|  |
| --- |
| 3GPP TR 23.700-18 V1.1.0 (2022-10) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on system enabler for service function chaining(Release 18) |

|  |
| --- |
|   |

|  |  |
| --- | --- |
|  |  |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms and abbreviations 8

3.1 Terms 8

3.2 Abbreviations 8

4 Architectural Assumptions and Principles 8

5 Key Issues 9

5.1 Key Issue #1: Traffic Steering Policy and SFC Enhancements 9

5.1.1 Description 9

5.2 Key Issue #2: Exposure to enable AF to request predefined SFC for traffic flow(s) related with target UE(s) 9

5.2.1 Description 9

6 Solutions 10

6.0 Mapping of Solutions to Key Issues 10

6.1 Solution #1: Re-use of existing TSP for N6-LAN 10

6.1.1 Description 10

6.1.1.1 Solution Description 10

6.1.1.2 Analysis of Stage 1 requirements 11

6.1.2 Procedures 13

6.1.3 Impacts on existing nodes and functionality 13

6.2 Solution #2: AF influence with explicit traffic steering policies per flow 14

6.2.1 Description 14

6.2.2 Procedures 14

6.2.3 Impacts on existing nodes and functionality 15

6.3 Solution #3: AF influencing Service Function Chaining support by 5GC 16

6.3.1 Description 16

6.3.2 Procedures 17

6.3.2.0 Introduction 17

6.3.2.1 Procedure to associate SFC with certain traffic and UE(s) 18

6.3.2.2 Procedure to associate SFC with an individual UE 19

6.3.2.3 Discovery of available SFCs 20

6.3.2.4 Selection of an UPF that supports the proper SFC/SFP 20

6.3.3 Impacts on existing nodes and functionality 21

6.4 Solution #4: SFC support in 5GS 21

6.4.1 Description 21

6.4.1.1 Architecture Assumption 22

6.4.2 Procedures 24

6.4.3 Impacts on existing nodes and functionality 27

6.5 Solution #5: UPF enhancement with SFC capability 27

6.5.1 Description 27

6.5.2 Procedures 29

6.5.2.1 N6-LAN traffic steering with SFC capabilities 30

6.5.2.2 AF influenced traffic steering with SFC capabilities 30

6.5.3 Impacts on existing nodes and functionality 31

6.6 Solution #6: Service Function Chaining Configuration 32

6.6.1 Description 32

6.6.2 Procedures 32

6.6.3 Impacts on existing nodes and functionality 33

6.7 Solution #7: Enhancing Application Function influence on traffic routing to an N6-LAN based on pre-defined SFC policies 33

6.7.1 Description 33

6.7.2 Procedures 34

6.7.2.1 AF requesting SFC policies in a 3GPP network 34

6.7.2.2 AF influence on traffic routing by including pre-defined SFC policies 36

6.7.3 Impacts on services, entities and interfaces 37

6.8 Solution #8: AF request predefined SFC for traffic flow(s) related with target UE(s) 37

6.8.1 Description 37

6.8.2 Procedures 39

6.8.2.1 Handling an AF request targeting an individual UE address 39

6.8.2.2 Handling an AF request not identified by an UE address 39

6.8.2.3 Traffic steering enforcement control 40

6.8.3 Impacts on existing nodes and functionality 41

7 Overall Evaluation 42

8 Conclusions 42

Annex A: Pre-Rel-18 Traffic Steering Control 44

Annex B: Change history 47

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, certain modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

NOTE 1: The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

NOTE 2: The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

NOTE 3: The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

NOTE 4: The constructions "can" and "cannot" shall not to be used as substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

NOTE 5: The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The Technical Report studies and performs evaluations of potential architecture enhancements to enhance the support of service function chaining in the 5G Core network (5GC). Specifically, two objectives are included:

WT#2: Investigate whether traffic steering policy is sufficient to support SA WG1 requirements in TS 22.101 [5], TS 22.261 [6] and TS 22.115 [7], study whether and how to define Service Function Chaining (SFC) policies, and investigate solutions and procedures for the 5G network with SFC capabilities to identify/detect/classify user plane traffic and steer the traffic to a chain of ordered service functions for SFC processing in non-roaming and home routed roaming scenarios.

WT#3: Depending on the outcome of WT#2, specify possible enhancement to northbound APIs for allowing an AF to request network capability exposure functionalities, e.g. request a service function chain for a certain traffic flow, etc. based on service level agreement with the third party.

NOTE 1: This study considers only traffic handled over N6 by PSA UPF(s) in 5G network.

NOTE 2: The definition of terms in RFC 7665 [8] may be re-used when applicable. The study targets the use of traffic steering concept, e.g. defined by 3GPP (FMSS) and SFC mechanisms defined in IETF when applicable. Especially the study aims at reusing user plane mechanisms (e.g. VXLAN, NSH, GENEVE, GRE, VLAN, etc.) defined at IETF to support SFC, as applicable.

NOTE 3: The study for SFC will ensure that existing (per 3GPP Rel-17) deployments flexibility can be preserved in deployments of SFC in 5G network.

NOTE 4: The study assumes a Home Routed roaming PDU Session does not have an offloading point in a VPLMN.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G system, Stage 2".

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System".

[5] 3GPP TS 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Service aspects; Service principles".

[6] 3GPP TS 22.261: "Service requirements for next generation new services and markets; Stage 1".

[7] 3GPP TS 22.115: "Service aspects; Charging and billing".

[8] IETF RFC 7665: "Service Function Chaining (SFC) Architecture".

[9] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane Nodes".

[10] IETF RFC 7665: "Service Function Chain (SFC) Architecture".

[11] IETF RFC 8300: "Network Service Header (NSH)".

[12] 3GPP TS 22.105: "Services and service capabilities".

# 3 Definitions of terms and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1], in TS 23.501 [2] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1] or in TS 23.501 [2].

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1], in TS 23.501 [2] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1] or in TS 23.501 [2].

SF Service Function

SFC Service Function Chaining

# 4 Architectural Assumptions and Principles

The concept of the SFC is as shown in Figure 4-1 and the following assumptions are applied in this study:

- Each service function (SF) is an opaque processing element in user plane. The SF forwarder, and SF behaviour/control are out of scope of this study that reuses the features defined by IETF for these purposes.

- The initial classification for the service chain to be applied to traffic flow is performed by 5GC.

- The management aspects of SFs, service function paths (SFP), and service function chains are out of scope of the present TR.

- Several service function chains can be simultaneously applied within 5GC of an operator network to meet various business requirements with third parties based on service level agreements. A traffic flow of a PDU Session is subject to a single SFP at a given time.

- The definition of terms and mechanisms in RFC 7665 [8] may be re-used when applicable.

- The study targets the use of traffic steering concept, e.g. defined by 3GPP (FMSS) and SFC mechanisms defined in IETF when applicable. Especially the study aims at reusing user plane mechanisms (e.g. VXLAN, NSH, GENEVE, GRE, VLAN, etc.) defined at IETF to support SFC, as applicable.



Figure 4-1: Illustration of the service function chaining concepts

For all objectives, the architectural assumptions and principles include:

- Solutions shall build on the 5G System architectural principles as in TS 23.501 [2], including flexibility and modularity for newly introduced functionalities.

- Service path (i.e. for traffic handled by the service functions) is traversed over N6 after PSA UPF(s) in 5G network.

- The case where SFC would apply for a Home Routed roaming PDU Session at an offloading point in a VPLMN is not considered in this study.

- Existing (per 3GPP Rel-17) deployments flexibility should be preserved in deployments of SFC in 5G network.

# 5 Key Issues

## 5.1 Key Issue #1: Traffic Steering Policy and SFC Enhancements

### 5.1.1 Description

Currently, the SMF may be configured with the traffic steering policy related to the mechanism enabling traffic steering to the N6-LAN, DN and/or DNAIs associated with N6 traffic routing requirements provided by the AF. Also, UPF with SFC capabilities need to support flexible SFC configuration for a PDU session that requires different SFC processing for different applications. Based on architectural assumptions and principles in clause 4 and service requirements in clause 6.35 of TS 22.261 [6], this key issue is for WT2 to study:

- Whether the existing traffic steering policy is enough to fulfil the SA1 requirements or needs to be enhanced for SFC, and if it needs to be enhanced whether SFC policy need to be defined and how it relates to traffic steering policy. If SFC policy is defined, based on the SFC policy definition, what are the required architecture enhancement for the network functions, interfaces, and the procedures to enforce SFC policies and/or traffic steering policies to identify/detect/classify user plane traffic and steer the traffic flows of the UEs requiring SFC processing for their applications in non-roaming scenarios.

- If SFC policy is defined, based on the SFC policy definition:

- Whether and how the HPLMN can apply traffic steering policies and/or SFC polices for home routed traffic for cases that UE is at VPLMN, UE returns from VPLMN to HPLMN, or UE changes of serving VPLMN.

- What are the relationship between traffic steering and SFC processing in the user plane.

- What (if any) are the new features that the UPF may support in order to allow improved Rel-18 SFC capabilities.

- Whether and how to enhance interfaces and procedures to support UPF with SFC capability including how such capabilities may be available, discovered, and controlled by the SMF.

NOTE: 5GC exposure aspects are addressed in another Key Issue.

## 5.2 Key Issue #2: Exposure to enable AF to request predefined SFC for traffic flow(s) related with target UE(s)

### 5.2.1 Description

For allowing an AF, e.g. a third party AF, to request predefined SFC for traffic flow(s), etc. (when the AF belongs to a third party, this is based on service level agreement with the third party), this key issue will study solutions on:

- How to enable support for AF to request usage of predefined SFC/SFP(s) for traffic flow(s) related with target UE(s).

- Whether and if yes how to enhance network capability exposure functionalities based on solutions of the User plane related Key issue (WT#2). This includes leveraging that Key issue work on whether the existing traffic steering policy is enough to fulfil the SA1 requirements.

- Based on the requests from the AF, what are the solutions and procedures to interact with network functions in the 5GC.

# 6 Solutions

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |
| --- | --- |
|  | Key Issues |
| Solutions | #1 | #2 |  |  |
| Solution based on existing TSP for N6-LAN | X |  |  |  |
| AF influence with explicit traffic steering policies per flow |  | X |  |  |
| AF influencing Service Function Chaining support by 5GC |  | X |  |  |
| SFC support in 5GS | X | X |  |  |
| UPF enhancement with SFC capability | X |  |  |  |
| Service Function Chaining Configuration |  | X |  |  |
| Enhancing Application Function influence on traffic routing to an N6-LAN based on pre-defined SFC policies | X |  |  |  |
| Solution X: AF to request predefined SFC for traffic flow(s) related with target UE(s) | X | X |  |  |

## 6.1 Solution #1: Re-use of existing TSP for N6-LAN

### 6.1.1 Description

#### 6.1.1.1 Solution Description

This solution is based on the existing Rel-17 solution for steering the subscriber's traffic to appropriate operator or 3rd party service functions (e.g. NAT, antimalware, parental control, DDoS protection) in the N6-LAN, as described in e.g. TS 23.503 [4]. The solution is also summarized in Annex A.

The solution is based on the following key aspects, based on existing standards:

- The PCF determines a policy per SDF/application for the purpose of steering the subscriber's traffic to appropriated N6 service functions deployed by the operator or a 3rd party service provider. The policy is expressed in a Traffic Steering Policy (TSP) ID that may be separate in UL and DL directions.

- The TSP ID refers to a traffic steering behaviour that is configured in the SMF/UPF.

- The PCF provides the TSP ID in the PCC rules to SMF.

- The UPF indicates its capability to support traffic steering in N4 and in UPF profile in NRF, as described in TS 29.244 [9]. The SMF may take this capability into account when selecting UPF.

- The SMF instructs the UPF to perform necessary actions to enforce the traffic steering policy referenced by the PCF. This includes the provisioning of corresponding PDRs, FARs, QERs etc. In particular, the SMF creates a FAR with the Forwarding Policy parameters set to the TSP ID.

- The UPF performs the necessary actions to enforce the forwarding policy referenced by the SMF, e.g. performing packet marking and routing the traffic towards the service functions within the N6-LAN.

As referred in clause 6.3.3 of TS 23.501 [2], several parameter(s) and information may be considered by the SMF for UPF selection and re-selection, e.g.:

- Capability of the UPF and the functionality required for the particular UE session: An appropriate UPF can be selected by matching the functionality and features required for a UE.

- How the SMF determines information about the user plane network topology and what information is considered by the SMF, is based on operator configuration.

In this particular context, SMF shall be able to select appropriate UPF regards specific Traffic Steering Policy based on:

- If UPF indicated that Traffic Steering is supported by the UP function (TRST flag already present in clause 8.2.25 of TS 29.244 [9] and part of association procedure).

- It is assumed that 5GC configuration is homogeneous for providing the same set of traffic steering policies within same DNAI/ DNN/ S-NSSAI. SMF can select then, UPF based on DNAI / DNN / S-NSSAI.

#### 6.1.1.2 Analysis of Stage 1 requirements

Below the new SA WG1 requirements introduced for SFC in Rel-18 are listed and comparison with the current TSP based solution is provided.

Table 6.1.1-1: Analysis of Stage 1 requirements

|  |  |  |
| --- | --- | --- |
| TS | Stage 1 requirement | Comment |
| TS 22.101 [5] | *30 Flexible Mobile Service Steering**30.1 Introduction**In order to realize efficient and flexible mobile service steering in (S)Gi-LAN, the network operator uses information (e.g. user profile, network operator's policies, RAT type, application characteristics) to define traffic steering policies. These policies are used to steer the subscriber's traffic to appropriate enablers (e.g. NAT, antimalware, parental control, DDoS protection) in the (S)Gi-LAN.**The term (S)Gi-LAN used in the present document represents a system which is out of 3GPP scope. Corresponding term for the 5G network is N6-LAN.**For traffic steering to service functions in 5G network, enhancement beyond the service requirements below are defined in TS 22.261 [6].* | These are pre-rel-18 requirements. Fulfilled based on TSP ID. |
| TS 22.261 [6] | *6.35 Service Function Chaining**6.35.1 Introduction**In order to support enhancement of service function chaining for 5G networks beyond the requirements for FMSS in TS 22.101, the network operator defines service function chaining policies for service function chaining to steer the traffic associated to the application and its users on per UE basis to appropriate ordered service functions.**A service function chain for 5G networks contains service functions such as firewall functions, NAT, antimalware, parental control, DDoS protection, TCP proxies, load balancers, KPI monitoring, and video optimization, etc.**NOTE: these are non-exhaustive examples of service functions. Other service functions can be provided by an operator.**6.35.2 General Requirements**The following requirements apply for supporting enhancement of service function chaining for 5G networks:**The network operator shall be able to define and modify service function chaining policies for steering traffic on per application per UE basis through required service function chaining with ordered service functions to improve the user's QoE.**Service functions chaining policies shall be able to distinguish between upstream and downstream traffic.* | Current solution already allows to steer the traffic per application and UE basis to appropriate ordered service functions using Traffic Steering Policy (TSP)PCF can send this TSP to SMF. SMF can send PDRs to UPF using associated FAR forwarding policies. It can be modified and distinguished between upstream and downstream as it is needed with a specific PDR with PDI elements for uplink matching criteria and other for downlink. |
|  | *The coexistence of traffic with and without service function chaining shall be supported.* | Coexistence of traffic with and without service function chaining is supported as Traffic Steering Policy (TSP), routing influence, and forwarding parameters in FAR on N4 are optional. |
|  | *Service function chaining shall provide suitable means for authorized third parties to request a chain of service functions provided by the network operator based on operator's service function chaining policies.* | AF can already influence traffic routing by providing routing information with e.g. routing profile ID that may refers to a pre-agreed policy between the AF and the 5GC. However, an enhancement is proposed in Solution #2. |
|  | *In case of roaming, the HPLMN shall be able to apply traffic steering policies and service function chaining polices for home routed traffic.* | Service Chaining based on TSP ID already covers HPLMN to apply the steering policies for home routed roaming. |
|  | *In case of roaming with local breakout, the HPLMN shall be able to provide the traffic steering policies and service function chaining policies to the VPLMN providing local breakout with support of service function chaining.* | This point was scoped out from the SA WG2 study. |
|  | *Service function chaining shall support deployments where the Hosted Services are provided by the operator and deployments where the Hosted Services are provided by a third party.* | This is up to operator deployment and SLA with third parties. It is supported by current traffic steering solution as described in TS 23.503 [4]:"The traffic steering control consists in …<snip>… applying a specific N6 traffic steering policy for the purpose of steering the subscriber's traffic to appropriated N6 service functions deployed by the operator or a 3rd party service provider as described below." |

There are also additional SA WG1 requirements related to service function management and charging (including also clause 5.2.14 of TS 22.105 [12]). These are not explicitly analysed above since:

- SF deployment, management and definition are out of scope of SA WG2.

- SF charging is out of scope of SA2. It could however be noted that the TSP based solution allows differentiated charging per service chain, since the PCF can select Charging Key in the PCC rule based e.g. on TSP ID.

- Service Chains are predefined by the operator and then be referenced by TSP ID.

- Steering protocols to be used (e.g. for encapsulation and/or packet marking) are configured at UPF based on SLA, and it is out of scope of 3GPP what is already described in RFC standards.

### 6.1.2 Procedures

The procedure below shows an example with dynamic PCC Rules. It is also possible to activate predefined PCC Rules with traffic steering policy applied by UPF (not shown in the figure).



Figure 6.1.2-1: Procedure using traffic steering policy

1. The PCF makes a policy decision and creates a PCC Rule with SDF filter information or Application ID, TSP IDs, Charging Key, etc.

2. The SMF creates N4 rules based on the PCC Rule content.

3. The UPF applies the configured forwarding behaviour to steer the traffic to the appropriate Service Chain based on TSP IDs, e.g. encapsulation, packet marking, forwarding.

### 6.1.3 Impacts on existing nodes and functionality

No impacts to current standard.

Assumptions: All UPFs in the operator network serving as PSA for the DNN/S-NSSAI/DNAI that is used for traffic that is potentially subject to SFC controls need to be configured with traffic steering information towards all SFPs supported on that DNN/S-NSSAI/DNAI.

## 6.2 Solution #2: AF influence with explicit traffic steering policies per flow

### 6.2.1 Description

In order to fulfill traffic steering policies using AF routing influence directly, without re-using the existing routing profiles provided by AF, it can be added new elements in the interface so that traffic steering policies can be explicitly requested per flow.

The PCF then provides PCC rules including traffic steering policies based on the traffic steering that are explicitly requested from AF (directly or through NEF).

Note that currently in PCC rule information in 5GC, the traffic routing policies and traffic steering policies are considered mutually exclusive (see NOTE 18 in table 6.3.1 of TS 23.503 [4]). That means that the PCC rule either indicates traffic steering or N6 traffic routing, but not both simultaneously. It is also not clear how the UPF would handle a PCC Rule that contains (potentially conflicting) Routing Profile IDs and Traffic Steering Policy IDs. Therefore, in order to not impact further in PCF, SMF and UPF, the proposal is to add new traffic steering rules ID(s) from AF in mutually exclusive way with current routing info and/or routing profile ID.

This solution thus proposes to add Traffic Steering Policy ID(s) to the existing Nnef\_TrafficInfluence (and NpcfPolicyAutorization, Nudr\_DataNotification). The AF request can either contain AF-TSP-ID(s) (if two Traffic steering policy identifiers are provided, then one is for uplink direction, while the other one is for downlink direction) for Service Chaining or Traffic Routes for steering to a local DN, not both. PCF may use AF-TSP ID(s) directly, or map to locally defined TSP ID(s) provided to the SMF in the PCC Rule to avoid that AF needs to know how TSP ID are set in the 5GC and therefore isolate it from system configuration changes.

As referred in clause 6.3.3 of TS 23.501 [2], several parameter(s) and information may be considered by the SMF for UPF selection and re-selection, e.g.:

- Capability of the UPF and the functionality required for the particular UE session: An appropriate UPF can be selected by matching the functionality and features required for a UE.

- How the SMF determines information about the user plane network topology and what information is considered by the SMF, is based on operator configuration.

In this particular context, SMF shall be able to select appropriate UPF regards specific Traffic Steering Policy based on:

- If UPF indicated that Traffic Steering is supported by the UP function (TRST flag already present in clause 8.2.25 of TS 29.244 [9] and part of association procedure).

- It is assumed that 5GC configuration is homogeneous for providing the same set of traffic steering policies within same DNAI/ DNN/ S-NSSAI. SMF can then select then, UPF based on DNAI / DNN / S-NSSAI.

### 6.2.2 Procedures

The procedure below shows an example of AF using the Traffic Influence API to allow an AF to request a predefined SFC.



Figure 6.2.2-1: Procedure using traffic steering policy

1. AF uses Nnef\_TrafficInfluence API to influence how to route a specific traffic on specific session, by providing the UE IP address together with the request. The AF includes AF Traffic Steering Policy ID(s) in the request. The NEF identifies the PCF serving the PDU Session and triggers a Npcf\_PolicyAuthorization Request, as described in clause 4.3.6.4 of TS 23.502 [3].

2. AF uses Nnef\_TrafficInfluence API to influence how to route a specific traffic for a UE ID or a group of UEs, by providing UE ID (GPSI) or External Group ID together with the request. The AF includes AF Traffic Steering Policy ID(s) in the request. The NEF stores the information in the UDR, as described in clause 4.3.6.2 of TS 23.502 [3].

3. PCF used the AF TSP ID(s) requested by the AF and creates PCC rule(s) with TSP ID(s).

4. PCF sends PCC rule(s) to the SMF.

5. SMF sends PDRs information to identify the traffic and forwards it accordingly with the TSPs.

6. UPF applies the PDRs with specific forwarding policies based on TSP ID.

### 6.2.3 Impacts on existing nodes and functionality

AF: Support of providing new information in the Nnef\_TrafficInfluence API, to provide explicitly traffic steering policy ID(s) (AF-TSPs) in its requests.

NEF: Support of new information in the Nnef\_TrafficInfluence API, and pass it to UDR and PCF.

UDR: Supports storage AT-TSP IDs in the AF influence in routing parameters.

PCF: Accepts new information and use it (or maps to local TSP defined) as traffic steering policies associated to the PCC rule(s) impacted.

No normative impacts to SMF and UPF. It is assumed that all UPFs in the operator network serving as PSA for the DNN/S-NSSAI/DNAI that is used for traffic that is potentially subject to SFC controls need to be configured with traffic steering information towards all SFPs supported for that DNN/S-NSSAI/DNAI.

## 6.3 Solution #3: AF influencing Service Function Chaining support by 5GC

### 6.3.1 Description

This solution addresses mostly Key Issue #2.

As already specified by IETF in RFC 7665 [10], Service Function Chain (SFC) is defined as a logical representation of an ordered set (sequence) of Service Functions that need to successively handle some traffic, e.g. traffic is first handled by SF1 (e.g. Deep Packet Inspection (DPI)), then SF 2 (e.g. TCP/IP optimization) and lastly by SF 3 (e.g. Firewall). Service Function Path (SFP) is an implementation/instance of an SFC. In other words, an SFC can be implemented as more than one different SFP instances (e.g. different instances/SFP corresponding to different N6 interfaces between 5GS and the DN). In an SFC the next hop SF (Service Function) may be determined based on the result of traffic processing by the previous SF.

The solution aims at improving how an AF can better control SFC related traffic classification in 5GC; it does not address SF control / deployment or SFF (Service Flow Forwarding) that are out of scope of the study.

Current traffic steering allows an AF to refer to abstract traffic steering policies that are predefined in 5GC: the AF cannot control the mapping from these abstract traffic steering policies to the actual user plane actions carried out by the PSA UPF (adding Vxlan/NSH/… headers to the traffic referred to as SFP Id and metadata information in this solution). This is suitable for SFC entirely controlled by the 5GC operators

The format of the SFP Id and of metadata (when provided) being referred to refers to existing IETF specifications such as the IETF specifications defining VxLAN and NSH.

Current Traffic steering control includes applying a specific N6 Traffic Steering Policy (TSP) to steer traffic to N6. TSP ID(s) are mapped within the 5GC based on local configuration: in PCF, in SMF or in UPF; this means that AF that can't influence the local configuration for TSP mapping lacks control on service flow classification in 5GC.

NOTE: Rel-17 specification (TS 23.501 [2]) e.g. tells "The PCF, based on information received from the AF, operator's policy, optionally service experience analytics per UP path received from NWDAF, etc. authorizes the request received from the AF and determines for each DNAI, a traffic steering policy ID (derived from the routing profile ID provided by the AF) and/or the N6 traffic routing information (as provided by the AF) to be sent to the SMF as part of the PCC rules. The traffic steering policy IDs are configured in the SMF or in the UPF. The traffic steering policy IDs are related to the mechanism enabling traffic steering to the DN".

For this scenario it is desirable for the AF to be able to discover the SFC(s) made available by the 5GC operator.

The SFC information, i.e. the available SFCs and their types, as well as the service path related classification tag (referred to as SFP Id and metadata information in this solution) and DNAI, is available to 5GC so that such information can be exposed to the AF via NEF API, and the AF can therefore associate some traffic with a certain SFC by indicating the SFC ID. This corresponds to Rel-17 specifications where the TSP ID takes the value of the SFC ID.

NOTE 3: When the 3RD party can use SFP and SF(s) deployed by the operator following issue can take place: if the operator changes the configuration of the SF(s) then it can change the data service provided to the (3rd party) users of the SFP/SF(s). When as in scenario 2, the 3rd party manages the SFC/SFP/SF(s) and uses just 5GC as traffic classifier (to identify and tag the traffic and send it to the SFP(s)) there is no such issue as the same entity (3rd party) manages the SFP(s) and uses it.

NEF APIs is used:

(new) NEF (optional) API allowing the AF to contact 5GC to discover available SFC/SFP. This allows the AF to discover SFC(s) that are deployed by the operator. This is intended for the first scenario.

NOTE 4: The NEF API allowing the AF to discover available SFC/SFP is just an optional capability to facilitate invocation of the NEF API allowing the AF to associate certain traffic and UE(s) with 5GC defined SFC/SFP(s) identified by traffic steering policies.

The AF provides a SFC ID to NEF in Nnef\_SFCInfluence.

NOTE: As soon as a 3RD party use SFP and SF(s) deployed by the operator, if the operator changes the configuration of the SF(s) then the operator may change the data service provided to the (3rd party) users of the SFP/SF(s).

### 6.3.2 Procedures

#### 6.3.2.0 Introduction

The SFC / SFP configuration (from the AF) aims at providing PCF with information on:

- Traffic classification (SFC classification role of the PSA UPF):

- Which PDU Session should a SFC apply to, for which UE(s), DNN(s) and or S-NSSAI(s));

- Which traffic of such PDU Session is to be handled by the SFC.

- (for the second scenario) the How should the UPF "tag" (e.g. NSH / VXLAN tag etc.) the classified traffic for each SFP associated with the SFC (SFP Id and metadata information to be used by the UPF).

The above information is used by PCF to create PCC rules for PDU Sessions. In order to support the second scenario PCC rules and N4 rules (FAR) need extension to carry the SFP Id and metadata information. For example, the FAR / Outer header creation information needs new values corresponding to NSH / VXLAN tag etc to be added after SFC classification done by the PSA UPF.

For the NEF, the following new northbound APIs are introduced:

- Nnef\_SFCInfluence: This API allows an AF to associate traffic that is identified by traffic filters and UE(s) (e.g. one UE, a group of UEs, a (set of) DNN/SNSSAI pair, etc.) with SFC and SFP(s).

 When the solution refers to "Nnef\_SFCInfluence", updates to Nnef\_TrafficInfluence may fulfill the requirements set by the solution.

 When SFCInfluence targets multiple UEs the NEF stores the AF policy in an UDR record.

 The PCF(s) that have subscribed to modifications of AF requests (Data Set = Application Data; Data Subset = SFC or traffic influence request information, Data Key = S-NSSAI and DNN and/or Internal Group Identifier or SUPI) receive(s) a Nudr\_DM\_Notify notification of data change from the UDR.

 The keys for these data in UDR are:

|  |  |
| --- | --- |
| AF Nnef\_SFCInfluence information | AF transaction internal ID |
|  | S-NSSAI and DNNand/orInternal Group Identifier or SUPI |

 This is further defined in clause 6.3.2.1.

- Nnef\_SFCDefinition: This API allows an AF to discover SFCs for the first scenario. The AF can also subscribe to be notified when new SFCs are deployed or existing SFCs are undeployed or modified. In case of SFC discovery, the NEF returns the Identifier of the available SFC(s) and an ordered list of service functions in each SFC to NEF which forwards the information to the AF.

NOTE: The name of each service function should be understandable to the AF, (allowing AF to understand that SFC 1 has Parental control first then NAT, then FW); such naming convention may be based on SLA with the AF.

NOTE: Nnef\_SFCDefinition assume that via SLA the operator and the third party agree on a common understanding on the name of each service function and let's the 5GC operator the possibility to create SFC(s) using these SF without needing to update the SLA.

 Usage of Nnef\_SFCDefinition is further defined in clause 6.3.2.3.

#### 6.3.2.1 Procedure to associate SFC with certain traffic and UE(s)



Figure 6.3.2.1-1: Associating an SFC with certain traffic and UE(s)

0. The PCF(s) subscribe to modifications of AF requests with Nudr\_DM\_Subscribe (Data Set = Application Data; Data Subset = AF SFC influence request information, Data Key = S-NSSAI and DNN and/or Internal Group Identifier or SUPI).

1. The AF is made aware of the available SFC(s). This may be via mechanisms of Figure 6.3.4-1 or via mechanism out of scope (e.g. SLA).

2. AF issues Nnef\_SFCInfluence\_Create request. The request may include

- traffic filters of the traffic to which the SFC applies;

- the identification of the target UE(s) (one UE a group of UE(s) or any UE), possibly the target DNN, S-NSSAI (if this is not provided by the AF, the NEF determines the target (DNN(s), S-NSSAI(s) based on the AF identifier);

- (for the second scenario) for each SFP associated with the SFC, the SFP Id and metadata information on how should the UPF "tag" (e.g. NSH / VXLAN tag etc.) the classified traffic;

- in scenario 1 the AF provides a SFC ID Nnef\_SFCInfluence;

- AF Transaction Id.

 To update or remove an existing request, the AF invokes a Nnef\_SFCInfluence\_Update or Nnef\_SFCInfluence\_Delete service operation providing the corresponding AF Transaction Id.

3. (in the case of Nnef\_ SFCInfluence\_Create or \_Update): The NEF stores the AF request information in the UDR (Data Set = Application Data; Data Subset = AF SFC influence request information, Data Key = AF Transaction Internal ID, S-NSSAI and DNN and/or Internal Group Identifier or SUPI).

NOTE: Both the AF Transaction Internal ID and, S-NSSAI and DNN and/or Internal Group Identifier or SUPI are regarded as Data Key when the AF request information are stored into the UDR.

 (In the case of Nnef\_SFCInfluence\_Delete): The NEF deletes the AF requirements in the UDR (Data Set = Application Data; Data Subset = AF SFC influence request information, Data Key = AF Transaction Internal ID).

3b. The NEF responds to the AF.

4. The PCF(s) that have subscribed to modifications of AF requests (Data Set = Application Data; Data Subset = AF SFC influence request information, Data Key = S-NSSAI and DNN and/or Internal Group Identifier or SUPI) receive(s) a Nudr\_DM\_Notify notification of data change from the UDR.

5. The PCF determines if existing PDU Sessions are potentially impacted by the AF request. For each of existing or new PDU Sessions, the PCF updates the SMF with corresponding policy information about the PDU Session by invoking Npcf\_SMPolicyControl\_UpdateNotify Npcf\_SMPolicyControl\_Create service operation as described in clause 4.16 of TS 23.502 [3].

 (For the second scenario) policy information indicates for each SFP, how the UPF should "tag" (e.g. NSH / VXLAN tag etc.) the classified traffic identified by the PCC rule traffic filters.

 (For the first scenario) The PCF maps the SFC ID to a TSP ID provided in the PCC rules: policy information indicates how the UPF should "tag" (e.g. via traffic steering identifiers etc.) the classified traffic identified by the corresponding SF filter(s).

6. When policy information about the PDU Session is received from the PCF, the SMF may take appropriate actions to configure the User Plane of the PDU Session (policy information received at PDU Session establishment) or reconfigure the User Plane of the PDU Session (policy information while a PDU Session establishment is already established).

NOTE: How the 5GC selects the PSA UPF that can support traffic classification and tagging for SFPs corresponding to AF request of the 3rd party is discussed in clause 6.3.2.4.

 (For the second scenario) N4 rules (FAR/ Outer Header creation) indicate how the UPF should "tag" (e.g. NSH / VXLAN tag etc.) the classified traffic identified by the corresponding PDR(s).

 (For the first scenario) N4 rules (FAR/ Outer Header creation) indicate how the UPF should "tag" (e.g. via traffic steering identifiers etc.) the classified traffic identified by the corresponding PDR(s).

#### 6.3.2.2 Procedure to associate SFC with an individual UE

If an SFC needs to be associated with an individual UE identified by its address, BSF is involved to select the corresponding PCF.



Figure 6.3.2.2-1: Associating an SFC with an individual UE

1. The AF sends the AF request via NEF, and the Nnef\_SFCInfluence\_Create/Update/Delete Request targets an individual UE address. This request corresponds to an AF request to influence the association of an SFC to an individual UE address.

2. NEF consumes Nbsf\_Management\_Discovery service operation (providing at least the UE address) to find out the address of the relevant PCF if the PCF address is not available on the NEF based on local configuration.

NOTE: The NEF finds the BSF based on local configuration or using the NRF.

3. BSF provides the PCF address in the Nbsf\_Management\_Discovery response to NEF.

4. NEF invokes the Npcf\_PolicyAuthorization service to the PCF to transfer the AF request.

5. As in steps 5 and 6 of Figure 6.3.2.1-1.

#### 6.3.2.3 Discovery of available SFCs

The AF may discover the available SFCs deployed over N6 via NEF with a new Nnef\_SFCDefinition service. This is further described in the rest of this clause.



Figure 6.3.2.3-1: Discovering available SFC(s)

1. The AF uses Nnef\_SFCDefinition\_GET to request a catalogue / list of existing SFC(s) matching some criteria (such as SFC involving NFx and NFy; the criteria could also list all existing SFC(s)). The NEF validates the request and forwards it to the O&M together with information on the AF Id and on the allowed (DNN, S-NSSAI) for the request.

2. The O&M entity responds with a list of SFC(s) that:

- match the criteria requested by the AF, or

- are allowed for the AF (for example that apply to the slices and AF Id indicated by the NEF).

 The O&M entity response contains a list of SFC(s) with at least their SFC ID, the ordered set of NFs of the SFC. This response is forwarded by the NEF using Nnef\_SFCDefinition\_GET result to the AF.

After the AF selects one SFC based on its own requirement, the AF can procedure to associate certain traffic and UE(s) to the selected SFC, as illustrated in Figure 6.3.2.2-1.

#### 6.3.2.4 Selection of an UPF that supports the proper SFC/SFP

At PDU Session establishment (and when it selects a new PSA UPF, e.g. when IPV6 Multi-Homing applies), the SMF needs to ensure that it selects PSA UPF(s) that can support traffic classification and tagging that may be required by PCC rules applying to the PDU Session where these PCC rules correspond to corresponding to SPF related AF requests.

The operator can have SLAs with multiple 3rd parties and the predefined SFPs for distinct 3rd parties can be deployed in distinct UPFs or in the same UPF(s).

When a UPF is registered / registers in NRF its capability to support a (DNN, S-NSSAI) this means that it supports the classification capability and traffic tagging capabilities (e.g. support NSH header insertion and/or support VxLAN addressing) required by SFP(s) applicable for this (DNN, S-NSSAI). Thus when the SMF selects a PSA UPF that supports the DNN and slice of the PDU Session this ensures that this PSA UPF can support traffic classification and traffic tagging capabilities that may be needed to support SFP(s) that may be required by an AF request that applies to this PDU Session. When PSA UPF(s) with very specific capabilities are required to handle some traffic the URSP sent to the UE guide the UE to use for this traffic a (DNN, S-NSSAI) leading the SMF to select these PSA UPF(s)

This does not mean that all traffic filters values and traffic tagging values are known in advance and defined as part of the SLA between the operator and the Third party. Nnef\_SFCInfluence allows the 3rd party to define new set of traffic filters and of traffic tagging values but within predefined capabilities negotiated in the SLA with the third party

### 6.3.3 Impacts on existing nodes and functionality

- A new NEF API(s) and possibly updates to Nnef\_TrafficInfluence.

- PCC rules and N4 rules (FAR) need extension to carry the SFP Id and metadata information (traffic tagging information) to support the second scenario.

- The format of the SFP Id and of metadata (when provided) being referred to refers to existing IETF specifications such as the IETF specifications defining VxLAN and NSH.

- It is assumed that all UPFs in the operator network serving as PSA for the DNN/S-NSSAI/DNAI that is used for traffic that is potentially subject to SFC controls need to be configured with traffic steering information towards all SFPs supported for that DNN/S-NSSAI/DNAI.

## 6.4 Solution #4: SFC support in 5GS

### 6.4.1 Description

This solution addresses Key Issue#1 (Traffic Steering Policy and SFC Enhancements) and Key Issue#2 (Exposure to enable AF to request predefined SFC for traffic flow(s) related with target UE(s)).

This solution proposal assumes that there is a service level agreement between the operator and a third party that includes a list of authorized predefined Service Function Paths (SFPs), each SFP being identified by a Service Function Chaining Identifier (SFP ID). Each SFP implements a set of pre-agreed policies (i.e. an ordered set of operations to be applied on the user plane packets) whose definition is outside of SA WG2 scope. By indicating an SFP ID, the third party can request that selected traffic flows be steered towards a specific SFP, either at PDU Session establishment or any time after PDU Session establishment.

The service level agreement can also contain a pre-agreed set of Metadata that the third party is allowed to insert into the SFP. Example use of Metadata is to allow the third party to include/exclude specific service operation in/from the SFP (e.g. age verification, denial of using specific application, etc.) for selected users.

The solution reuses the following definition from RFC 7665 [8].

*-* ***Metadata:*** *Provides the ability to exchange context information between classifiers and SFs, and among SFs.*

*-* ***Service Function Path (SFP):*** *The service function path is a constrained specification of where packets assigned to a certain service function path must go. While it may be so constrained as to identify the exact locations, it can also be less specific. The SFP provides a level of indirection between the fully abstract notion of service chain as a sequence of abstract service functions to be delivered, and the fully specified notion of exactly which SFF/SFs the packet will visit when it actually traverses the network. By allowing the control components to specify this level of indirection, the operator may control the degree of SFF/SF selection authority that is delegated to the network.*

*-* ***SFC Encapsulation:*** *The SFC encapsulation provides, at a minimum, SFP identification, and is used by the SFC-aware functions, such as the SFF and SFC-aware SFs. The SFC encapsulation is not used for network packet forwarding. In addition to SFP identification, the SFC encapsulation carries metadata including data-plane context information.*

#### 6.4.1.1 Architecture Assumption

This solution assumes that there is a user plane function with SFC capability (denoted as UPF-SFC), which interfaces with the PDU Session Anchor (UPF-PSA) over the N6 reference point. The UPF-SFC includes at least the Service Classification Function as defined in IETF RFC 7665 [8]. In addition, the UPF-SFC may include support for SFC Encapsulation, SFC Forwarding Function, etc. as described in IETF RFC 7665 [8]).

In the Control Plane the following network functions are impacted for handling of the SFP ID and/or Metadata: NEF, UDR, SMF and PCF.

Figure 6.4.1-1 shows the 5G system architecture for SFC support.



Figure 6.4.1-1: 5G system architecture for SFC support (uplink traffic)



Figure 6.4.1-2: 5G system architecture for SFC support (downlink traffic)

Uplink traffic: solid orange line for traffic that is steered to the UPF-SFC; dashed orange line for traffic that goes directly to the Data Network as illustrated in Figure 6.4.1-1.

Downlink traffic: solid green line for traffic that is steered to the UPF-SFC; dashed green line for traffic that goes directly to the UE as illustrated in Figure 6.4.1-2.

In Figure 6.4.1-2, it is assumed that each SFP for downlink traffic enforces the steering of processed traffic flows back into the same UPF-SFC.

In pre-Rel-18 3GPP specifications, the AF can provide traffic steering information (TSI) that can contain e.g. targeted traffic descriptor, a list of DNAI(s), a Routing Profile ID and/or N6 routing information. As an example, the traffic steering information can instruct the UPF to select a specific preconfigured tunnel on N6 for the traffic flows matching the traffic descriptor.

This solution proposes that the main SFC-specific impact (i.e. SFC service classification, SFP selection, SFC encapsulation etc.) is concentrated in the UPF-SFC. The other impacted functions (PCF, NEF, SMF, UDR) primarily participate in forwarding of the SFC-specific parameters (SFP ID and Metadata) between the AF and the UPF-SFC.

An example deployment option would be where the SFC is hosted in a trusted Edge Data Network environment and is operated by a trusted 3rd party. The AF in the trusted Edge Data Network environment can dynamically make decisions for steering of selected traffic flows onto a selected SFP and optionally convey Metadata to the Service Functions on that SFP. Such a deployment corresponds to RFC 8300 [11] Figure 10 (External Metadata and Policy), whereby an external network can provide Metadata containing classification information for policy enforcement and context information for forwarding packets within an SFC.

The following are the salient features of this solution:

- The UPF-PSA uses existing mechanisms for packet data detection (local F-TEID and SDF filters) and forwarding (remote F-TEID) to steer the targeted traffic flows towards the UPF-SFC. There is no specification impact on the UPF-PSA.

- In the presence of multiple UPF-PSAs and multiple UPF-SFCs, the traffic forwarding between a specific UPF-PSA and a specific UPF-SFC takes place over a pair of N6s tunnels associated with the UPF-PSA and UPF-SFC, one tunnel per traffic direction as illustrated in Figure 6.4.1-1 and Figure 6.4.1-2. This pair of N6s tunnels is set up dynamically by the SMF and is UE-specific. The same pair of tunnels can be used for all traffic flows between UPF-PSA and UPF-SFC for this UE, regardless of the SFP that is used at the UPF-SFC.

- Note that due to the "hairpin" forwarding of downlink traffic over N6s, the N6s tunnel for downlink traffic is used in both directions. In contrast, the N6s tunnel for uplink traffic is used in one direction only.

- The UPF-PSA is the IP anchor point for the PDU sessions. When downlink traffic arrives at the UPF-PSA from the Data Network (see Figure 6.4.1-2), the UPF-PSA detects the traffic that is subject to SFC and steers it towards the UPF-SFC based on the FAR configured in the UPF-PSA. Once the service function processing is applied in UPF-SFC, the DL traffic is sent from the UPF-SFC to the UPF-PSA based on the FAR configuration in the UPF-SFC which is then further forwarded towards the UE by the UPF-PSA.

NOTE 1: When the SFP for uplink traffic contains a Network Address Translation (NAT) device, the corresponding downlink traffic will arrive directly at the NAT device. In that case, after performing the network address translation, the NAT device needs to steer the downlink packet towards the N6 interface of the UPF-PSA. The steering is performed via standard IP routing because the new IP address will automatically steer the downlink packet towards the N6 interface of the UPF-PSA.

- Uplink traffic that is not subject to SFC can break out directly to the DN via N6 (see Figure 6.4.1-1). Downlink traffic always enters the 5GS at the UPF-PSA and only selected traffic is steered towards SFC (via "hairpin" forwarding), while the rest of the traffic is forwarded to N3/N9.

- The UPF with SFC capability (UPF-SFC) deploys an SFC functionality with several SFPs corresponding to pre-defined SFC polices as indicated in Figure 6.4.1-1 and Figure 6.4.1-2.

- The AF indicates the SFP ID and optionally Metadata for a selected target (e.g. a traffic flow, a UE, a group of UEs, etc.) per traffic direction.

- The PCF authorizes the requested SFP ID(s) and Metadata strings (if provided by the AF) e.g. by checking whether it is part of a pre-agreed SFP ID list in the service level agreement. The 5GC may need to parse or interpret the Metadata strings e.g. to check whether the requested Metadata strings is on the agreed SLA list, but it does not make any other use of the Metadata strings apart from forwarding it to the UPF-SFC.

- The SMF indicates the SFP ID(s) and optionally Metadata to the UPF-SFC via N4 interface in a FAR. The targeted traffic flows description is provided in a PDR.

- The UPF-SFC steers the targeted traffic flows towards the SFP indicated by the received SFP ID. Additionally it may perform SFC encapsulation as defined in RFC 8300 [11] and include the received Metadata in the SFC encapsulation header.

NOTE 2: It is also possible to rely on the existing traffic steering information to identify a specific SFP, rather than introducing the new SFP ID parameter. For instance, there can be several pre-defined N6 tunnels between the UPF-PSA and the UPF-SFC, each N6 tunnels corresponding to a distinct SFC path. However, this would create an undesired dependency between the configuration of N6 tunnels and the configuration of SFPs. For instance, every time an SFP is added or removed, this would imply reconfiguration of the N6 tunnels. Moreover, the use of preconfigured N6 tunnels may have scalability issues because the SMF would need to select a specially configured UPF-PSA upon PDU Session establishment, even if there is no SFC-related request from a 3rd party during the lifetime of the PDU Session. In contrast, keeping SFP ID as a distinct parameter allows for changes in the SFP configuration without any impact on the 5GC user plane configuration. It also allows for selecting a generic UPF-PSA during PDU Session establishment with no SFC-related pre-configuration. Note also that N4 is needed to convey the Metadata information to the UPF-SFC.

- The UPF-SFC can support data usage reporting on per SFP basis to the SMF. The SMF can provision the URR in UPF-SFC and the UPF-SFC can send the report back to SMF when the threshold or trigger condition is met as described in clause 5.2.2 of TS 29.244 [9].

### 6.4.2 Procedures

Figure 6.4.2-1 illustrates the enhancements to the procedure for processing AF requests to influence traffic routing for PDU Sessions not identified by a UE address, as described in clause 4.3.6.2 of TS 23.502 [3]. This procedure is used when targeting a group of UE(s), or any UE accessing a combination of DNN and S-NSSAI, or targeting individual UE by a GPSI. The SFP ID and Metadata provided as part of this procedure are applied upon PDU Session establishment, but can also result in modification of already established PDU Sessions that are impacted by the AF request.



Figure 6.4.2-1: Procedure for AF influenced traffic routing for SFC in 5GC for PDU Sessions not identified by a UE address

1. The AF creates AF request that includes an SFP ID and, optionally, Metadata corresponding to that SFP ID, in addition to existing parameters (e.g. Traffic descriptor, Application Identifier, to the NEF for requesting traffic routing to a SFP identified by the SFC ID. The Metadata is optional and available only when needed for configuring required application related information at UPF-SFC.

2. The AF sends the AF request via Nnef\_TrafficInfluence\_Create/Update/Delete message to NEF.

3a. The NEF requests to store/update/remove information of PFD(s), SFP ID and Metadata based on Application ID/Traffic descriptor.

3b. The NEF returns Nnef\_TrafficInfluence\_Create/Update/Delete response message to AF.

4. The PCF(s) that have subscribed to modifications of AF requests (Data Set = Application Data; Data Subset = AF traffic influence request information, Data Key = S-NSSAI and DNN and/or Internal Group Identifier or SUPI) receive(s) a Nudr\_DM\_Notify notification of data change from the UDR including the SFP ID and the Metadata.

5. The PCF checks if the indicated SFP ID corresponds to an authorized SFC policy for the AF. If the check is successful, the PCF notifies SMF via Npcf\_SMPolicyControl\_UpdateNotify message including PCC rules. The PCC rules contain SFP ID and Metadata (if available), in addition to existing parameters, such as PFD(s)

6a. The SMF selects UPF-SFC taking into account specific optional UPF capabilities as described in clause 6.3.3 of TS 23.501 [2] and the SFP ID. In this case the specific capabilities refer to the SFC-related capability and configuration in the UPF.

6b. In case there is no established tunnel between UPF-PSA and UPF-SFC for this UE, the SMF requests allocation of two tunnel endpoints at the UPF-PSA (one tunnel per traffic direction).

6c. In case there is no established tunnel between UPF-PSA and UPF-SFC for this UE, the SMF requests allocation of two tunnel endpoints at the UPF-SFC (one tunnel per traffic direction).

6d. Based on the PCC rules received from the PCF, the SMF configures the UPF-PSA via N4 message including PDR and FAR as described in Table 6.4.2-1.

Table 6.4.2-1: PDR and FAR configuration in UPF-PSA

|  |
| --- |
| **UPLINK traffic** |
| IN interface | OUT interface | PDR | FAR |
| N3/N9 | N6s | Local F-TEID (N3/N9), UL SDF | Remote F-TEID (N6s) for UL traffic |
| **DOWNLINK traffic** |
| IN interface | OUT interface | PDR | FAR |
| N6 | N6s | DL SDF | Remote F-TEID (N6s) for DL traffic |
| N6s | N3/N9 | Local F-TEID (N6s) for DL traffic, DL SDF | Remote F-TEID (N3/N9) |
| NOTE: In this table "downlink" refers to the global traffic direction. In reference to N6s, it is noted that the "downlink" traffic is carried in both directions. |

6e. Based on the PCC rules received from the PCF, the SMF configures the UPF-SFC with uplink and downlink PDR and FAR via N4message as described in Table 6.4.2-2.

Table 6.4.2-2: PDR and FAR configuration in UPF-SFC

|  |
| --- |
| **UPLINK traffic** |
| IN interface | OUT interface | PDR | FAR |
| N6s | SFC | Local F-TEID (N6s) for UL traffic, UL SDF | SFP ID (uplink), Metadata (uplink) |
| **DOWNLINK traffic** |
| IN interface | OUT interface | PDR | FAR |
| N6s | SFC | Local F-TEID (N6s) for DL traffic, DL SDF | SFP ID (downlink), Metadata (uplink) |
| SFC | N6s | SFP ID (downlink), DL SDF | Remote F-TEID (N6s) for DL traffic |
| NOTE: In reference to N6s, it is noted that the DOWNLINK traffic is carried in both directions. |

Figure 6.4.2-2 illustrates the enhancements to the procedure for processing AF requests to influence traffic routing when targeting a specific UE address, as described in clause 4.3.6.4 of TS 23.502 [3]. The SFP ID and Metadata provided as part of this procedure are applied any time after PDU Session establishment.



Figure 6.4.2-2: Procedure for AF influenced traffic routing for SFC in 5GC when targeting an individual UE address

Depending on the AF deployment (see clause 6.2.10 of TS 23.501 [2]), the AF may send the AF request to PCF directly, in which case step 1 is skipped, or via the NEF.

4. If step 1 was performed, NEF invokes the Npcf\_PolicyAuthorization service to the PCF to transfer the AF request. If an AF sends the AF request directly to the PCF, AF invokes Npcf\_PolicyAuthorization service and the PCF responds to the AF. The Npcf\_PolicyAuthorization service request includes the SFP ID and (optionally) the Metadata, in addition to existing parameters e.g. UE address and targeted traffic flows description.

5. The PCF authorizes the AF request and performs the steps 5, 6a and 6b described in Figure 6.4.1-1.

### 6.4.3 Impacts on existing nodes and functionality

NEF:

- NEF forwards the SFC-specific parameters from the AF to the PCF.

PCF:

- PCF checks if the indicated SFP ID and Metadata corresponds to an authorized SFC policy for the AF.

- Includes SFP ID and Metadata (if available).

UDR:

- The UDR stores the SFP ID and Metadata based on Application ID/Traffic descriptor.

SMF:

- The SMF configures the UPF-SFC with PDR and FAR via N4 message. The FAR includes the SFP ID and the Metadata (if available).

UPF-SFC:

- The UPF with SFC capability deploys an SFC functionality (i.e. SFC service classification, SFP selection, SFC encapsulation etc.) with several SFPs corresponding to pre-defined SFC polices.

## 6.5 Solution #5: UPF enhancement with SFC capability

### 6.5.1 Description

In this study, the UPF with SFC capabilities need to be enabled to offer flexible SFC configuration for a PDU session that requires different SFC processing for applications. This solution will resolve key issue 1 in order to provide UPF support with SFC capabilities.

5GS performs classification and SFC encapsulation used by the SFC-aware functions as a traffic classifier (Figure 6.5.1-1). The SFC encapsulation offers, at a minimum, Service Function Path (SFP) identification as defined in IETF RFC 7665 [8], such that SFC-aware functions can use it. The AF supplies predefined SFC ID and optional metadata allowing the 5GS to transport the classified packets along the service path via SFC encapsulation. If the AF does not provide SFC ID, predefined SFC ID referenced by TSP ID is used for SFC encapsulation. This solution explains how SFC capabilities in the 5GS may be made available, identified, and controlled.



Figure 6.5.1-1: 5GS as a traffic classifier

When the AF provides predefined SFC ID, 5GS can employ AF influenced traffic routing to detect application traffic for classification. The information requested by the AF is shown in Table 6.5.1-1. The data can also be used to detect traffic flows in order to perform SFC processing. The SFC encapsulation, however, requires SFC ID and optional metadata. As a result, in the AF influenced traffic routing, SFC ID and optional metadata are newly defined in AF requests. Metadata includes data plane context information which is carried in the SFC encapsulation. In this solution, metadata is an optional addition to the SFC ID, as indicated in Table 6.5.1-1.

Table 6.5.1-1: AF request in AF influenced traffic routing

|  |  |  |  |
| --- | --- | --- | --- |
| Information Name | Applicable for PCF or NEF  | Applicable for NEF only | Category |
| Traffic Description | Defines the target traffic to be influenced, represented by the combination of DNN and optionally S-NSSAI, and application identifier or traffic filtering information. | The target traffic can be represented by AF-Service-Identifier, instead of combination of DNN and optionally S-NSSAI. | Mandatory |
| Target UE Identifier(s) | Indicates the UE(s) that the request is targeting, i.e. an individual UE, a group of UE represented by Internal Group Identifier (NOTE 3), or any UE accessing the combination of DNN, S-NSSAI and DNAI(s). | GPSI can be applied to identify the individual UE, or External Group Identifier can be applied to identify a group of UE. | Mandatory |
| AF transaction identifier | The AF transaction identifier refers to the AF request. | N/A | Mandatory |
| N6 Traffic Routing requirements | Routing profile ID and/or N6 traffic routing information corresponding to each DNAI and an optional indication of traffic correlation. | N/A | Optional(NOTE 2) |
| SFC ID | Indicates SFC ID and optionally metadata for the SFC encapsulation. | N/A | Optional |

According to the PCC rule, traffic steering can be handled in one of the following ways in the solution:

- N6-LAN traffic steering (Figure 6.5.2-1).

- AF influenced traffic steering (Figure 6.5.2-2).

The PCF decides which traffic steering can be operated in the 5GS between N6-LAN traffic steering and AF influenced traffic steering. Therefore, SFC ID can be decided by the PCF when the AF requests them via the NEF, or they can be pre-configured statically in the PCF. According to the predefined SFC policy, which is agreed upon by PLMN and a third party and specified in a SLA, the 5GS may employ combined N6-LAN traffic steering for downlink traffic and AF influenced traffic steering for uplink traffic.

With the addition of SFC ID and optional metadata for the SFC encapsulation in the UPF, the PCC rule can be used to detect and steer traffic flows. SFC ID and metadata are now defined in the PCC rule and the Forwarding Action Rule (FAR), as shown in Tables 6.5.1-2 and 6.5.1-3. The traffic steering policies for all SFCs supported by the DNN/S-NSSAI/DNAI should be set in the UPF with SFC capability, which serves as the PSA for the DNN/S-NSSAI/DNAI. It is believed that the same set of traffic steering policies are configured on the 5GS within the same DNN/S-NSSAI/DNAI. As a result, the UPF can be chosen using DNN/S-NSSAI/DNAI. With the inclusion of SFC ID, the existing traffic steering mechanism is reused. Predefined SFC policy may indicate SFC header (e.g. network service header (NSH)) and transport protocol (e.g. VXLAN, GRE, MPLS, IP-in-IP) for the traffic flow. SFC ID may be used as SFP ID for the traffic flow to provide SFC encapsulation for the traffic flow. Alternatively, UPF may map SFC ID to one of the SFP ID(s) in the predefined SFC policy.

Table 6.5.1-2: The elements related to traffic steering in the PCC rule information in 5GC

|  |  |  |  |
| --- | --- | --- | --- |
| Information name | Description | Category | PCF permitted to modify for a dynamic PCC rule in the SMF |
| Rule identifier | Uniquely identifies the PCC rule, within a PDU Session.It is used between PCF and SMF for referencing PCC rules. | Mandatory | No |
| **N6-LAN Traffic Steering Enforcement Control**  | *This part describes information required for N6-LAN Traffic Steering.* |  |  |
| Traffic steering policy identifier(s) | Reference to a pre-configured traffic steering policy at the SMF. |  | Yes |
| SFC ID | Describes SFC Identification and optionally metadata for the SFC encapsulation. |  | Yes |
| **AF influenced Traffic Steering Enforcement Control** | *This part describes information required for AF influenced Traffic Steering.* |  |  |
| Data Network Access Identifier | Identifier(s) of the target Data Network Access (DNAI). It is defined in clause 5.6.7 of TS 23.501 [2]. |  | Yes |
| Per DNAI: Traffic steering policy identifier | Reference to a pre-configured traffic steering policy at the SMF. |  | Yes |
| Per DNAI: N6 traffic routing information | Describes the information necessary for traffic steering to the DNAI. It is described in clause 5.6.7 of TS 23.501 [2]. |  | Yes |
| Per DNAI: SFC ID  | Describes SFC Identification and optionally metadata for the SFC encapsulation. |  | Yes |

Table 6.5.1-3: Forwarding Action Rule related to traffic steering

|  |  |  |
| --- | --- | --- |
| Attribute | Description | Comment |
| N4 Session ID | Identifies the N4 session associated to this FAR. |  |
| Rule ID | Unique identifier to identify this information. |  |
| Forwarding policy | Reference to a preconfigured traffic steering policy or http redirection (NOTE 4). | Contains one of the following policies identified by a TSP ID:- an N6-LAN steering policy to steer the subscriber's traffic to the appropriate N6 service functions deployed by the operator, or- a local N6 steering policy to enable traffic steering in the local access to the DN according to the routing information provided by an AF as described in clause 5.6.7, or- a Redirect Destination and values for the forwarding behaviour (always, after measurement report (for termination action "redirect")). |
| SFC ID | Indicates SFC Identification and optionally metadata for the SFC encapsulation. |  |

### 6.5.2 Procedures

Traffic steering can be operated in either N6-LAN traffic steering or AF influenced traffic steering, according to the PCC rule.

#### 6.5.2.1 N6-LAN traffic steering with SFC capabilities

The traffic steering policy identifier(s) are used with N6-LAN traffic steering to direct traffic to the relevant N6 service functions deployed by the operator. Figure 6.5.2-1 depicts the procedure of N6-LAN traffic steering with SFC capabilities.



Figure 6.5.2-1: The procedure of N6-LAN traffic steering with SFC capabilities

1. The PCF provides N6-LAN traffic steering policy with additional SFC ID in the PCC rule to the SMF during SM Policy Association Establishment, SMF initiated SM Policy Association Modification, or PCF initiated SM Policy Association Modification procedure as defined in clauses 4.16.4 and 4.16.5 of TS 23.502 [3].

2. The SMF is triggered to either provision or remove the traffic steering policy when the PCC rule with SFC ID is provided from the PCF.

3. The SMF sends N4 Session Establishment/Modification/Release request to the UPF in order for the traffic steering policy with SFC capabilities to be provisioned or removed. Then, the UPF acknowledges with N4 Session Establishment/Modification/Release response message.

#### 6.5.2.2 AF influenced traffic steering with SFC capabilities

Figure 6.5.2-2 depicts AF influenced traffic steering with SFC capabilities. The procedure for SFC capabilities is summarized here.



Figure 6.5.2-2: The procedure of AF influenced traffic steering with SFC capabilities

The procedure of Processing AF requests to influence traffic routing for Sessions not identified by an UE address in clause 4.3.6.2-1 of TS 23.502 [3] is performed with the following modifications and clarifications:

1. To create a new request, the AF invokes a Nnef\_TrafficInfluence\_Create service operation. The content of this service operation (AF request) is defined in clause 5.2.6.7 of TS 23.502 [3] with additional SFC ID.

2. SFC ID is delivered in AF request from the AF to the NEF.

3. The NEF stores the AF request information in the UDR including SFC ID.

5. For PDU Sessions impacted by the AF request, the PCF updates the SMF with corresponding new policy information including SFC ID.

6. When the updated policy information about the PDU Session is received from the PCF, the SMF may take appropriate actions to reconfigure the User plane of the PDU Session includingSFC ID, as shown in Table 6.5.1-3.

### 6.5.3 Impacts on existing nodes and functionality

AF:

- Needs to support SFC ID for requesting AF influenced traffic routing.

NEF:

- Needs to support SFC ID in order to deliver them from the AF to the PCF.

- Needs to store SFC ID in the UDR.

PCF:

- Needs to support SFC ID in the PCC rule, either for N6-LAN traffic steering or for AF influenced traffic steering.

SMF:

- Needs to use the N4 interface to provision/remove SFC ID contained in FAR.

UPF:

- Needs to support SFC encapsulation with several SFPs corresponding to predefined SFC polices.

## 6.6 Solution #6: Service Function Chaining Configuration

### 6.6.1 Description

This solution aims to address KI#2 (i.e. "How to enable support for AF to request predefined SFC/SFP(s) for traffic flow(s) related with target UE (s)").

To address how to enable support for AF to request predefined SFC/SFP(s) for traffic flow(s) related with target UE (s) i.e. how to enable support for AF to configure pre-defined SFC policy for target UE(s) to 5GS, this solution follows the principles below:

- From the SLA, AF already knows the granularities of SFC classification rules and predefined SFC information (SFC IDs)

- AF interacts with NEF to request to apply predefined SFCs for target UE(s) by using new service operations (i.e., Nnef\_SFC\_ConfigCreate service operation with SFC Configuration Parameter) or extended AF traffic influence service operations (i.e., Nnef\_TrafficInfluence\_Create service operation with SFC Configuration Parameter).

- The service operations' request message may contain at least the SFC Configuration Parameter. The following table shows the SFC Configuration Parameter:

Table 6.6.1-1: SFC Configuration Parameter

|  |  |
| --- | --- |
| SFC Configuration Parameter | Description |
| UE identities | Target UE(s) identifier(es) (e.g. IP addresses) |
| SFC ID | Indicates the target SFC ID that will be applied for the target UE(s)  |
| Classification rule | Indicates classification rule for detecting the flows that will be treated by target SFC ID. This parameter is optional parameter and it is used when the AF wants to use the certain classification rules that are not included in the SLA results. |

- The granularity classification rule in Table 6.6.1-1 should be followed by "Traffic Description" that represents the target traffic by the combination of DNN and optionally S-NSSAI, and application identifier or traffic filtering information.

### 6.6.2 Procedures

Figure 6.6.2-1 outlines the procedure for configuring SFC policy for target UE(s).



Figure 6.6.2-2: Procedure for configuring SFC policy for target UE(s)

1. AF requests a SFC policy for the target UE(s) to NEF by invoking Nnef\_SFC\_ConfigCreate service operation or enhanced Nnef\_TrafficInfluence\_Create service operation with SFC Configuration Parameter.

 For instance, if AF wants to use the predefined SFC 1 (e.g., Firewall  DPI) for the traffic from UE1 (IP address: y.y.y.z) to the application server (IP address: X.X.X.2, port number: 80), AF sends the request message with below SFC Configuration Parameter.

 [UE identities: "y.y.y.z", [SFC ID: "SFC 1", [Classification rules: [Classification rule type: "IP Packet Filter Set", [Source IP address: "y.y.y.z", Destination IP address: "x.x.x.2", Source Port: "any", Destination Port: "80"]]]].

2. NEF interacts with PCF to configure SFC policy for target UE(s).

3. NEF responds with the Nnef\_SFC\_ConfigCreate or Nnef\_TrafficInfluence\_Create response.

### 6.6.3 Impacts on existing nodes and functionality

AF:

- Needs to support SFC Configuration Parameter for requesting SFC policy.

NEF:

- Needs to support SFC Configuration Parameter in order to configure SFC policy in the PCF.

## 6.7 Solution #7: Enhancing Application Function influence on traffic routing to an N6-LAN based on pre-defined SFC policies

### 6.7.1 Description

Editor's note: This clause will describe the solution principles and architecture assumptions for corresponding key issue(s) which should be explicitly stated. (Sub) clause(s) may be added to capture details.

The present solution addresses the following:

- How an AF is aware of the available pre-defined SFC policies in a 3GPP network.

- How an AF influences traffic steering for application traffic to an N6-LAN.

The solution supports both scenarios where network operator owns/deploys SFCs that are hosted in the 5GC network (Scenario 1) and SFCs hosted by 3rd party network.

Two options are proposed:

**Option 1: AF is aware via SLA agreements the SFC policy identifier(s) that corresponds to a specific Service Function Chaining.**

This option assumes that AF is aware of the SFC Policy identifier(s) corresponding to a service function chain based on SLA agreements.

**Option 2: AF requesting an SFC policy based on the available /pre-configured Service Function Chain policies supported by the 5GS network.**

The AF then requests from the 3GPP network if there are available/pre-configured an SFC policies based on the Service Functions required, via a new SBI interface. The AF request to the 3GPP network (via NEF) can include the following information:

- An ASP identifier.

- Optionally a UE identifier (or Group identifier).

- A list of one or more SF service identifier. The SF identifier is a scalar value that identifies a particular service of the Service Function, for example, Firewall, Video Transcoding etc. The SF Service Identifiers are negotiated between the 3rd party AF and network operator based on SLA agreements.

The 3GPP network authorises the AF request and provides the SFC policies to the AF where each SFC policy is identified by a specific SFC policy identifier.

When the AF requires to enable SFC policies the AF can re-use the Nnef\_TrafficInfluence SBI including in the request the target UEs, service data flow information of the traffic to be routed an SFC policy identifier. To address scenario 2 the AF additionally includes:

- DNAI information allowing the SMF to select a UPF capable to interface with a 3rd party SFC.

- Metadata information allowing a UPF to identify how to tag user plane traffic sent to an external 3rd party SFC.

### 6.7.2 Procedures

Editor's note: This clause describes high-level procedures and information flows for the solution.

#### 6.7.2.1 AF requesting SFC policies in a 3GPP network

The procedure for requesting N6-LAN services is as follows:



Figure 6.7.2.1-2: AF requesting pre-defined SFC policies

The procedure is as follows:

0. OPTION 1: The AF is aware of the available SFCs and corresponding SFC policy identifier(s) in a network. This can be based on SLA agreements.

 OPTION 2: AF requesting SFC policies based on pre-defined SF services available either in the 5GC or hosted by a 3rd party.

1. The AF is triggered to discover an SFC policy. For example, enable voice transcoding.

2. The AF invokes an Nnef\_SFC\_Policy\_Get\_Request including an identifier of the ASP, optionally external identifiers (GPSI) and a list of SF service ID(s).

3. The NEF forwards the request to the PCF invoking an Npcf\_SFC\_Policy\_Create request.

4. The PCF may check in the UDR if there are available SFC policies for the ASP.

5. The PCF makes a policy decision and determines the SFC policies for the ASP.If there in no SFC policy available for the requested service the PCF rejects the request.

6. The PCF includes the SFC policy according to the AF request identified by an SFC policy identifier.

7. The NEF forwards the response to the AF.

Editor's note: Whether Option 1 or Option 2 will be used for configuration of SFC policies when the SFC is hosted by the 5GC operator is to be determined at conclusions phase.

#### 6.7.2.2 AF influence on traffic routing by including pre-defined SFC policies

When the AF is triggered to enable an N6-LAN service the AF invokes an Nnef\_TrafficInfluence\_Create that includes the UE ID or Group ID of the affected UEs and N6-LAN steering information.

The N6-LAN steering information includes:

- Application ID or Traffic Filters of the affected application.

- SFC policy identifier according to the N6-LAN service requested by the AF as described in Figure 6.7.2.1-1.

- Applicable S-NSSAI/DNN information.

If S-NSSAI/DNN is included the policy is applicable for all UEs that have established a PDU session at this DNN and/or S-NSSAI.

The NEF determines the internal identifier of the UE(s) (i.e. SUPI) and update the subscription in the UDR by invoking an Nnef\_DM\_Update request service operation. The NEF updates the subscription data in the UDR.

The UDR notifies the PCF of the updated subscription information. The PCF determines the affected UEs, PDU sessions and application traffic and determines new or updated PCC rules where the PCC rule includes traffic descriptors of the traffic that needs to be routed to the operator's N6-LAN network and corresponding traffic steering policy identifier of the associated SFC policy (identified by the SFC policy identifier). The PCF then provides updated PCC rules to the SMF. The SMF configures the UPF with the traffic steering policy identifier corresponding to the SFC policy identifier that allows the UPF to route application traffic to the N6-LAN network.

The detailed procedure is illustrated below:



Figure 6.7.2.2-1: AF requesting to enable an N6-LAN service for a UE

1. The AF is triggered to enable an SFC policy for a UE or group of UEs.

2. The AF invokes an Nnef\_TrafficInfluence Create including in the request the external identifier of the UE (or Group of UEs) and in a container SFC steering information that includes, an application id or traffic filters of the application and an SFC policy identifier. The AF may include a DNAI and metadata information for the case where SFC are owned by a 3rd party.

3. The NEF determines the SUPI of the UE by interfacing with the UDM. The NEF may also determine if the ASP is authorized to use the SFC policy by interfacing with the UDR.

4. The NEF updates the subscription data in the UDR by invoking an Nudr\_DM\_Update service operation including SFC steering information as a data subset under the Application Data Set and adding the SUPI of the affected UEs as a Data Key.

5. The UDR notifies the PCFs that have subscribed to be notified of the changes in the subscription profile

6. The UDR invokes an Nudr\_DM\_Notify service operation including the updated subscription information.

7. The PCF determines the affected UEs, traffic and PDU sessions where the SFC policy needs to be included/updated.

8. The PCF provides updated PCC rules including the corresponding pre-defined traffic steering policy identifier for N6-LAN to the SMF. If metadata information is provided in step 2 the PCF forwards the information to the SMF.

9. The SMF selects a UPF based on existing mechanisms and configures the UPF according to the PCC rules. The SMF sends over N4 a Forward Action Rule request including in the request traffic filters and the traffic steering policy identifier. The SMF includes the metadata if provided by the PCF in step 8.

NOTE: SMF selects a UPF based on DNAI if provided by the AF in step 2.

10. The UPF and routes traffic corresponding to the traffic filters to N6-LAN. If metadata information is provided by the SMF, the UPF classifies the packet, e.g. by adding VxLAN information according to the metadata information, before routing the packet to the SFC function.

### 6.7.3 Impacts on services, entities and interfaces

Editor's note: This clause captures impacts on existing 3GPP nodes and functional elements.

- New SBI supporting an AF to discover the available SFC policies.

- Enhancing Nnef\_TrafficInfluence SBI supporting steering of traffic to N6-LAN.

- If metadata is supported:

 AF including metadata information in traffic influence request,

- NEF, PCF, SMF forwarding metadata information to UPF,

- UPF tagging the packet according to metadata information before routing the packet to the N6-LAN network.

## 6.8 Solution #8: AF request predefined SFC for traffic flow(s) related with target UE(s)

### 6.8.1 Description

The AF-influenced traffic steering enforcement control information is used to influence SMF routeing decisions for an identified traffic of PDU Session. It steers the user traffic to a local access to a Data Network (identified by a DNAI) per AF request. The AF-influenced traffic steering enforcement control information can be derived by the PCF based on the N6 Traffic Routing requirements provided by the AF. Until Rel-17 this is supported in non-roaming scenarios and to LBO deployments only.

The N6-LAN traffic steering enforcement control steer the identified traffic to appropriate operator 3rd party service functions in the N6-LAN. When the PCF generate the PCC rule for the SMF, the N6-LAN traffic steering enforcement control information is generated based on the operator's policy. This is supported in non-roaming and home-routed scenarios only. However that information is not generated or derived based on AF request.

The AF-influenced traffic steering enforcement control is only applied to the uplink traffic in the existing specification. The N6-LAN traffic steering enforcement control can be applied to the downlink traffic, uplink traffic or both. The N6-LAN Traffic steering policy identifiers can be different for uplink and downlink direction.

Table 6.3.1 of TS 23.503 [4] indicates that either N6-LAN Traffic Steering Enforcement Control or AF influenced Traffic Steering Enforcement Control can be included within a PCC rule. It means that traffic steering and SFC can't be applied to the same application traffic simultaneously.

From above analysis, it can be concluded that the N6-LAN traffic steering control (i.e. SFC policy) is different from the AF-influenced traffic steering enforcement control (i.e. traffic steering policy).

It is proposed that SFC policy and traffic steering policy is separated. An Application Function may send a request to influence SFC enforcement for the application traffic. In the request, the AF shall include the N6-LAN traffic steering control information, which includes target UE Identifier(s), DNN, S-NSSAI, SFC identifier (uplink and/or downlink), to the 5GC based on the SLA between the operator and the 3rd party. The PCF authorizes the N6-LAN traffic steering control information received from AF based on the SFC identifier (uplink and/or downlink) and operator's policy when generating the PCC rule. And then the N6-LAN traffic steering enforcement control information provisioning and enforcement defined in clauses 6.1.3.14 and 6.2.2.6 of TS 23.503 [4] can be applied, i.e. installing the related rule at UPF.



Figure 6.8.1-1: Architecture and traffic steering control flow

NOTE 1: based on the local configuration, the UPF can differentiate the packet coming from N6-LAN or from N6 interface as described in clause 5.4.8 of TS 29.244 [9]

It is possible that N6-LAN traffic steering control and AF-influenced traffic steering control are both applied to the same application traffic simultaneously.

- If the N6-LAN traffic steering enforcement control in downlink is applied when the AF-influenced traffic steering enforcement control is applied, the PCF include N6-LAN traffic steering policy identifier in downlink, and AF-influenced traffic steering policy identifier or N6 traffic routing information per DNAI within a PCC rule.

- If the N6-LAN traffic steering enforcement control in uplink is applied simultaneous as the AF-influenced traffic steering enforcement control is applied, the PCF shall include N6-LAN traffic steering policy identifier in uplink and AF-influenced traffic steering policy identifier or N6 traffic routing information per DNAI within a PCC rule.

Similar with the AF influenced traffic steering control defined in clause 4.3.6.1 of TS 23.503 [4], the following cases can be distinguished:

- AF requests targeting an individual UE by a UE address; these requests are routed (by the AF or by the NEF) to an individual PCF using the BSF. This is described in clause 6.8.2.1.

- AF requests targeting a group of UE(s), or any UE accessing a combination of DNN and S-NSSAI, or targeting individual UE by a GPSI. This is defined in clause 6.8.2.2.

Same general handing as described in clause 4.3.6.1 of TS 23.502 [3] are executed, e.g. how the NEF map the AF request to the DNN, S-NSSAI.

NOTE 2: The solution assumes that the 5GC and the AF have agreed via SLA on the mapping between a SFC identifier and for each DNAI/ N6 interface: the corresponding SFP, the metadata that the UPF should send to the SFP once it has done its SFC related classification.

### 6.8.2 Procedures

#### 6.8.2.1 Handling an AF request targeting an individual UE address



Figure 6.8.2.1-1: Handling an AF request targeting an individual UE address

1. Step 1 to step 5 of figure 4.3.6.4 of TS 23.502 [3] are performed with following modifications and exceptions:

- In step 1, the AF provides the N6-LAN traffic steering control information in the request. If the AF-influenced traffic steering control for the same application traffic is required simultaneously, the AF-influenced traffic steering control are provided additionally in the request.

- In step 4, the AF or the NEF provides the N6-LAN traffic steering control information in the request. If the AF-influenced traffic steering control for the same application traffic is required simultaneously, the AF-influenced traffic steering control are provided additionally in the request.

 In both cases the N6-LAN traffic steering control information includes SFC identifier (uplink and/or downlink).

- In step 5, the PCF authorizes the N6-LAN traffic steering enforcement control information based on the received the N6-LAN traffic steering control information and the operator's policy. The N6-LAN traffic steering enforcement control information includes the appropriate N6-LAN Traffic steering policy identifier(s) (uplink and/or downlink), which is derived from the AF provided SFC identifier (uplink and/or downlink). If both the N6-LAN traffic steering control information and AF-influenced traffic steering control information are provided, the PCF authorizes the N6-LAN traffic steering enforcement control information and AF-influenced Traffic Steering Enforcement Control information separately.

2. Step 1 to Step 4 of Figure 6.8.2.3-1 is performed.

#### 6.8.2.2 Handling an AF request not identified by an UE address



Figure 6.8.2.2-1: Handling an AF request not identified by an UE address

1. Step 1 to step 5 of Figure 4.3.6.2 of TS 23.502 [3] are performed with following modifications and exceptions:

- In step 1, the AF provides the N6-LAN traffic steering control information in the request, which includes SFC identifier (uplink and/or downlink). If the AF-influenced traffic steering control for the same application traffic is required simultaneously, the AF-influenced traffic steering control information are provided additionally in the request.

NOTE: The AF that issues the AF-influenced traffic steering control information may be different from the AF that issues N6-LAN traffic steering control information. When the PCF receives the kind of information via N5 or via UDR notifications, it is up to the PCF to create PCC results that result from the aggregation of both information.

- In step 3, the NEF stores the AF request information in the UDR (Data Set = Application Data; Data Subset = N6-LAN traffic steering control information, Data Key = AF Transaction Internal ID, S-NSSAI and DNN and/or Internal Group Identifier or SUPI).

- In step 4, the PCF(s) that have subscribed to modifications of AF requests (Data Set = Application Data; Data Subset = N6-LAN traffic steering request information, Data Key = S-NSSAI and DNN and/or Internal Group Identifier or SUPI) receive(s) a Nudr\_DM\_Notify notification of data change from the UDR.

- In step 5, the PCF authorizes the N6-LAN traffic steering enforcement Control information based on the received N6-LAN traffic steering control information and the operator's policy. The N6-LAN traffic steering enforcement control information includes the appropriate N6-LAN Traffic steering policy identifier(s) (uplink and/or downlink), which is derived from the AF provided SFC identifier (uplink and/or downlink).

2. Step 1 to Step 4 of Figure 6.8.2.3-1 is performed.

#### 6.8.2.3 Traffic steering enforcement control



Figure 6.8.2.3-1: Traffic steering enforcement control

1. The PCC rule which include the N6-LAN traffic steering enforcement control information is installed at the SMF as described in clause 6.8.2.1 or clause 6.8.2.2.

2. If both the N6-LAN traffic steering enforcement control information and AF-influenced traffic steering enforcement control information are provided by the same AF, the SMF may inserts/reselect an I-UPF/L-PSA according to current procedure.

NOTE 1: It is assumed that 5GC configuration is homogeneous for providing the same set of traffic steering policies within same DNAI/ DNN/ S-NSSAI. SMF can select then, UPF based on DNA/DNN/ S-NSSAI.

3. The SMF generates the N4 rule based on the received PCC rule as follows:

- if only N6-LAN traffic steering enforcement control is enforced, besides the PDR SMF derives the forwarding policy identifier (uplink and/or downlink) within the FAR based on the authorized the N6-LAN traffic steering enforcement control information.

- if only AF-influenced traffic steering enforcement control is enforced, besides the PDR SMF derives the forwarding policy within the FAR based on the authorized the AF-influenced traffic steering enforcement control information.

- if both N6-LAN traffic steering enforcement control and AF-influenced traffic steering enforcement control are enforced:

- If the N6-LAN traffic steering enforcement control in downlink is applied when the AF-influenced traffic steering enforcement control is applied, the SMF generates two PDR and FAR pairs. The first PDR and FAR pair is associated the downlink N6-LAN traffic steering policy handing. The second PDR and FAR is associated with the uplink AF influenced traffic steering policy handling.

- If the N6-LAN traffic steering enforcement control in uplink is applied when the AF-influenced traffic steering enforcement control is applied, the SMF generates two PDR and FAR pairs. The first PDR and FAR pair is associated the N6-LAN traffic steering policy handing. The second PDR and FAR is associated with the AF influenced traffic steering policy handling for traffic after N6-LAN traffic steering handling.

NOTE 2: The UPF enforce the first PDR and FAR pair to steer the uplink traffic to the N6-LAN and then enforce the second PDR and FAR pair to steering the uplink traffic, which has been processed by the SF(s) and routed back to the UPF, to the local network.

 The SMF provisions the N4 rule to the UPF (PSA) by initiating the N4 session establishment or modification.

4. Per the received forwarding policy, when the UPF (PSA) detects the related traffic, the UPF steers the corresponding traffic to the service function(s) deployed in the N6-LAN if applicable, and further steer the traffic to the local data network if applicable. How to steering the traffic is out of 3GPP scope.

### 6.8.3 Impacts on existing nodes and functionality

The solution has impacts in the following entities:

 AF:

- Needs to support to include the N6-LAN traffic steering control request information in the request.

 NEF:

- Needs to support to transfer the N6-LAN traffic steering control request information.

 UDR:

- Needs to support to store the N6-LAN traffic steering control request information.

 PCF:

- Needs to support to authorize the N6-LAN traffic steering enforcement control information based on the received the N6-LAN traffic steering control information.

 SMF:

- Needs to support to derive two PDR and FAR pairs. The first PDR and FAR pair is associated the N6-LAN traffic steering policy handing. The second PDR and FAR is associated with the AF influenced traffic steering policy handling.

It is assumed that all UPFs in the operator network serving as PSA for the DNN/S-NSSAI/DNAI that is used for traffic that is potentially subject to SFC controls need to be configured with traffic steering information towards all SFPs supported for that DNN/S-NSSAI/DNAI.

# 7 Overall Evaluation

Editor's note: This clause will provide evaluation of different solutions.

Evaluation of solutions for KI1 and KI#2:

Solutions are so far split into the following categories:

- AF influencing steering of subscriber traffic to SFC deployed by the 3GPP operator or 3rd party service provider. Solutions propose to re-use the Nnef\_TrafficInfluence API where the AF includes an identifier that denotes steering the traffic to specific N6 service functions/Service Function Chain. The solutions can be further categorized into:

- Solutions where the AF includes a new SFC Policy Identifier corresponding to specific Service Function chain based on SLA agreements (Solutions 2, 3, 4, 5, 6, 7, 8). AF is aware of the SFC policy identifier based on SLA agreements between the AF and 3GPP operator.

- In solution 1 it is assumed that the same existing Traffic Steering Policy identifier can be used.

- Some solutions also propose the AF to include additionally metadata information denoting specific SFC classification. (Solutions 3, 4, 5, 7).

- Solutions where the AF discovers the available Service Function Chain policies (and corresponding SFC Policy Identifier(s) of a 3GPP operator (Solutions 3, 6, 7). A new API is proposed where the AF gets a list of available SFC matching some criteria (e.g. SFC involving specific Service Function) (Solutions 3,6) or the AF requesting configuration of an SFC policy.

- Procedure in the 3GPP network to steer traffic to corresponding Service Function Chain over N6-LAN:

- All solutions propose the PCF to construct PCC rules taking into account the information in the AF request. The PCC rule includes a SFC Policy Identifier (potentially different for UL and DL traffic). The SMF based on the PCC rule, provides appropriate N4 rules (e.g. FAR, PDR etc) for the application traffic including the SFC policy identifier. The UPF based on the N4 rules and SFC Policy Identifier routes traffic to appropriate SFC in N6-LAN.

- One solution proposes to re-use the existing Traffic Steering Policy Identifier to steering traffic to N6-LAN (Solution 1).

- There are different proposals on how to handle UPF selection for SFC. Some solutions propose the SMF to select a UPF based on existing mechanisms (e.g. based on DNN/S-NSSAI, DNN) (Solutions 1, 2, 3, 7, 8), or the SMF ensures that an SFC-capable UPF is selected (Solutions 4). An SFC-capable UPF meaning a UPF that is able to do service classification as defined in IETF specifications. An SFC-capable UPF is able to use metadata information (if provided by the AF) to carry out the service classification.

- Some proposals also denote that if the AF includes metadata information, then the PCC and SMF provide the metadata transparently to the UPF for service classification (Solutions 3, 4, 5, 7).

# 8 Conclusions

Conclusions for KI#1 are as follows:

It is recommended to use the following principles and procedures as the basis for the normative work.

- 5GC may receive from the AF policies associating for one UE, a group of UE(s) or all UE(s) some traffic (filter) with SFC policy IDs together with optional metadata.

- PCF checks whether the indicated SFC policy IDs and Metadata correspond to an authorized SFC policy.

- Based on AF request, the PCF determines a policy per SDF/application for the purpose of steering the subscriber's traffic to appropriated N6-LAN service functions deployed by the operator or a 3rd party service provider. The policy is expressed in a Traffic Steering Policy (TSP) IDs that may be different in UL and DL directions.

- The PCF maps the SFC ID(s) into a TSP ID(s) (possibly one per direction) that refers to a traffic steering behaviour that is configured in the SMF/UPF. The SMF/UPF do not need to be aware of SFC IDs.

- The PCF provides the TSP ID(s) and the metadata (if available) in the PCC rules to SMF. The TSP ID refers to a traffic steering behaviour that is configured in the SMF/UPF.

- The SMF provisions corresponding PDRs, FARs, QERs to support SFC.

- The SMF creates a FAR with the Forwarding Policy parameters set to the TSP ID, and the FAR includes the metadata (if available).

- The UPF serving as PSA uses TSP ID to steer traffic over N6-LAN. The UPF performs the necessary actions to enforce the Forwarding Policy, e.g., performing packet encapsulation, packet marking and routing the traffic towards the service functions in the N6-LAN. The UPF provides the metadata (if available) together with the traffic sent to the N6-LAN service functions.

NOTE 1: How the UPF transforms the metadata into actual information sent with the traffic (e.g., NSH header, etc.) is based on local policies related with the TSP ID and not specified.

NOTE 2: The NEF, PCF and SMF do not need to understand the metadata.

- It is assumed that all UPFs in the operator network serving as PSA for the DNN/S-NSSAI/DNAI subject to SFC control need to be configured with the same traffic steering information for SFC processing.

Conclusions for KI#2 are as follows:

To enable the AF to request pre-defined SFC for traffic flow(s) related with target UEs.

- The Nnef\_TrafficInluence API is enhanced to include additionally an SFC policy identifier corresponding to a pre-defined Service Function Chain policy. The request may include separate SFC policy identifiers for Uplink and Downlink traffic of the subscriber traffic.

- Only following information of Nnef\_TrafficInfluence API are reused with N6 Traffic Routing requirements containing the SFC related additions described in this clause.

Table 8-1

|  |
| --- |
| Information Name |
| Traffic Description |
| Target UE Identifier(s) |
| Spatial Validity Condition |
| AF transaction identifier |

- The AF is aware of SFC policy identifiers based on SLA agreements.

- The PCF maps the SFC policy identifier to a corresponding identifier within the PCC rule. This mapping is defined in the conclusions of KI1.

- Support the N6-LAN traffic steering control and AF-influenced traffic steering control to be applicable to the same traffic simultaneously.

- The procedure for the Nnef\_TrafficInluence service in TS 23.502, clause 4.3.6 is re-used, for example, in case the AF is not providing UE address the NEF stores the AF request information in UDR.

Annex A:
Pre-Rel-18 Traffic Steering Control

This Annex provides the excerpts referring to the existing traffic steering control as well as general PCC and edge computing related concepts in TS 23.501 [2], TS 23.502 [3] and TS 23.503 [4].

**1. TS 23.503 [4], clause 4.3.7: Traffic steering control.**

 Traffic Steering Control refers to the capability to activate/deactivate traffic steering policies from the PCF in the SMF for the purpose of:

- steering the subscriber's traffic to appropriate operator 3rd party service functions (e.g. NAT, antimalware, parental control, DDoS protection) in the N6-LAN. This is supported in non-roaming and home-routed scenarios only.

- AF influence on traffic routing which enables the routing of the user traffic matching the traffic filters provided in the PCC rule to a local Data Network identified by the DNAI per AF request. This is supported in non-roaming and LBO scenarios only, as described in clause 5.6.7 of TS 23.501 [2].

**2. TS 23.503 [4], clause 4.2.4 and 6.1.2.3: PFD management.**

 Management of Packet Flow Descriptions (PFDs) refers to the capability to create, update or remove PFDs in the NEF (PFDF) and the distribution from the NEF (PFDF) to the SMF and finally to the UPF. This feature may be used when the UPF is configured to detect a particular application provided by an ASP.

 The Management of Packet Flow Descriptions enables the UPF to perform accurate application detection when PFD(s) are provided by an ASP and then to apply enforcement actions as instructed in the PCC Rule.

**3. TS 23.503 [4], clause 6.1.3.14: Traffic steering control.**

 Traffic steering control is triggered by the PCF initiated request and consists of steering the detected service data flows matching application detection filters or service data flow filter(s) in PCC Rules. The traffic steering control consists in:

- diverting (at DNAI(s) provided in PCC rules) traffic matching traffic filters provided by the PCF, as described in clause 5.6.7 of TS 23.501 [2].

- applying a specific N6 traffic steering policy for the purpose of steering the subscriber's traffic to appropriated N6 service functions deployed by the operator, or a 3rd party service provider as described below.

 The PCF uses one or more pieces of information such as network operator's policies, user subscription, user's current RAT, network load status, application identifier, time of day, UE location, DNN, related to the subscriber session and the application traffic as input for selecting a traffic steering policy.

 The PCF controls traffic steering by provisioning and modifying traffic steering control information in PCC rules. Traffic steering control information consists of a traffic description and a reference to a traffic steering policy that is configured in the SMF.

 The SMF instructs the UPF to perform necessary actions to enforce the traffic steering policy referenced by the PCF. The actual traffic steering applies at the UPF. For enforcing the traffic steering policy, the UPF may support traffic steering related functions as defined by other standard organizations. The mechanism used for routing the traffic over N6 is out of 3GPP scope.

**4. TS 23.503 [4], clause 6.2.2.6: Traffic steering.**

 The SMF shall support traffic steering control as defined in clause 6.1.3.14 of TS 23.503 [4].

 The SMF may be configured with the traffic steering policy IDs related to the mechanism enabling traffic steering to the N6-LAN, DN and/or DNAIs associated with N6 traffic routing requirements.

 Upon receiving a PCC rule which contains the traffic steering control information, the SMF shall provide the information to the UPF for the enforcement. The traffic steering control information in the PCC rule may include a set of DNAI(s) and for each DNAI a traffic steering policy ID and/or N6 traffic routing information dynamically provided by the AF.

NOTE: The UPF can, for example, perform marking packets in order to indicate a certain type of traffic to the DN side of the N6 reference point which enables those packets to be steered in the DN. As another example the UPF can forward, i.e. offload, traffic identified by the traffic descriptor to a local tunnel.

**5. TS 23.501 [2], clause 5.8.2.8: for the PCC related functions.**

**- Clause 5.8.2.8.1: Activation/Deactivation of predefined PCC rules which is configured in the SMF.**

- The traffic detection filters, e.g. IP Packet Filter, required in the UP function can be configured either in the SMF and provided to the UPF, as service data flow filter(s), or be configured in the UPF, as the application detection filter identified by an application identifier. For the latter case, the application identifier has to be configured in the SMF and the UPF.

- The traffic steering policy information can be only configured in the UPF, together with traffic steering policy identifier(s), while the SMF has to be configured with the traffic steering policy identifier(s).

**- Clause 5.8.2.8.2: Enforcement of Dynamic PCC Rules in which the SMF shall maintain the mapping between a PCC rule received over Npcf and the flow level PDR(s) used on N4 interface.**

- The application detection filters required in the UPF can be configured either in the SMF and provided to the UPF as the service data flow filter, or be configured in the UP function identified by an application identifier.

- When receiving a dynamic PCC rule from the PCF which contains an application identifier and/or parameters for traffic handling in the UPF:

- if the application detection filter is configured in the SMF, the SMF shall provide it in the service data flow filter to the UPF, as well as parameters for traffic handling in the UPF received from the dynamic PCC rule;

- otherwise, the application detection filters is configured in UPF, the SMF shall provide to UPF with the application identifier and the parameters for traffic handling in the UPF as required based on the dynamic PCC rule.

**- Clause 5.8.2.8.4: for the Support of PFD Management.**

**6. TS 23.501 [2], clause 5.6.7.1 and clause 6.3.7.2: for AF influence on traffic routing.**

- For AF influence on traffic routing, the information can be either determined by the PCF when requested by AF via NEF or statically pre-configured in the PCF.

- The AF request sent by the AF can provide the following information to influence traffic routing towards N6-LAN:

- the information to identify the traffic.

- Potential Locations of Applications: Indicates potential locations of applications, represented by a list of DNAI(s) or AF-Service-Identifier.

- N6 Traffic Routing requirements: contains Routing profile ID and/or N6 traffic routing information corresponding to each DNAI and an optional indication of traffic correlation.

NOTE 1: The N6 traffic routing requirements are related to the mechanism enabling traffic steering in the local access to the DN. The routing profile ID refers to a pre-agreed policy between the AF and the 5GC. This policy may refer to different steering policy ID(s) sent to SMF and e.g. based on time of the day, etc.

NOTE 2: The mechanisms enabling traffic steering in the local access to the DN are not defined.

**7. TS 23.502 [3], clause 4.4 and 4.18: for SMF and UPF interactions including N4 session management procedures and N4 PFD management procedures.**

**8. TS 23.502 [3], clause 5.6.7: Packet Flow Descriptions (PFDs) for application detection and AF request information for multiple UEs.**

- When a PDR is provided for an application identifier corresponding to the PFD(s), the SMF shall provide either the PFDs retrieved from NEF (PFDF) as described in TS 23.503 [4], or the pre-configured PFDs for an application identifier to the UPF. If the PFDs are managed by local O&M procedures, PFD retrieval is not used; otherwise, the PFDs retrieved from NEF (PFDF) override any PFDs pre-configured in the SMF.

**9. TS 23.502 [3], clause 4.3.6: AF influence on traffic routing.**

 Clause 4.3.6 describes the procedures between an Application Function and the SMF to maintain an efficient user plane path for Application Functions that require it.

 As described in clause 5.6.7 of TS 23.501 [2], an Application Function may send requests to influence SMF routeing decisions for User Plane traffic of PDU Sessions. The AF requests may influence UPF (re)selection and allow routeing of user traffic to a local access (identified by a DNAI) to a Data Network. The AF may also provide in its request subscriptions to SMF events.

Annex B:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-02 | SA2#149E | [S2-2201079](https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_149E_Electronic_2022-02/Docs/S2-2201079.zip) | - | - | - | Proposed skeleton approved at S2#149E | 0.0.0 |
| 2022-02 | SA2#149E | [S2-2201086](https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_149E_Electronic_2022-02/Docs/S2-2201086.zip) |  |  |  | FS\_SFC TR Scope. | 0.1.0 |
| 2022-02 | SA2#149E | [S2-2201848](https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_149E_Electronic_2022-02/Docs/S2-2201848.zip) |  |  |  | FS\_SFC architectural assumptions and Principles | 0.1.0 |
| 2022-02 | SA2#149E | [S2-2201849](https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_149E_Electronic_2022-02/Docs/S2-2201849.zip) |  |  |  | KI related with WT2 | 0.1.0 |
| 2022-02 | SA2#149E | [S2-2201747](https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_149E_Electronic_2022-02/Docs/S2-2201747.zip) |  |  |  | KI related with WT3 | 0.1.0 |
| 2022-02 | SA2#149E | [S2-2201748](https://www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_149E_Electronic_2022-02/Docs/S2-2201748.zip) |  |  |  | Annex for Pre-Rel-18 Traffic Steering Control | 0.1.0 |
| 2022-04 | SA#150E | - |  |  |  | Inclusion of documents approved in SA2#150e meeting:S2-2203433,S2-2202651,S2-2203434,S2-2203435,S2-2203436,S2-2203437,S2-2203438,S2-2203439,S2-2203440,S2-2203441 | 0.2.0 |
| 2022-04 | SA#150E | - |  |  |  | Editorial corrections | 0.2.1 |
| 2022-05 | SA2#151E | - | - | - | - | Inclusion of documents approved in SA2#151e meeting:S2-2205121S2-2205122S2-2205123S2-2205124S2-2205125S2-2205126 | 0.3.0 |
| 2022-08 | SA2#152E | - | - | - | - | Inclusion of documents approved in SA2#152e meeting:S2-2207704S2-2206526S2-2206727S2-2206728S2-2206814S2-2207705 | 0.4.0 |
| 2022-09 | SA#97-e | SP-220837 | - | - | - | MCC editorial update for presentation to TSG SA for information | 1.0.0 |
| 2022-10 | SA2#153E | - | - | - | - | Inclusion of documents approved in SA2#153e meeting: S2-2209858 | 1.1.0 |