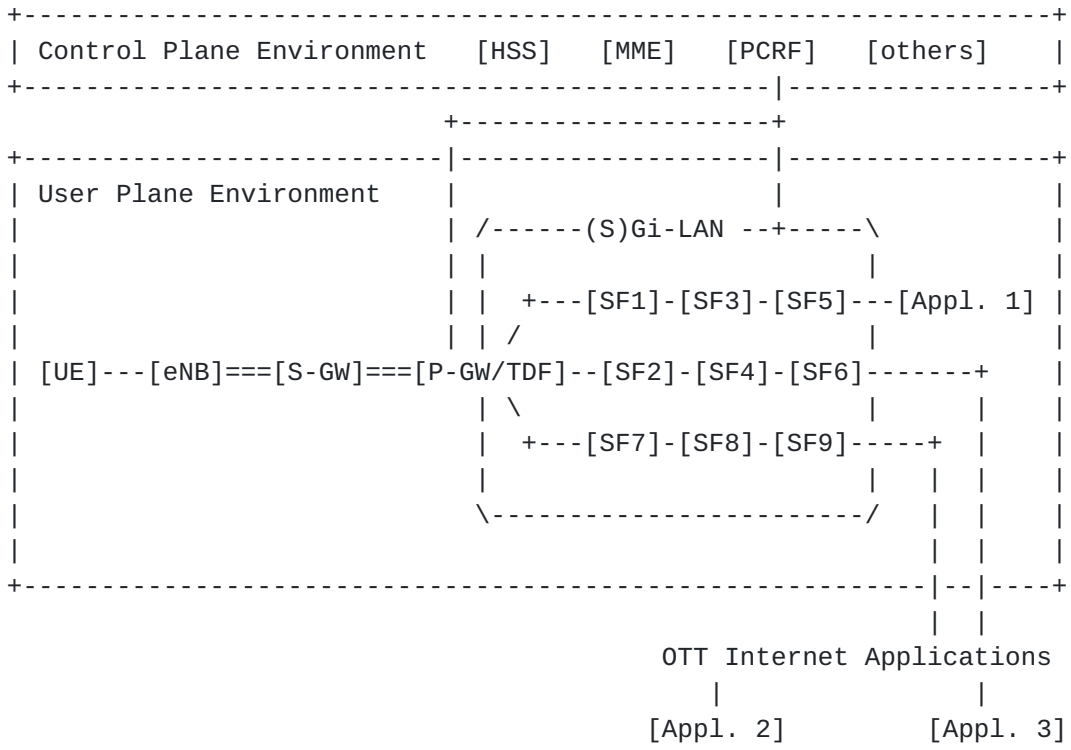

Figure 3: Typical service chain topology.

Service functions typically observe, alter or even terminate and re-establish application session flows between mobile user equipment and application platforms. Control plane metadata supporting policy based traffic handling may be linked to individual service functions SFn. Because in Figure 3 the P-GW classifies service chains, we consider the P-GW as a component of the service chaining environment. However, more sophisticated classification schemes are possible and discussed later.

Care must be taken in classifying and directing flows in different directions (upstream versus downstream) or different flows from the same subscriber when Service Functions observe or alter session flows. Such functions can maintain local state that is necessary to the correct functioning of session flows or to enforcing the policies of the service provider (e.g., fair-use policies). Such stateful service functions can require steering both upstream and downstream

directions of a flow through a single service function instance (e.g., from a set of identical service function instances deployed for scale) or for steering all flows with a common criteria (e.g., belonging to the same subscriber) through such a single service function instance.

2.3. The most common classification scheme

Mobile user equipment like smartphones, tablets or other mobile devices use Access Point Names (APNs) to address a service network or service platform. APNs are DNS host names comparable to FQDN (Fully Qualified Domain Name) host names. While an FQDN refers to an Internet IP address, an APN (loosely speaking) specifies a P-GW IP address. These APNs are used to distinguish certain user groups and their traffic, e.g., there can be an APN for a mobile service offered to the general public while enterprise customers get their own APN. For APN details see [TS.23.003].

Operators often associate a designated Virtual LAN ID (VLAN-ID) with an APN. A VLAN-ID n then may classify the service function chain n (SFC n) related to an application platform n (Appl. n), as shown in the following Figure 4.

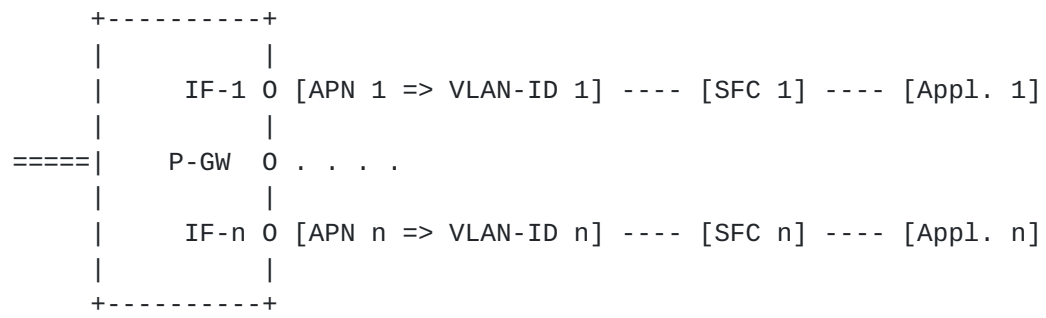

Figure 4: Association of a service chain to an application platform.

Examples for an APN are, e.g.:

APN:	web.vodafone.de
User Name:	not required
Password:	not required

Table 1: Example APN for Vodafone Germany

APN:	internet.telekom
User Name:	t-mobile
Password:	tm

Table 2: Example APN for Deutsche Telekom/T-Mobile

2.4. More sophisticated classification schemes

More sophisticated classifications are feasible using metadata that is UE related, subscriber and service related, as well as network related metadata. Typical metadata and their sources are:

UE: terminal type (e.g., vendor), IMSI (country, carrier, user)

GTP tunnel endpoint: eNB-Identifier, time, and many more

PCRF: subscriber info, APN (service name), QoS, policy rules

Mobile operator defined subscriber, service or network specific policies are typically encoded in the 3GPP-based Policy and Charging Rules Function (PCRF), see [TS.23.203]. For instance, a PCRF may encode the rules that apply to pre-paid and post-paid users, users with a classification of gold, silver, or bronze, or even as detailed as describing rules that apply to "gold users, wishing to download a video file, while these subscribers are subjected to a fair-usage policy". It is up to the mobile service providers to encode the precise mappings between its subscriber classes and the associated service chains.

The Traffic Detection Function (TDF) is part of the 3GPP PCC (Policy and Charging Control Architecture, [TS.23.203]) architecture. Such a TDF, when deployed in the network, resides on the SGi interface, can inspect the user traffic after leaving the P-GW function (see Figure 4) and can maintain connections to the charging infrastructure: Online Charging System (OCS) and Offline Charging System (OFCS). The TDF can be used to classify traffic originating from an APN into more detailed services. This can be used to classify traffic into different Service Functions.

The Traffic Steering Support Function (TSSF) has also been defined recently (since Rel. 13) as part of the 3GPP PCC architecture to support classification of traffic into different Service Functions. The TSSF does not have any connections into the charging infrastructure (OFS or OFCS), but does maintain an interface (St) into the PCRF. Over this interface, the PCRF can provision, modify

and remove classification rules for steering traffic into different Service Functions.

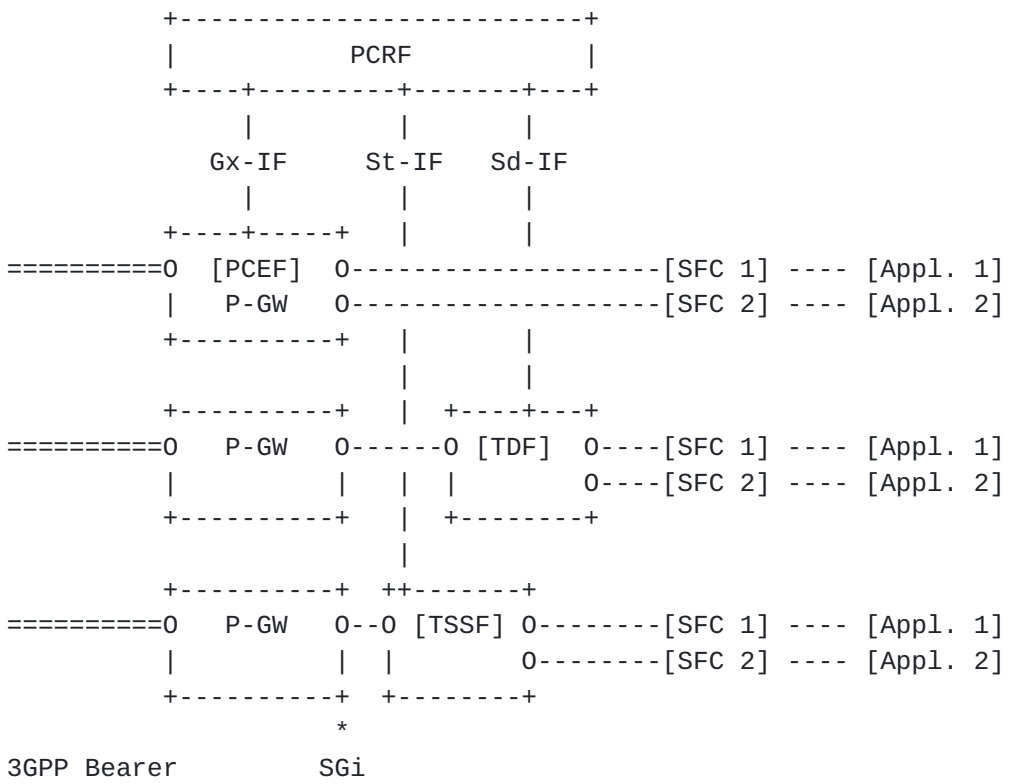

Figure 5: 3GPP combined service chaining classification and steering points. The Policy and Charging Enforcement Function (PCEF) and the Traffic Detection Function (TDF) enforce policies received from the PCRF and, in the other direction, the PCEF provides the PCRF with subscriber and access information via Gx interface. The TSSF can also be used by the PCRF over the St interface to steer traffic into Service Functions.

In general, there are several possibilities to specify classification and steering in mobile networks. Figure 5 demonstrates combined classification and steering deployments. There are also separated classification and steering deployments. 3GPP considers these approaches: [TS.23.203]:

- Classification and steering by the P-GW alone with rules received from Gx.
- Classification and steering by the TDF alone with rules received from Sd.
- Classification and steering by the TSSF alone with rules received from St.

- Initial classification by the P-GW (with rules received from Gx) and steering by the TDF (with rules received from Sd).

- Initial classification by the TDF (with rules received from Sd) and steering by the TSSF (with rules received from St interface).

3. Example use cases specific to mobile networks

HTTP via TCP port 80 (or TCP port 443 for HTTPS) is by far the most common Internet traffic class. Therefore, we discuss two typical examples of an associated service function chaining model in some more detail.

The models presented below are simplified compared to real life service function chain implementations because we do not discuss differentiated traffic handling based on different subscriber-specific service level agreements and price plans or even actual network load conditions.

3.1. Service chain model for Internet HTTP services

With the increase of Internet traffic in mobile networks, mobile operators have started to introduce Performance Enhancement Proxies (PEPs) to optimize network resource utilization. PEPs are more or less integrated platforms that ensure the best possible Quality of Experience (QoE). Their service functions include but are not limited to Deep Packet Inspection (DPI), web and video optimizations, subscriber and service policy controlled dynamic network adaption, analytics and management support.

A simple service function chain model for mobile Internet upstream and downstream traffic is shown in Figure 6 below. The function chain includes Load Balancers (LB), which split HTTP over TCP port 80 away from the rest of the Internet traffic. Beside basic web content, this traffic class includes more and more video. To act on this traffic type we force this traffic to pass Performance Enhancement Proxies (PEPs). The firewall function (FW) protects the carrier network from the outside and Network Address Translation (NAT) maps the private IP address space dedicated to user equipment to a public IP address.

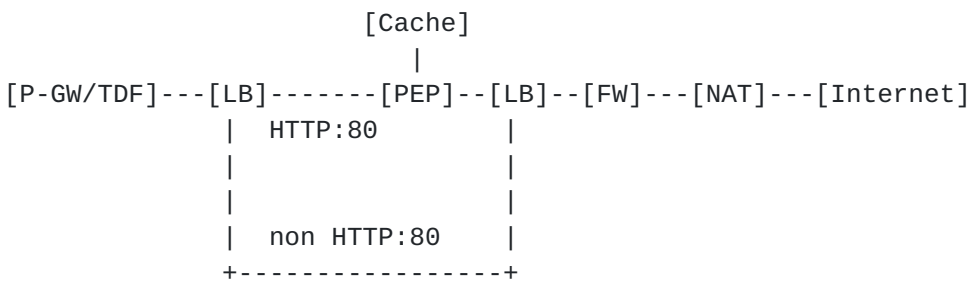

Figure 6: Service function chain for HTTP traffic over TCP port 80.

The first application in this Service Chain example caches web content to help reduce Round Trip Times (RTT) and therefore contributes to improved web page load times. Optimizing RTT and thereby improving Quality of Experience (QoE) is generally more important for mobile service providers than reducing Internet peering costs. Similar arguments hold for cached video content. We also avoid potential large jitter imported from the Internet.

An example for non HTTP port 80 traffic in Figure 6 is UDP-encapsulated IPsec traffic, which is dedicated to port 10000. Note that in a real environment not only port 80 but for example additional traffic via port 8080, 25 for SMTP, 110 for POP3 or 143 for IMAP may be forced to pass a service chain.

A second application is video optimization. Video content from the Internet may not fit to the size of mobile device displays or simply would overload the mobile network when used natively. Therefore mobile operators adapt internet-based video content to ensure the best QoE.

Video content optimization very often is also an additional premium-related component in service offers and price plans.

A typical PEP environment for video optimization consists of three basic service functions as shown in Figure 7: a steering proxy which is able to redirect HTTP traffic, a DPI-based controller which checks for video content and an optimizer which transcodes videos to an appropriate format on the fly in real time.

Figure 7: Service functions required for video optimization.

In Figure 8 we show one possible way for HTTP flows and their redirection in some more detail. The intention here is to show every elementary functional step in a chain as a separate physical or

virtualized item, but this state diagram does not necessarily reflect every existing vendor-specific proprietary implementation.

Specifically, the Steering Proxy includes a TCP proxy and an ICAP (Internet Content Adaptation Protocol) client which communicates with an ICAP server residing in the controller function which is supported by a L7 DPI.

The video optimization process acts on the downstream flow only.

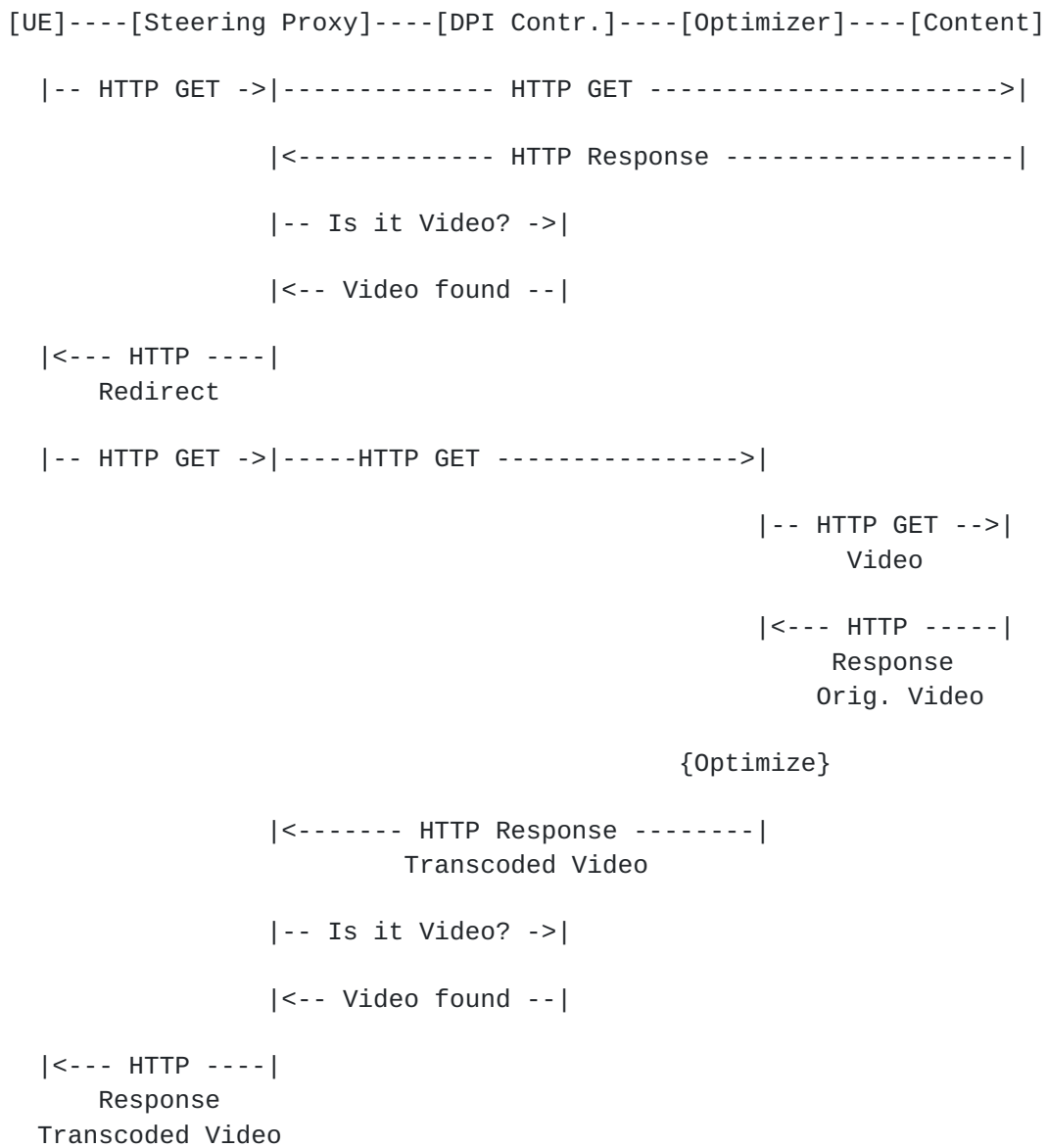

Figure 8: Flow diagram between UE and video optimization PEP.

In such an application scenario one may have reclassification or off-loading on the fly.

Assume a video is streamed within a 4G LTE radio cell. The video optimizer would then apply a transcoding scheme appropriate to the abilities of the 4G network. If one is now leaving the 4G cell and entering a 3G radio cell, the network conditions will most probably become different and the video optimizer has to use another transcoding scheme to keep a certain QoE. This requires that the video optimizer service function is aware of the Radio Access Technology (RAT) in use. One may transfer RAT type from the P-GW (or Gateway GPRS Support Node (GGSN) in case of 3G traffic) via an Authorization, Authentication and Accounting (AAA) Proxy to the service function chain. The RAT information will then be embedded in an appropriate Radius message. Other 3GPP steering mechanisms may apply as well.

If for example the 4G network has sufficient bandwidth, one could also think of another, different use case. The rule could be that only 3G video streams are forced to pass the video optimizer while all 4G video traffic will be bypassed. Bypassing certain Service Functions is also known as off-loading.

Additionally, network utilization information can be used to trigger the behavior of the service function. The degree of video compression applied could depend on the actual current network load.

Last but not least the behavior of the video optimizer service function (or any other service function) could additionally depend on the user-specific service contract (price plan, gold, silver, bronze) or on individual on demand requests.

3.1.1. Weaknesses of current approaches

This use case model highlights the weakness of current service deployments in the areas of traffic selection, reclassification, and multi-vendor support. Traffic in this example is classified after the P-GW or TDF and separated into separate flows based on whether it is (in this example) TCP traffic destined to port 80. This classification could be done by the load balancer (see Figure 6), possibly directed by a TSSF (not shown), if it initiates the service chain selection, or the traffic can be reclassified at the load balancer if the traffic is already embedded in a Service Chain (e.g., when combined with other functions such as the TCP optimization in the following use case). Multi-vendor support is needed because every element in the use case can be provided by a different vendor: load-balancer, HTTP proxy, firewall and NAT.

3.2. Service chain for TCP optimization

The essential parameters influencing TCP behavior are latency, packet loss and available throughput.

Content servers are mostly attached to fixed networks. These are characterized by high bandwidth and low latency. On the other side, Radio Access Networks (RANs) tend to have higher latency, packet loss and congestion.

The fixed network part will typically get a TCP Rx/Tx buffer size different to that on the radio network side because buffer sizes are typically set proportional to the latency (rule of thumb: 2 x latency x bandwidth).

TCP cannot handle such disparate end-to-end situations very well. One way to mitigate this problem is to use split TCP. However, even without congestion, packet losses on the mobile network side may result in time outs and finally cause the content server on the fixed network side to stall.

Therefore mobile operators often use TCP optimization proxies in the data path. These proxies monitor latency and throughput real-time and dynamically optimize TCP parameters for each TCP connection to ensure a better transmission behavior.

A rudimentary service chain setup for TCP optimization is shown in Figure 9. Examples of non-TCP flows are UDP/RTP voice or video traffic.

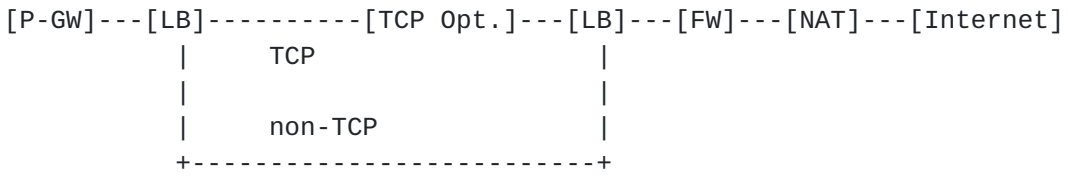

Figure 9: Optimizing TCP parameterization in a mobile network.

3.2.1. Weaknesses of current approaches

This use case highlights weaknesses of current service deployments in the areas of traffic selection, reclassification and multi-vendor support as in the previous use case presented in Section 3.1.

3.3. HTTP header enrichment in mobile networks

3.3.1. HTTP header enrichment in legacy mobile data networks

In legacy mobile networks WAP (Wireless Application Protocol) gateways mediated between traditional mobile phones and the Internet translating HTML web content into a WML (Wireless Markup Language) and vice versa. By functionality, WAP-GWs fit also in the SFC category.

Traditionally WAP-GWs use HTTP header enrichment to insert subscriber related data into WAP and HTTP request headers in real time. These data were (are) used to identify and charge subscribers on third party web sites.

3.3.2. HTTP header enrichment in modern mobile data networks

Today, in 3G and 4G mobile networks HTTP header enrichment is done by the Gateway GPRS Support Node (GGSN)/P-GW/TDF or a dedicated transparent HTTP optimizer as most of the data traffic on a mobile network no longer passes a WAP-GW.

Information typically added to the header includes:

- Charging Characteristics
- Charging ID
- Subscriber ID
- GGSN or PGW IP address
- Serving Gateway Support Node (SGSN) or SGW IP address
- International Mobile Equipment Identity (IMEI)
- International Mobile Subscriber Identity (IMSI)
- Mobile Subscriber ISDN Number (MSISDN)
- UE IP address

3.3.3. HTTP header enrichment security condiderations

In today's networks HTTP header enrichment is commonly used across operator and ISP boundaries. In such cases one must implement security mechanisms, e.g., solutions which are based on a one-time,

session-based key exchanged between user equipment and third party over the top (OTT) service platforms.

4. Remarks on QoS in mobile networks

As indicated in Figure 3, service functions may be linked to the control plane to take care of additional subscriber or service related metadata. In many cases the source of metadata would be the PCRF and the link would be a Diameter-based Gx or Sd reference point. Diameter is specified in [RFC6733], Gx/Sd in [TS.29.212] and St in [TS.23.203].

Service functions within the (S)Gi-LAN are less focused on the explicit QoS steering of the actual mobile wireless network. QoS in mobile networks is based on the 3GPP "Bearer" concept. A Bearer is the essential traffic separation element enabling traffic separation according to different QoS settings and represents the logical transmission path between the User Equipment (UE) and the Packet Gateway (P-GW).

5. Weaknesses of current implementations

In many operator environments every new service introduction can result in a further dedicated (S)Gi-LAN service chain because service chaining has been deployed historically in an ad hoc manner.

It typically requires placement of new functions in the operator's data center, changing the actual wiring to include any new or changed service function, configuration of the functions and network equipment, and finally testing of the new configuration to ensure that everything has been properly setup.

5.1. Granularity of the classification scheme

Often the coarse grained classification according to APNs is not fine enough to uniquely select a service function chain or a processing scheme within a service function chain required to support the typical user-, service- or network- related policies which the operator likes to apply to a specific user plane flow.

It is very likely that an APN, such as shown in Section 2.3, is carrying an extremely diverse set of user traffic. This can range from HTTP web traffic to real-time traffic.

5.2. Service chain implementations

In many carrier networks service chain LANs grow incrementally according to product introductions or modifications. This very often ends in a mix of static IP links, policy based routing or individual VRF (Virtual Routing and Forwarding) implementations, etc. to enforce the required sequence of service functions. Major weak points seen in many carrier networks are:

- Very static service chain instances, hard-wired on the network layer leads to no flexibility with respect to reusing, adding, and removing service nodes and reprogramming service chains.
- Evolutionary grown "handcrafted" connectivity models require high complexity to manage or maintain.
- Basic implementation paradigm is based on APNs (that is service types) only, which requires individual injections of context-related metadata to obtain granularity down to user/service level.
- There is currently no natural (or standardized) information exchange on network status between services and the network, complicating management of network resources based on subscriber profiles.
- It is currently practically impossible to implement an automated service provisioning and delivery platform.
- Scaling up flows or service chains with service or subscriber related metadata is extremely difficult.

6. Operator requirements

Mobile operators use service function chains to enable and optimize service delivery, offer network related customer services, optimize network behavior or protect networks against attacks and ensure privacy. Service function chains are essential to their business. Without these, mobile operators are not able to deliver the necessary and contracted Quality of Experience (QoE) or even certain products to their customers.

6.1. Simplicity of service function chain instantiation

Because product development cycles are very fast in mobile markets, mobile operators are asking for service chaining environments which allow them to instantly create or modify service chains in a very flexible and very simple way. The creation of service chains should be embedded in the business and operation support layers of the

company and on an abstract functional level, independent of any network underlay. No knowledge about internetworking technology should be required at all. The mapping of the functional model of a service chain onto the actual underlay network should be done by a provisioning software package similar to that shown in Figure 10. Details of the architecture and design are the subject of forthcoming standards and proprietary implementation details.

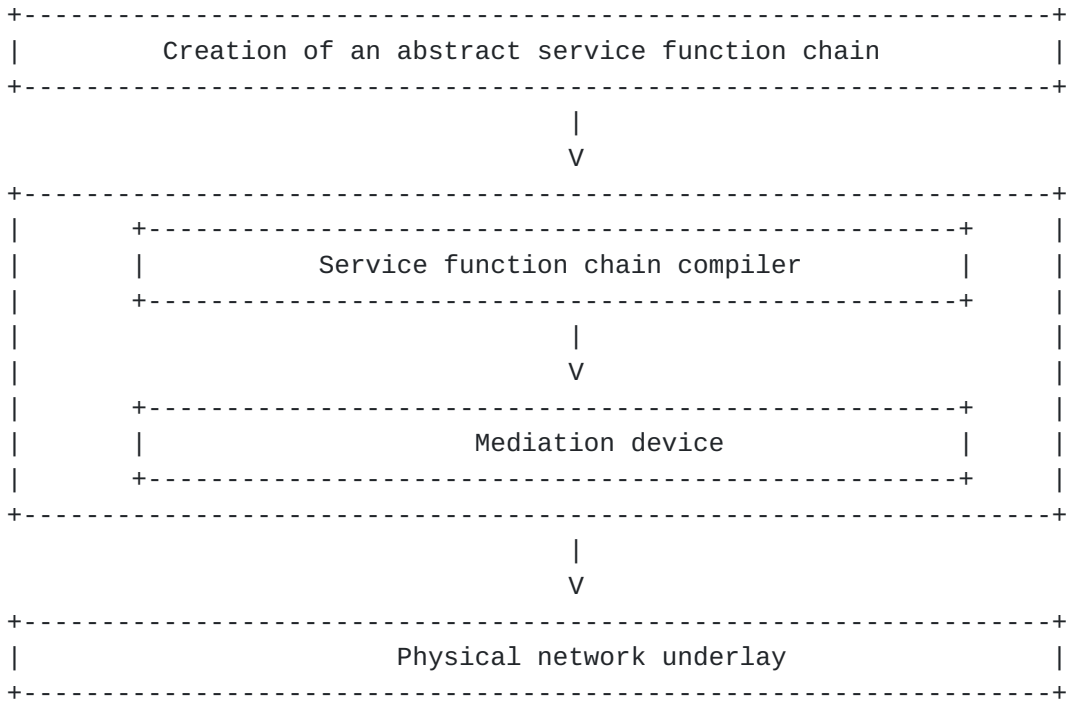

Figure 10: Creation and provisioning system for service function chains.

Service functions can be physical or virtualized. In the near future the majority of mobile service functions will typically reside in the local cloud computing environment of a mobile core location. Nevertheless, first trials have shown that (virtualized) Service Function interconnects via WAN links require careful latency considerations.

Last but not least, any implementation must take into account that in the migration phase a mixed infrastructure including virtual machines, classical hardware "boxes" and bare metal based systems (i.e., computes without using virtualization) must be supported.

6.2. Extensions

A service function chain should be generalized by a directed graph where the vertices (nodes) represent an elementary service function. This model allows branching conditions at the vertices. Branching in a graph could then be triggered by typical 3GPP specified mobile metadata (see Section 2.3) and allow for more sophisticated steering methods in a service chain. Typically these data will be injected by the mobile control plane, commonly but not exclusively by the PCRF via a Diameter-based 3GPP Sd/St reference point.

Service chain behavior and output should additionally depend on actual network conditions. For example, the selection of a video compression format could depend on the actual load of the mobile network segment a mobile user is attached to. That is to say that classification of flows may allow very dynamic inputs while specification of such inputs from a 3GPP network will need to be done by 3GPP or another standards body.

Although necessary metadata can be obtained from the PCRF, to avoid Diameter signaling storms in the (S)Gi-LAN, individual service functions should probably not be attached individually to the control plane. A mechanism where such metadata are carried by a metadata header can reduce requests to the PCRF, provided these extensions do not increase the original payload size too much.

6.3. Reflections on Metadata

At the moment we see just two types of metadata classes. Metadata which are static and related to subscriber and service policies typically reside in the control plane environment and dynamic metadata, which may reflect time and location dependent status somewhere in the network or other service platforms, e.g., load conditions or relevant network technology indicators. It may be useful to have proper interfaces to inject these metadata into the Service Function Chain domain.

Summarized, metadata may by injected into individual Service Chain Functions:

- asynchronously from the control plane environment by means of individual standardized interfaces,
- synchronously, piggypacked with the user IP packet:
  - by means of a to-be-defined metadata header

* or carried with http header enrichments within the user payload.

6.4. Delimitations

A clear separation between service chaining functionality and 3GPP bearer handling is required. This may be subject of forthcoming studies.

7. Security Considerations

Organizational security policies must apply to ensure the integrity of the SFC environment.

SFC will very likely handle user traffic and user specific information in greater detail than the current service environments do today. This is reflected in the considerations of carrying more metadata through the service chains and the control systems of the service chains. This metadata will contain sensitive information about the user and the environment in which the user is situated. This will require proper considerations in the design, implementation and operations of such environments to preserve the privacy of the user and also the integrity of the provided metadata.

8. IANA Considerations

This document has no actions for IANA.

9. Acknowledgments

We thank Peter Bosch, Carlos Correia, Dave Dolson, Linda Dunbar, Alla Goldner, Wim Hendericks, Dirk von Hugo, Konstantin Livanos, Praveen Muley, Ron Parker, Nirav Salot and Takeshi Usui for valuable discussions and contributions.

We especially thank Narseo Vallina Rodriguez (ICSI Berkeley University) for multiple discussions on HTTP header extensions and network security.

10. References

10.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

10.2. Informative References

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

[RFC6459] Korhonen, J., Ed., Soininen, J., Patil, B., Savolainen, T., Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", RFC 6459, DOI 10.17487/RFC6459, January 2012, <http://www.rfc-editor.org/info/rfc6459>.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, DOI 10.17487/RFC6733, October 2012, <http://www.rfc-editor.org/info/rfc6733>.

[RFC7498] Quinn, P., Ed. and T. Nadeau, Ed., "Problem Statement for Service Function Chaining", RFC 7498, DOI 10.17487/RFC7498, April 2015, <http://www.rfc-editor.org/info/rfc7498>.

[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>.

[TS.23.003]
"Numbering, addressing and identification", 3GPP TS 23.003 14.1.0, September 2016.

[TS.23.203]
"Policy and charging control architecture", 3GPP TS 23.203 14.1.0, September 2016.

[TS.23.401]
"General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", 3GPP TS 23.401 14.1.0, September 2016.

[TS.29.061]
"Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)", 3GPP TS 29.061 14.1.0, September 2016.

[TS.29.212]
"Policy and Charging Control (PCC); Reference points", 3GPP TS 29.212 14.1.0, September 2016.

[TS.29.274]
"3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3", 3GPP TS 29.274 14.1.0, September 2016.

[TS.29.281]
"General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)", 3GPP TS 29.281 13.2.0, June 2016.

[TS.33.210]
"3G security; Network Domain Security (NDS); IP network layer security", 3GPP TS 33.210 13.0.0, December 2015.

Authors' Addresses

Walter Haeffner
Vodafone
Vodafone D2 GmbH
Ferdinand-Braun-Platz 1
Duesseldorf 40549
DE

Phone: +49 (0)172 663 7184
Email: walter.haeffner@vodafone.com

Jeffrey Napper
Cisco Systems
Cisco Systems, Inc.
Haarlerbergweg 17-19
Amsterdam 1101 CH
NL

Email: jenapper@cisco.com

Martin Stiemerling
NEC
NEC Europe Ltd.
Kurfuersten-Anlage 36
Heidelberg 69181
DE

Email: mls.ietf@gmail.com

Diego R. Lopez
Telefonica I+D
Don Ramon de la Cruz, 82
Madrid 28006
ES

Phone: +34 913 129 041
Email: diego@tid.es

Jim Uttaro
AT&T
200 South Laurel Ave
Middletown, NJ 07748
US

Email: uttaro@att.com