Distributed Mobility Management (DMM)
Internet-Draft
Intended status: Standards Track
Expires: September 12, 2019

U. Fattore
M. Liebsch
NEC

March 11, 2019

Control-/Data Plane Aspects for N6 Traffic Steering
draft-fattore-dmm-n6-cpdp-trafficsteering-01.txt

Abstract

Current standardization effort on the evolution of the mobile communication system reconsiders the mobile data plane protocol. The IETF DMM Working Group has work that proposes and analyzes various protocols as alternative to the GPRS Tunneling Protocol for User Plane (GTP-U) for an overlay deployment in between the mobile device's assigned data plane anchor and its current radio base station, which are denoted as N9 and N3 interfaces. In the view of some future deployment and the original intent per the very early DMM WG charter, a mobile device's data plane anchor may be highly distributed and re-selected for optimization throughout a mobile device's communication with one or more correspondent services. Such re-configuration has impact on the packet routing in between the mobile device's data plane anchor and the one or multiple data networks hosting the services, which is denoted as N6 interface. This draft proposes and discusses a solution to control, setup and maintain traffic treatment policy on the cellular communication system's N6 interface while taking the UE's PDU session settings per the cellular system's control plane, such as QoS and locator information, into account.

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 September 12, 2019.

Table of Contents

1. 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].

2. Introduction

Recent releases and deployments of cellular mobile communication systems utilize an overlay on the mobile data plane to forward a mobile device's data packets in between the mobile device and an anchor point, which serves as first hop router to the mobile device. The overlay is realized by the GPRS Tunneling Protocol for user plane

(GTP-U), which is able to carry network-specific attributes in the tunnel protocol headers.

The 3rd Generation Partnership Project (3GPP) is in charge of the cellular mobile communication system's specification and is currently finalizing a 15th release, which has fundamental changes compared to previous releases. Such changes include a clean split between control- and data plane functions, more flexible deployment and re-configuration of data plane anchors, as well as support for local data network (DN) access and multi-homing.

In between a mobile device's current radio base station in the radio access network (RAN) and its data plane anchor, the release 15 specification assumes an overlay per the previous releases utilizing GTP-U. The data plane anchor is denoted as User Plane Function (UPF) to anchor a Packet Data Unit (PDU) Session for the mobile device. This draft abbreviates the UPF, which serves a device's PDU session anchor, as UPF_a. In between a UPF_a and the device's current radio base station, none, one or multiple additional UPFs can be deployed to classify uplink traffic in support of policy-based routing to a particular DN without traversing the UPF_a. This draft denotes such intermediate UPF as UPF_i. Interfaces between a DN and a mobile device's UPF_a is denoted as N6, the interface between a UPF_i and one or multiple UPF_a is denoted as N9, and the interface between a UPF_i and a radio base station is denoted as N3. Whereas regular routing of mobile devices' PDUs is assumed on N6, N9 and N3 deploy a GTP-U overlay with UPF_a, UPF_i and the radio base station serving as tunnel endpoints. This end-to-end architecture is depicted in Figure 1. For a more detailed description of anchor and intermediate UPF and associated deployment and operation, please refer to [I-D.bogineni-dmm-optimized-mobile-user-plane] and the 3GPP specification [TS23.501].

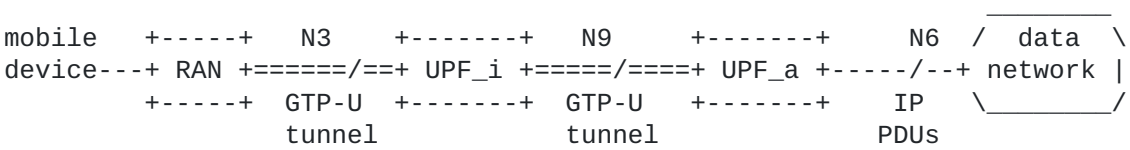

Figure 1: Architecture and interfaces of a 3GPP release 15 data plane in between a data network and a mobile device.

In alignment with the 3GPP's current directions to study data plane protocol candidates which can serve as suitable alternative to GTP-U, the IETF's DMM WG has valuable ongoing individual work that analyzes the GTP-U protocol and derives requirements for an alternative mobile data plane protocol [I-D.hmm-dmm-5g-uplane-analysis], as well as work

that investigates the use of alternative protocol candidates based on SRv6, ID-Locator separation, and locator re-writing in the current release 15 system architecture [I-D.bogineni-dmm-optimized-mobile-user-plane]. The focus of these drafts is on N9 and N3.

In the view of optimization options on the complete end-to-end data plane, [I-D.gundavelli-dmm-mfa] complements other draft and proposes data plane optimization on N6. Such operation is of particular interest when the mobile device's UPF_a is decentralized and deployed close to the device's current radio base station. Such deployment may be preferable for some services, such as edge computing and access to associated edge DNs, and mitigates the role of the UPF_i and N9 interfaces. In particular the selection and configuration of UPF_i instances can omitted and associated signaling costs can be saved. However, such deployment strengthens the expectation on IP-based PDU routing on N6, as the serving DN may not be always topologically close to the device and its current UPF_a. Such requirements include QoS support on N6, metering support and traffic steering in case the mobile device's UPF_a changes while its IP address and associated sessions should continue.

The same requirements on N6 apply for multi-homing per [TS23.501] where the mobile device's UPF_a is close to a first DN (DN1) whereas a UPF_i is used to enable access to a second DN (DN2), either through a secondary UPF_a close to DN2 or directly from the UPF_i, without the use of a secondary UPF_a. Since services in both DNs address the same IP address of the mobile device (IP_ue) to send downlink traffic, both DNs' traffic need to be forwarded to the most suitable (e.g. closest) UPF_a or UPF_i respectively.

This draft focuses on a solution to control, setup and maintain such dedicated routes and additional traffic treatment policy on N6, while taking the UE's PDU session settings per the cellular system's control plane, such as QoS and locator information, into account.

3. Positioning of N6 policy control

This section briefly introduces the relevant mobile system architecture components and interfaces, and covers some high-level use cases which can benefit from data plane policy control on N6 interface endpoints.

3.1. System architecture for mobile access to data networks

The 3GPP's 5G system architecture introduces in the core network a clear control-/user plane separation (CUPS), in order to have flexible deployment of the different functions (e.g., user plane

nodes can scale independently from control plane elements in case of user traffic growth). Again to leverage flexibility and efficiency, the control plane is split in different functions, each offering a specific service, in the so called Service Based Architecture (SBA).

Among all the control plane functions, the Session Management function (SMF) takes care of the session management (session establishment, modification, release), IP allocation and selection of an IP anchor point for the session, as well as traffic steering in between UPFs and radio base stations. In order to manage the user session, the SMF collaborates with other control plane services (e.g., Policy Control Function - PCF - providing policy rules for traffic treatment and monitoring), in particular with the Access and Mobility Management Function (AMF), which manages registration, authentication and authorization and security context. One of the main task of the SMF is to instruct User Plane Functions (UPFs), through N4 interface. When a new session is to be created, the SMF selects one or multiple UPFs for the user traffic and selects one UPF as session anchor (UPF_a). UPF_a acts as a proxy for user traffic, which means all traffic directed to the UE passes through the UPF anchor. Beside the UPF_a, if other UPFs are present (i.e., between the radio base station and the UPF_a), this are deployed as classifiers for user uplink traffic.

In Figure 2 a simplified 5G architecture [TS23.501] is depicted, showing two Data Networks (DN) to whom a user may need a connection. To each Data Network a UPF_a is associated, acting as session anchor and providing to the user an IP address needed for the connection. UPF_a also acts as tunnel termination point, since user traffic is encapsulated on both N3 and N9 interfaces, using the GPRS Tunneling Protocol for User Plane (GTP-U). Whereas, on N6 interface IP PDUs are routed without tunneling.

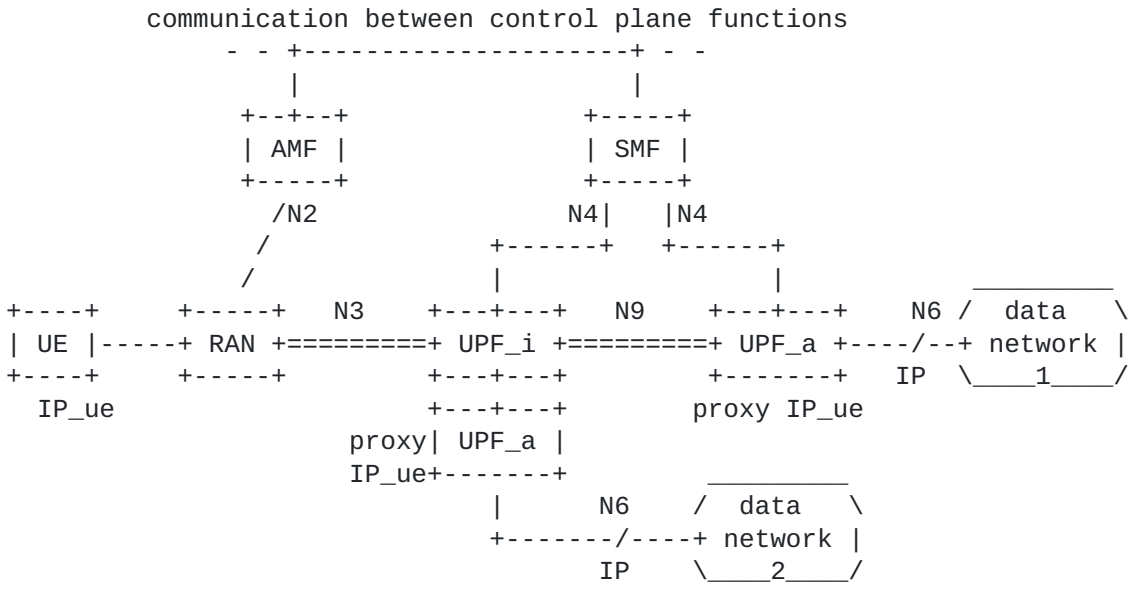

Figure 2: Data plane with a simplified release 15 control plane

Data networks host Application Servers (AS), which provide a services to UEs, and an internal network comprising data plane nodes (DPN), such as routers and switches, to connect the services with the transport network. Both, the transport network and the data network's internal network build the N6 interface, which is depicted in Figure 3. In order to apply traffic treatment policy to uplink traffic in between a UPF and a data network, the UPF receives policies via the N4 interface. For downlink traffic, the AS/DPN should have means to receive traffic treatment policies.

A way to enforce N6 policies to the DPN/AS in a data network is needed. It is evident that this rule must originate from the cellular control plane due to its knowledge about the UE's states, such as its locator or QoS, and when these states are updated or re-configured. Different means to convey and enforce associated traffic treatment policies in a DPN/AS exist, such as the use of routing protocols or control-/data plane configuration protocols.

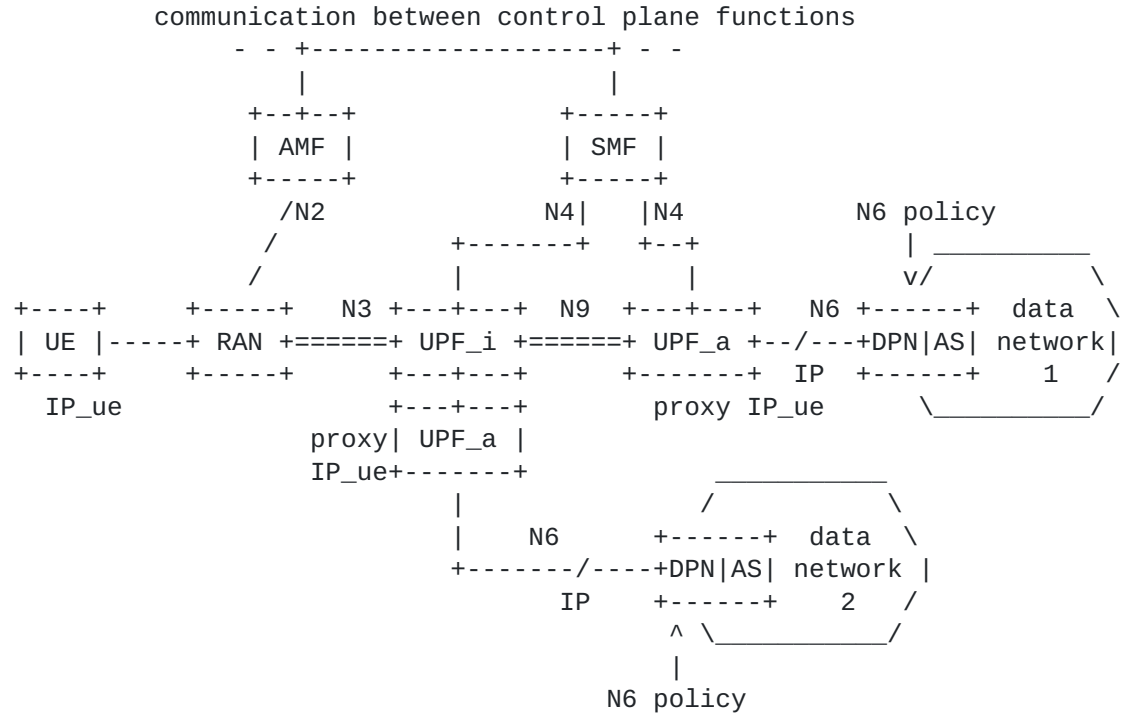

Figure 3: Data network DPN/AS as traffic treatment policy enforcement point

3.2. Use cases with demand for N6 traffic treatment policy

The motivations behind the need for N6 treatment policy are many. Following, some of the use cases are listed and described.

UE to UE communication: a scenario which is not explicitly shown in Figure 2 and Figure 3 is UE to UE communication, when a UPF_a via N6 interface is connected to another UPF_a (belonging to the same or to another network, and controlled by the same of another SMF), with the latter UPF being associated to a second UE. In this scenario, all the data plane elements on the path are controlled by control plane elements of the 5GC (i.e., SMFs), but anyway additional policies on N6 may be forwarded in order to steer traffic on an optimized route directly towards the edge UPF for the specific UE, without passing through the UPF_a.

UE to edge data network: in this use case, the UE connects to an edge Data Network, meaning a DN positioned at the edge of the core network, near to the access network (typical MEC scenario). In mobility, a new UPF_a may be assigned to UE, and routes to the previous edge network would follow a non-optimized path, passing through the new UPF_a for the UE. With traffic treatment policies

this can be avoid, giving a traffic steering policy to the DPN in charge for the edge DN.

Concurrent use of multiple data networks: a possible scenario is the one in which a UE collects the desired content from different data networks (e.g., because of Content Delivery Networks - CDN). To optimize routing in this scenario, the downlink traffic should traverse for each data network the optimized path through the UE and not be forced through a (central) UPF_a common to all the data networks. Again, this can be done with policies on N6 interface. This particular use case also highlights the importance to consider optimization on N6, whereas other works focus on N9: considering a UPF_a near the data network, as proposed in other solutions, would not allow multiple DN access in an unique user session and so would not allow for content access on different destinations.

4. N6 traffic treatment - Requirements and policy types

Use cases for traffic treatment on N6 per a data plane policy include cases where the UPF_a is deployed closer at the mobile edge, e.g. to not only access a local data network in the proximity of the UE, but also other data networks sharing the single edge UPF_a. In that case the N6 interface may span some distance in the transport network in between the data network(s) and the UPF_a. Dependent on the expected QoE/QoS of the traffic, traffic treatment policies for QoS differentiation, packet labeling, etc. may apply to the UE's packets on N6. For uplink traffic, the UE's UPF_a can enforce such traffic treatment policies to uplink traffic, where a DPN associated with the data network(s) (e.g. PE router, transit router, router/switch of the data center transport network, TOR switches of Application Servers, etc.) enforces such policies to downlink traffic.

The same need for traffic treatment policies applies to traffic between a UPF_i, which classifies uplink traffic for forwarding to a local data network, and the data network. Downlink traffic from the local data network to the UE should then be forwarded towards the UPF_i, not via the UE's UPF_a.

In advanced scenarios, the SMF may decide to reconfigure the UE's UPFs, e.g. by relocating the UPF_a or a UPF_i while maintaining the UE's IP address (IP_ue) and data sessions using this IP address. In such case, a DPN associated with the one or multiple data networks, which run correspondent services for the UE, must enforce traffic steering policies to downlink traffic to achieve routing of downlink traffic to the UE's current UPF_a or UPF_i respectively.

In summary, traffic treatment policies that apply to a UE's uplink and downlink traffic on N6 include the following types:

- QoS differentiation and traffic engineering"
- Packet label push/pop"
- Metering
- Traffic steering (e.g. SRv6 rules, locator re-write rules, etc.)
- E dormancy monitoring rules to initiate paging

Requirements for N6 traffic treatment include the following:

- Awareness of UE location information (first hop router accuracy, UPF_a/UPF_i) - Set or update DPN policy for traffic steering
- Awareness of topology - Select and update most suitable UPF (UPF_a/ UPF_i) for the communication with a data network, e.g. after UPF changed
- Availability of initial or updated policies when needed
- No/Low impact on data traffic (packet loss, re-ordering) when policies are updated - DPNs may request/solicit policies or get notified about initial and updated policies

5. Leveraging the mobile control plane for N6 policy control

Methods for N6 policy control consist in instructing the DPNs with rules for traffic steering, QoS policies enforcing, etc. The solution described in this draft is based on leveraging the mobile control plane, in order to introduce some logic to manage and forward policies to DPNs on N6 interface. To do this, the Application Function (AF) defined in 5GS [TS23.501] is used as binding element in between the cellular network control plane and the data network data plane.

Per [TS23.501], the AF is introduced to inter-work with the Policy Control Function (PCF) in order to condition and contribute to some SMF decisions. This happens with the AF sending specific requests to the PCF and the latter translating those requests in policies for the SMF. Depending on the domain in which the AF is located, a Network Exposure Function (NEF) may be in between to enable the AF collaborating with the other control plane elements of the cellular architecture.

In support of the proposed scenario, the AF can solicit data plane policies from the cellular control plane by sending a request. At reception of the policies, the AF can pass the policies on for

further processing and enfocement in the data network's AS/DPN. In this way, DPNs receive from the control plane policies for the user traffic traversing them. The AF may be co-located with a control function, which utilizes the DMM WG's Forwarding Policy Configuration (FPC) protocol to implement policies in the AS/DPN, or leverage an SDN controller for the selection and configuration of AS/DPN.

The policies defined and forwarded by the AF are based on the status of the mobile network, which the AF can obtain from the SMF. In any moment, in fact, the SMF is in charge of keeping track of the selected UPFs and of monitoring the user session. Based on this information, the AF forwards specific rules to a DPN (e.g., traffic steering rules to make the user's traffic reach the most suitable UPF_a). In some cases (e.g., user mobility), the SMF can also change UPFs for a specific user and in this case the AF will receive updated policies for enforcement in the involved AS/DPN.

Figure 4 shows how the previous architecture evolves with the introduction of the AF.

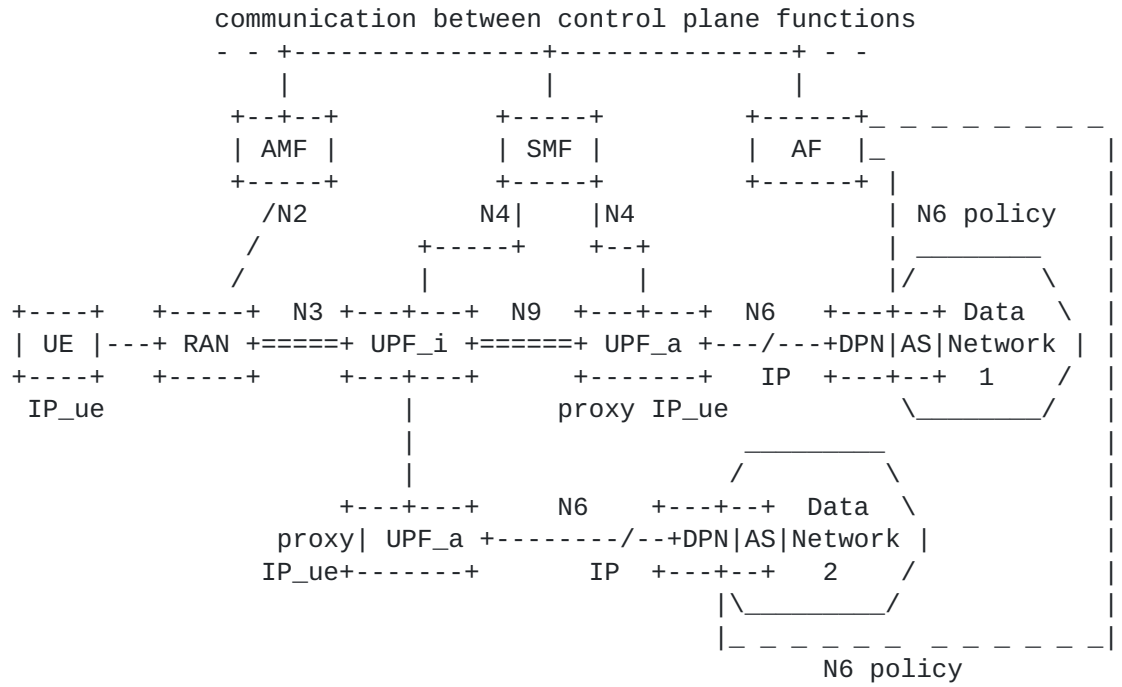

Figure 4: Using AF in control plane for traffic policy enforcement

6. N6 endpoints - loose and tight coupling options

As described in the previous section, we take advantage of the Application Function (AF) to bind the 3GPP's domain functions with those introduced in this draft for N6 policy enforcement. According to [TS23.501], an Application Function may send requests to influence SMF decisions for User Plane (UP) traffic of PDU Sessions (e.g., based on the relocation of an application on the Data Network side, the AF can notify this to the SMF in order to trigger a relocation of UPF(s) from the SMF, to choose a new UPF more suitable for the new Data Network).

In addition, the AF can subscribe to events from the SMF in order to receive notification about UP management events (e.g., when a PDU Session anchor has been established or released).

As defined in [TS23.502], the AF interacts with the PCF/SMF via the NEF or directly and the PCF then forwards requests from the AF towards the SMF as Session Management (SM) Policies. For the sake of simplicity, in this section all the 3GPP's functions apart from the AF are collected under the name of "3GPP's C-PLANE", and the specific service to which the AF interacts in the 3GPP C-PLANE is not relevant for this draft.

In order to forward specific policies to the Data Plane Nodes/ Application Servers (DPNs/ASs) associated with each Data Network, a Network Controller (NC) is considered to be co-located with the AF element. The NC performs the selection of a DPN/AS element based on the received information from the C-PLANE. The AF/NC forwards control messages to a DPN/AS through an AFNC-CPUP interface, giving indications to steer the downlink traffic properly and coherently with the UP updates from the 3GPP's side.

Forwarding N6 polices to the N6 endpoints involved (i.e., UPF and DPN) can happen in two different ways:

1) Tight coupling scenario: The UPF can enforce policies per the AF/NC decisions. The UPF receives associated policies from the 3GPP's C-PLANE. The corresponding DPN/AS receives the policy via teh AFNC-CPUP interface.

2) Loose coupling scenario: A separate DPN function is co-located with the UPF. Main policies for N6 traffic treatment do not traverse the 3GPP's C-PLANE but are controlled at both N6 interface endpoints' DPN by the AF/NC via the AFNC-CPUP interface.

In the tight coupling scenario, the N6 interface configurations for the UPF are all enforced though the 3GPP domain. Therefore, the 3GPP's C-PLANE interacts with the AF/NC element through the AFNC_3GPP interface and receives on this interface requests to influence the UP traffic policies. 3GPP decides if enforce those policies on the UPF(s) involved.

The architecture and interfaces involved in this tight coupling scenario are depicted in Figure 5.

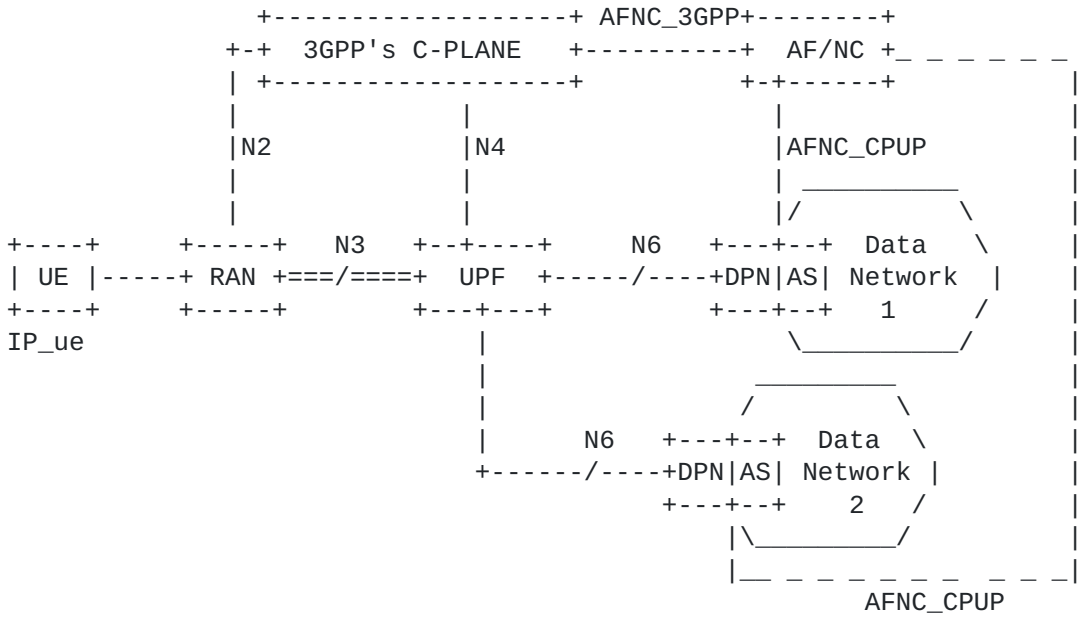

Figure 5: N6 endpoints tight coupling scenario

In Section 7.1 the operation flow and information model for the messages exchanged in this type of coupling are presented and described. Both the cases of a AF/NC-initiated and 3GPP-initiated message flow are considered.

In the loose coupling scenario, an additional DPN element is associated with a UPF and represents a key element to enforce N6 traffic treatment policies on the UPF-side of the N6 interface. This DPN is controlled by the AF/NC through the AFNC_CPUP interface, as depicted in Figure 6.

Loose coupling allows reducing 3GPP's role in the N6 endpoint management, potentially allowing under certain assumptions (e.g., no UPF re-selection is needed), an optimized control of the N6 interface from the AF/NC element, transparently from 3GPP's domain. This kind

of scenario results as an advantage particularly for use cases in which the UPF is deployed in the proximity of the Data Network and far from the 3GPP's C-PLANE (i.e., in a Mobile Edge Computing - MEC - alike scenario).

For particular cases which request 3GPP's C-PLANE involvement (i.e., UPF re-selection or other changes not related to the only N6 endpoint) the AFNC_3GPP is still used for notifications and requests between the AF/NC and the 3GPP's C-PLANE.

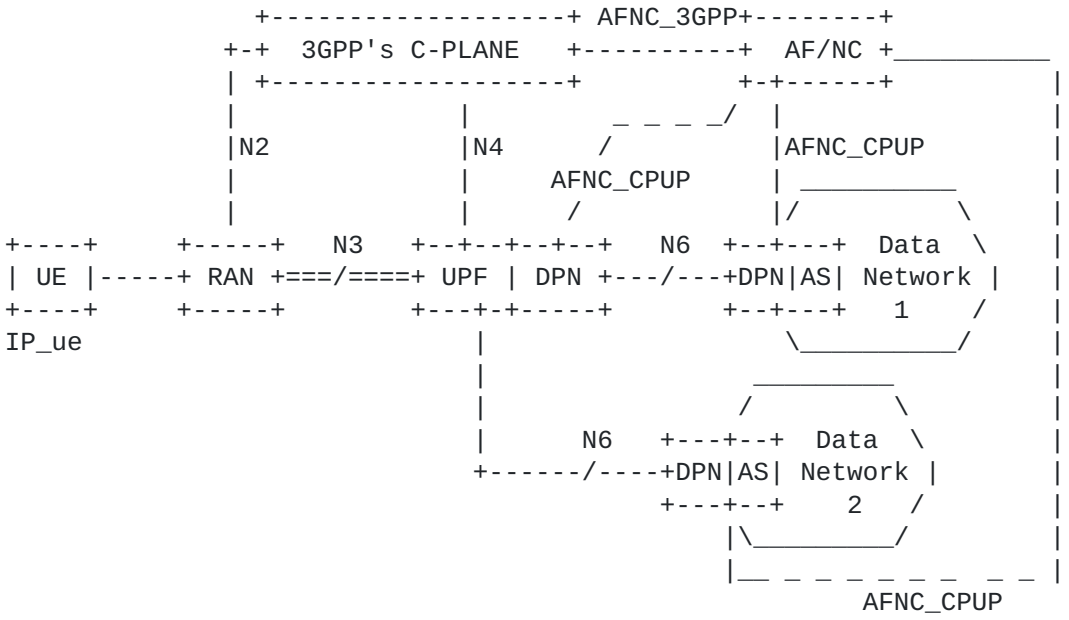

Figure 6: N6 endpoints loose coupling scenario

7. Operations for N6 policy enforcement in a tight coupling scenario

In the following sub-sections, message sequences are shown assuming a tight coupling scenario between N6 interface endpoints, as depicted in Figure 5. Two different operation flows can be distinguished, based on the entity initiating and requesting for the N6 policy. Section 7.1 describes the message sequence in the case of AF/NC-initiated N6 policy request, while Section 7.2 covers the alternative case in which the request for a N6 policy is initiated from the 3GPP's C-PLANE.

In the message sequences, special attention is given to the AFNC_CPUP and AFNC_3GPP interfaces defined in this draft and Information Models for messages exchanged on those interfaces are provided.

7.1. AF/NC-initiated N6 policy enforcement

A N6 policy can be triggered from the AF/NC element and is then forwarded directly to the DPN N6 endpoint (through AFNC_CPUP interface) and indirectly to the UPF N6 endpoint (through AFNC_3GPP interface).

As example, the AF/NC may request updated n6 policies for the following reasons:

- there is the need of a different QoS to be applied to traffic, which is identified in the request.
- there is the need for a re-location of the application to a different Data Network and therefore changes for traffic in uplink on the UPF's N6 endpoint should be applied.

Figure 7 depicts the AF/NC-initiaed N6 policy enforcement message sequence.

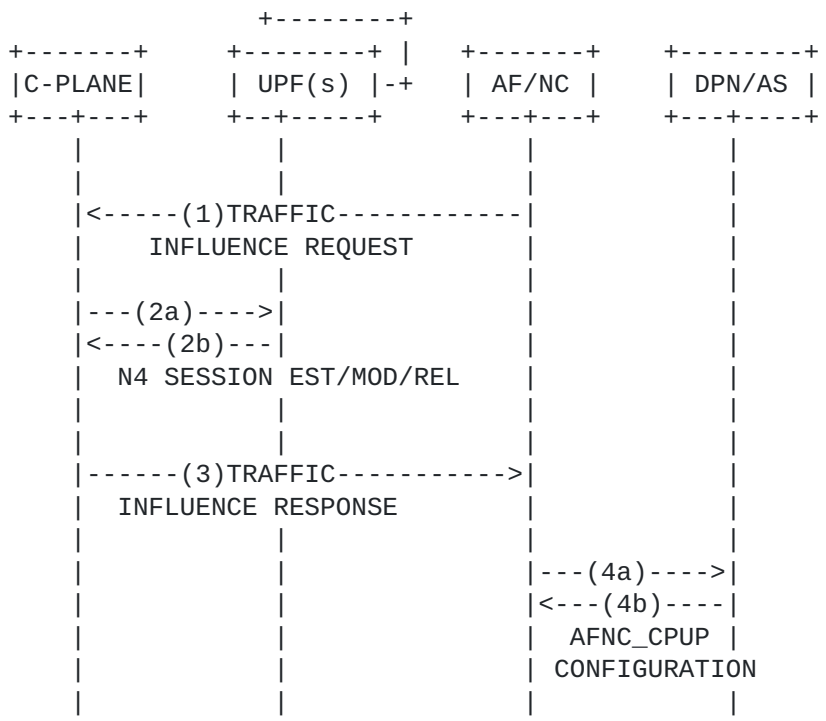

Figure 7: Message flow for AF/NC-initiated N6 policy enforcement

Following, a description for each message is given:

(1) TRAFFIC INFLUENCE REQUEST: this message is sent from the AF/NC to the 3GPP's C-PLANE in order to request a modification for UP traffic. The message contains the fields listed in Table 1.

Information model for TRAFFIC INFLUENCE REQUEST message

Message Fields	Description	Notes
Request ID	Identifies the current request in order to match it with following response messages.	-
Traffic Identifier	Identifies the UP traffic which is targeted by the request. Traffic may be identified based on the session, UE-based or even slice-based (i.e., addressing all the traffic belonging to a specific network slice).	3GPP's identifiers defined in [TS23.501] may be used to identify traffic (e.g., DNN for traffic toward a specific Data Network, NSSAI for a specific slice, UE GUTI for a specific user, etc.)
QoS parameters	Contains the QoS parameters for the targeted traffic	-
DPN N6 endpoint	Brings information about the N6 endpoint on the Data Network side.	-

Table 1

Based on the N6 endpoint information, the 3GPP's C-PLANE may take decisions on UPF(s) selection and re-location. For instance, this field could carry a Data Network Access ID (DNAI), identifying a specific Data Network on which the 3GPP's domain could select the best matching UPF (e.g., based on proximity).

(2a)(2b) N4 SESSION ESTABLISHMENT/MODIFICATION/RELEASE: this are 3GPP's messages defined in [TS23.502] and used to enforce changing to one or more UPF or to select and configure a new UPF. Through this messages, the N6 policies requested from the AF/NC can be enforced to the UPF(s).

(3) TRAFFIC INFLUENCE RESPONSE: this message is sent from the 3GPP's C-PLANE to the AF/NC in order to acknowledge the UP changes made based on the previous request message. The message contains the fields listed in Table 2.

Information model for TRAFFIC INFLUENCE RESPONSE message

Message Fields	Description	Notes
Request ID	Identifies the request message to which this response is referred to.	-
Traffic Identifier	Identifies the UP traffic which is targeted by the request. Traffic may be identified based on the session, UE-based or even slice-based (i.e., addressing all the traffic belonging to a specific network slice).	Traffic actually influenced could differ from the original traffic targeted in the request.
UPF N6 endpoint	Brings information about the N6 endpoint on the 3GPP's side.	-

Table 2

N6 endpoint information on 3GPP's side (e.g., IP address of the N6 endpoint UPF) are used from the AF/NC to set the DPN(s) in order to properly route downlink traffic.

(4a)(4b) AFNC_CPUP CONFIGURATION: This message is used to instruct the DPN(s) involved in the UP changes. For instance, in case of UPF re-selection and UPF's N6 endpoint (e.g., IP address) changing, traffic steering rules for downlink traffic need to be enforced to the DPN. The structure of this message is out of the scope of this draft and candidates for managing this interface are already present (e.g., Forwarding Policy Configuration (FPC) defined in [FPC]).

7.2. 3GPP-initiated N6 policy enforcement

A N6 policy can be triggered by the 3GPP domain. In this case, an initial subscription mechanism is needed, in which one or multiple AF subscribe the 3GPP's C-PLANE in order to receive notification about the subscribed events. Some of the events, of which a AF/NC could be interested in, are:

o re-selection one or multiple UPF(s) from the 3GPP's C-PLANE.

o changes in the UP traffic QoS parameters.

o etc.

Figure 8 depicts the message sequence described the AF subscription and a notification from the 3GPP's domain when the specific event occurs.

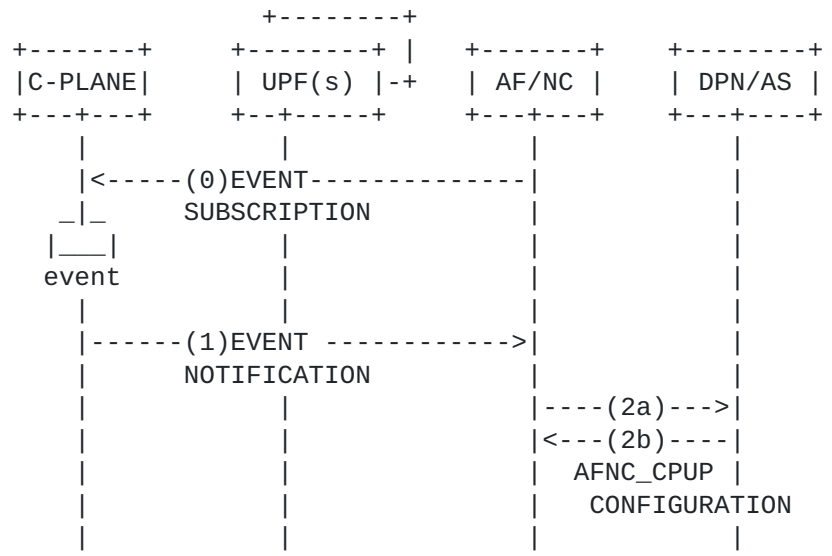

Figure 8: Message flow for 3GPP-initiated N6 policy enforcement

The messages used are here described:

(0) EVENT SUBSCRIPTION: this message is sent from the AF/NC to the 3GPP's C-PLANE in order for the AF/NC to subscribe to some specific UP events. When received from the 3GPP's C-PLANE, all future UP events (e.g., UPF re-selection, changing in UP traffic parameters) which match with the subscription will be notified to the AF/NC. This message fields are listed in Table 3.

Information model for EVENT SUBSCRIPTION message

Message Fields	Description	Notes
Subscription ID	Identifies the subscription in order to then match the resulting notification.	-
Event	Identifies the type of event to which the subscription is referred. For instance, the subscription could refer only to an UPF re-selection event, or may refer to any event for the targeted traffic.	Can be 'all-events' or identify a specific type of event.
Traffic Identifier	Identifies the UP traffic which is targeted by the request. Traffic may be identified based on the session, UE-based or even slice-based (i.e., addressing all the traffic belonging to a specific network slice).	3GPP's identifiers defined in [TS23.501] may be used to identify traffic (e.g., DNN for traffic toward a specific Data Network, NSSAI for a specific slice, UE IP address for a specific user, etc.)

Table 3

(1) EVENT NOTIFICATION: this message is sent from the 3GPP's C-PLANE to the AF/NC, triggered by the subscribed event for the targeted traffic. If no subscription for the specific traffic and event was received before the modification occurs the 3GPP's C-PLANE will not provide any notification for the UP traffic changes. Table 4 lists the field contained in the message.

Information model for EVENT NOTIFICATION message

Message Fields	Description	Notes
Subscription ID	Identifies the subscription message to which this notification is referred to.	-
Traffic Identifier	Identifies the UP traffic which has been change.	Even if there is no notification for traffic which has not been targeted through a subscription, this field may refer to a subset of the traffic targeted in the subscription (e.g., subscription to a specific user traffic and modification of only one PDU sessions for that user).
QoS parameters	Brings information about QoS parameters which have been changed.	-
UPF N6 endpoint	Brings information about the N6 endpoint on the 3GPP's side which have been changed.	-

Table 4

(2a)(2b) AFNC_CPUP CONFIGURATION: This message is used to instruct the DPN(s) involved in the UP changes. For instance, in case of UPF re-selection and UPF's N6 endpoint (e.g., IP address) changing,

traffic steering rules for downlink traffic need to be enforced to the DPN. The structure of this message is anyway out of the scope of this draft and candidates for managing this interface are already present (e.g., Forwarding Polciy Configuration (FPC) defined in [FPC]).

8. IANA Considerations

No IANA action is required for this version of the draft.

9. Security Considerations

Since the solution proposed in this document utilizes the AF to solicit and receive N6 traffic treatment policies from the cellular system's control plane, the trust relationship between the AF and the cellular system's domain matters. In case the AF is located in a different administrative domain, the communication from and to the AF may happen via the system's Network Exposure Functions (NEF). The semantic to request and receive the N6 policy at the AF and in particular the policy types and their descriptions must be aligned to the trust relationship.

Also, the trust relationship between the AF and the DPN/AS matters and a secure direct or indirect (e.g. through an Network Controller) interface, must be ensured.

10. Acknowledgments

The research leading to these results has been partially supported by the H2020-MSCA-ITN-2016 framework under grant agreement number 722788 (SPOTLIGHT).

Authors want to thank Sri Gundavelli, John Kaippallimalil and Shunsuke Homma for their interest and feedback to the use cases and the solution principles for N6 traffic treatment policies.

11. 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>.

[I-D.hmm-dmm-5g-uplane-analysis] Homma, S., Miyasaka, T., Matsushima, S., and d. daniel.voyer@bell.ca, "User Plane Protocol and Architectural Analysis on 3GPP 5G System", draft-hmm-dmm-5g-uplane-analysis-02 (work in progress), October 2018.

[I-D.gundavelli-dmm-mfa]
Gundavelli, S., Liebsch, M., and S. Matsushima, "Mobility-aware Floating Anchor (MFA)", draft-gundavelli-dmm-mfa-01 (work in progress), September 2018.

[I-D.bogineni-dmm-optimized-mobile-user-plane]
Bogineni, K., Akhavain, A., Herbert, T., Farinacci, D., Rodriguez-Natal, A., Carofiglio, G., Auge, J., Muscariello, L., Camarillo, P., and S. Homma, "Optimized Mobile User Plane Solutions for 5G", draft-bogineni-dmm-optimized-mobile-user-plane-01 (work in progress), June 2018.

[FPC] S.Matsushima, L.Bertz, M.Liebsch, S.Gundavelli, D.Moses, C. Perkins, "Protocol for Forwarding Policy Configuration (FPC) in DMM.", 3GPPTS 23.501, June 2018.

[TS23.501]
3rd Generation Partnership Project (3GPP), "Technical Specification TS23.501, System Architecture for the 5G System, Release 15.", 3GPPTS 23.501, June 2018.

[TS23.502]
3rd Generation Partnership Project (3GPP), "Technical Specification TS23.502, Procedure for the 5G System, Release 15.", 3GPPTS 23.502, June 2018.

Authors' Addresses

Umberto Fattore
NEC Laboratories Europe GmbH
Kurfuersten-Anlage 36
D-69115 Heidelberg
Germany

Email: umberto.fattore@neclab.eu

Marco Liebsch
NEC Laboratories Europe GmbH
Kurfuersten-Anlage 36
D-69115 Heidelberg
Germany

Email: marco.liebsch@neclab.eu