|  |  |
| --- | --- |
| 3GPP TR 23.700-49 V0.3.0 (2024-04) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Enhancement of support for Edge Computing in 5G Core network - Phase 3  (Release 19) | |
|  | |
|  |  |
|  | |
| 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 address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  https://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.  © 2024, 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 members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 6

1 Scope 8

2 References 8

3 Definitions of terms and abbreviations 9

3.1 Terms 9

3.2 Abbreviations 9

4 Architectural Assumptions and Principles 9

4.1 Architecture Assumptions 9

4.2 Architectural Requirements 9

5 Key Issues 9

5.1 Key Issue #1: Enhancements for EAS (re)discovery and UPF (re)selection with reducing impact on central 5GC NFs 9

5.1.1 Description 9

5.2 Key Issue #2: Enhancement of EAS and local UPF (re)selection 10

5.2.1 Description 10

5.3 Key Issue #3: EC Traffic Routing between local part of DN and central part of DN 10

5.3.1 Description 10

5.X Key Issue #X: <Key Issue Title> 11

5.X.1 Description 11

6 Solutions 12

6.0 Mapping of Solutions to Key Issues 12

6.1 Solution #1: Edge computing handling by I-SMF 12

6.1.1 Key Issue mapping 12

6.1.2 Functional Description 12

6.1.3 Procedures 13

6.1.4 Impacts on existing services, entities and interfaces 14

6.2 Solution #2: Edge computing handling by local SMF 14

6.2.1 Key Issue mapping 14

6.2.2 Functional Description 14

6.2.3 Procedures 16

6.2.4 Impacts on existing services, entities and interfaces 17

6.3 Solution #3: Reducing impact of DNS message handling on central SMF for EAS (re)discovery based on offload to L-SMF 17

6.3.1 Key Issue mapping 17

6.3.2 General Description 17

6.3.3 Procedures 18

6.3.3.1 EAS Deployment Information and BaselineDNSPattern Management in the EASDF by L-SMF 18

6.3.3.2 EAS discovery procedure with EASDF 20

6.3.3.3 EAS discovery procedure with Local DNS Server/Resolver 22

6.3.3.4 EAS rediscovery at Edge Relocation 22

6.3.3.4 Mobility Handling 23

6.3.4 Impacts on services, entities and interfaces 23

6.4 Solution #4: Enhanced EC Architecture with SMF selecting local SMF storing EC related information 24

6.4.1 Key Issue mapping 24

6.4.2 Description 24

6.4.3 Procedures 25

6.4.3.1 Local SMF and Local PSA insertion procedure (new) 25

6.4.3.2 Local SMF and Local PSA Removal procedure (new) 26

6.4.3.3 EAS Discovery with EASDF procedure 27

6.4.4 Impacts on services, entities and interfaces 28

6.5 Solution #5: Enhanced EC architecture with AMF selecting local SMF 28

6.5.1 Key Issue mapping 28

6.5.2 Description 28

6.5.3 Procedures 30

6.5.3.1 PDU Session Establishment/EAS discovery with local offloading control and local SMF 30

6.5.4 Impacts on services, entities and interfaces 31

6.6 Solution #X: Local management of EAS Deployment Information with local SMF 32

6.6.1 Key Issue mapping 32

6.6.2 Description 32

6.6.3 Procedures 32

6.6.3.1 Provisioning EAS Deployment Information to local SMF without involvement of SMF 32

6.6.3.2 Provisioning EAS Deployment Information to local SMF with involvement of SMF 33

6.6.4 Impacts on services, entities and interfaces 34

6.7 Solution #7: EAS deployment information report from L-UPF 34

6.7.1 Description 34

6.7.2 Procedures 35

6.7.3 Impacts on services, entities and interfaces 35

6.8 Solution #8: Selecting an EAS server leveraging analytics 35

6.8.1 Key Issue mapping 35

6.8.2 Description 36

6.8.3 Procedures 37

6.8.4 Impacts on services, entities and interfaces 39

6.9 Solution #9: local UPF and EAS (re)selection jointly considering N6 delay and EAS load 40

6.9.1 Description 40

6.9.3 Procedures 40

6.9.3.1 Enhancement on EAS Deployment Information Management 40

6.9.3.2 EAS/L-PSA discovery procedure with EASDF 40

6.9.3.3 EAS/L-PSA rediscovery at Edge Relocation 42

6.9.3 Impacts on services, entities and interfaces 43

6.10 Solution #10: L-PSA and EAS (re)selection based on N6 one-way and two-way delay measurement 44

6.10.1 Key Issue mapping 44

6.10.2 Functional Description 44

6.10.3 Procedures 45

6.10.4 Impacts on existing services, entities and interfaces 47

6.11 Solution #11: Provision weight factor of DNAIs from AF 47

6.11.1 Description 47

6.11.2 Procedures 48

6.11.3 Impacts on services, entities and interfaces 48

6.12 Solution #12: NWDAF and SMF-based EAS and local UPF (re)selection 48

6.12.1 Key Issue mapping 48

6.12.2 Description 49

6.12.3 Procedures 49

6.12.3.1 NWDAF and SMF-based EAS and local UPF (re)selection 49

6.12.3.2 N6 delay measurement and reporting 51

6.12.4 Impacts on services, entities and interfaces 51

6.13 Solution #13: EAS Discovery taking account of EAS load in EASDF 52

6.13.1 Key Issue mapping 52

6.13.2 Description 52

6.13.3 Procedures 53

6.13.3.1 EAS load subscription and notification procedure 53

6.13.4 Impacts on services, entities and interfaces 53

6.14 Solution #14: EAS selection considering DNS historical handling records 54

6.14.1 Key Issue mapping 54

6.14.2 Description. 54

6.14.3 Procedures 54

6.14.4 Impacts on services, entities and interfaces 55

6.15 Solution #15: The local EASDF assist for the EAS and local UPF (re)selection based on the AF provided N6 delay and EAS load information 55

6.15.1 Description 55

6.15.2 Procedures 56

6.15.3 Impacts on Existing Nodes and Functionality 57

6.16 Solution #16: Local UPF and EAS (re)selection considering access network delay and N6 delay information by 5GC or AF 57

6.16.1 Key Issue mapping 57

6.16.2 Description 58

6.16.3 Procedures 59

6.16.4 Impacts on services, entities and interfaces 62

6.17 Solution #17: EC Traffic Routing between local part of DN and central part of DN with IP replacement in EAS 63

6.17.1 Key Issue mapping 63

6.17.2 Description 63

6.17.3 Procedures 65

6.17.4 Impacts on services, entities and interfaces 66

6.18 Solution 18: Supporting traffic routing between local DN and central DN within a PDU Session 67

6.18.1 Description 67

6.18.2 Procedures 67

6.18.3 Impacts on services, entities and interfaces 69

6.19 Solution #19: Traffic Routing between local DN and central DN over session breakout model 69

6.19.1 Key Issue mapping 69

6.19.2 Description 69

6.19.3 Procedures 70

6.19.4 Impacts on services, entities and interfaces 71

6.20 Solution #20: EC Traffic Routing between local part of DN and central part of DN via PDU session 71

6.20.1 Key Issue mapping 71

6.20.2 Description 71

6.20.3 Procedures 73

6.20.3.1 EC traffic Routing for UL traffic 73

6.20.3.2 EC Traffic Routing for DL traffic 74

6.20.4 Impacts on services, entities and interfaces 75

6.21 Solution #21: Solution to traffic routing between local and central part of DN via tunnel(s) 75

6.21.1 Description 75

6.21.1.1 Overall architecture of the solution 75

6.21.1.2 AF control of the connectivity between different DN parts 76

6.21.2 Procedures 77

6.21.3 Impacts on existing nodes and functionality 79

6.22 Solution #22: Establishment of connectivity between the local DN and central part of DN based on OAM 80

6.22.1 Key Issue mapping 80

6.22.2 Description 80

6.22.3 Procedures 80

6.22.4 Impacts on services, entities and interfaces 81

6.23 Solution #23: Traffic steering between different parts of a DN 81

6.23.1 Key Issue mapping 81

6.23.2 Description. 81

6.23.3 Procedures 81

6.23.4 Impacts on services, entities and interfaces 82

6.X Solution #X: <Solution Title> 83

6.X.1 Key Issue mapping 83

6.X.2 Description 83

6.X.3 Procedures 83

6.X.4 Impacts on services, entities and interfaces 83

7 Overall Evaluation 83

8 Conclusions 83

Annex A: Change history 84

# 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 present document describes key issues and solutions for the phase 3 of the system enhancements for Edge Computing in 5GS.

This technical report will document the study of potential system enhancements for enhanced edge computing support, including:

- Whether and how to support more efficient Edge Hosting Environment information management and related EAS Discovery:

- Handle the edge network and EAS related information (e.g. UPF and EAS deployment information, DNAIs) locally with less impact to 5GC central NFs (e.g. central SMF) to address more flexible EAS (re)discovery/(re)selection, local UPF (re)selection.

- Whether and how to take into account N6 Delay between the local PSA and EAS for local UPF and EAS (re)selection.

- Whether and how to support traffic sent to/from PSA after being processed by Edge Hosting Environment, e.g. when there is no communication possibility between the local part of the DN and central part of the DN (e.g. due to usage of private IP address, lack of secure tunnel); whether and how to support traffic being routed between two EASs located in two different Edge Environments when there is no pre-established communication path between the two local part of the DNs.

# 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 (5GS)".

[3] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[4] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS)".

[5] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".

[6] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[7] IETF RFC 792: "Internet Control Message Protocol".

[8] IETF RFC 4443: "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification".

[9] 3GPP TS 28.538: "Management and orchestration; Edge Computing Management".

# 3 Definitions of terms and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] 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].

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] 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].

# 4 Architectural Assumptions and Principles

Editor’s Note: This clause will document any architectural assumptions and principles.

## 4.1 Architecture Assumptions

The architecture in this study should be based on the following assumptions:

- The existing architecture and procedures for Edge computing as specified in TS 23.501 [2], TS 23.502 [3], TS 23.503 [4] and TS 23.548 [5] are used as baseline for further potential enhancement;

- Roaming is not considered in this study;

- The Edge Hosting Environment (EHE) is under the control of the network of serving PLMN or a 3rd party.

## 4.2 Architectural Requirements

The solutions should minimize the impact on the application layer if possible.

# 5 Key Issues

## 5.1 Key Issue #1: Enhancements for EAS (re)discovery and UPF (re)selection with reducing impact on central 5GC NFs

### 5.1.1 Description

This key issue is to investigate whether and how to reduce impact on central NFs when supporting EAS (re)discovery and UPF (re)selection.

Current Edge Computing design has impact on central 5GC Control Plane NFs. For example, the EAS Deployment Information and local UPF information (deployment information, or load) may be changed dynamically, as a consequence, they should be updated at the central SMF. Furthermore, central SMF can also be a bottleneck point for the DNS message handling since all decision is made by the central SMF. This may also cause signalling overload across operator's data centres for a deployment scenario where Control Plane NF(s) such as SMF is deployed in the central data centre while other involving NFs (e.g. L-NEF, AF, etc.) are located in the local data centre.

In order to reduce the above mentioned impact on central SMF for the purpose of EAS (re)discovery and local UPF (re)selection, following aspects need to be studied:

- Whether and which edge computing related information (e.g. UPF and EAS deployment information, DNAIs) can be locally managed to support EAS (re)discovery and UPF (re)selection.

- How to manage the above identified edge computing related information, e.g. locally, centrally or in both places.

- Whether existing procedures (e.g. discovery, ULCL/BP, mobility and influence/exposure related procedures) suffice. If not, how to address the gap when the above identified edge computing related information is handled locally or both locally and centrally.

## 5.2 Key Issue #2: Enhancement of EAS and local UPF (re)selection

### 5.2.1 Description

Normally an edge application can be served by different EASs deployed in different sites. It is important to discover one suitable EAS to handle the edge application, especially considering that mostly the edge application have the stringent E2E delay and/or data rate requirement(s) which may depend not only on network metrics such as bandwidth and latency but also on compute metrics such as processing, storage capabilities, and capacity as indicators for EAS load. When multiple candidate paths to application service are available for selection of an optimal service instance, the topologically closest path may not always meet the service specific requirements and metrics. For instance, some of the available links may be congested. Moreover, once a discovered EAS becomes non-optimized (e.g. after the UE moves far away or excessive load on EAS), a new EAS and local PSA might need be reselected to replace the old ones to serve the UE.

In the existing design, 5GS provides support for means to determine, to report and to expose UE on-path congestions status, date rate information and round-trip delay between UE and PSA UPF. However, no means are defined to also consider above metrics on data network (e.g. N6 delay) when multiple EAS instance(s) are available for selection to provide best possible E2E user experience.

The purpose of this key issue is to investigate whether and how to enhance EAS and local UPF (re)selection considering dynamic information related to EAS (i.e. EAS load and N6 delay between the local PSA and EAS).

The following aspects shall be studied:

- How to enable 5GC and/or a third party trusted and/or non-trusted Application Function to select the most suitable local UPF and EAS considering end to end delay that includes delay between a candidate N6 interface of the 5GS and a candidate EAS, and/or potentially EAS load.

- Whether and how to define N6 delay information (e.g. RTT).

- Whether considering the EAS load is needed, and if it is needed how the information representing the EAS load would be defined.

- For local UPF and EAS (re)selection, whether and how to take into account potentially EAS load and N6 Delay between the local PSA and EAS, including how to obtain and update the above information.

## 5.3 Key Issue #3: EC Traffic Routing between local part of DN and central part of DN

### 5.3.1 Description

In some scenarios, the application traffic may need to be first steered to Edge and processed there. After initial processing, the application traffic may still need to be further forwarded to the Application Server in the central part of DN for further processing. The application traffic may not be able to be routed directly between the EAS in the local DN and the Server in the central DN in case there is no direct connectivity between the local DN and central DN.

In such cases:

- UL traffic related to an application first routed over EC to Application Server(s) for local-processing, and then further forwarded to a remote Application Server(s) in central part of DN.

- DL traffic related to an application first routed over central part of DN for processing, then forwarded to Application Server(s) in local EC for local-processing, and finally provided to the UE.

Following aspects need to be studied:

- How to determine and route the application traffic between the EAS in the local part of DN and the Application Server in the central part of DN for both UL and DL in case there is no direct connectivity between the local DN and central part of DN;

- How is the 5GC aware of the application traffic is required to be processed at different locations? and by what order? including how to distinguish the UL/DL traffic traversing through the PSA;

- How to guarantee the QoS when the traffic transmission between local and central parts of DN;

- Whether and what information is required to be provided to make the final destination (e.g. UE, server in central part of DN) be aware of the traffic being processed by Edge Hosting Environment.

## 5.X Key Issue #X: <Key Issue Title>

### 5.X.1 Description

Editor’s note: This clause provides a description of the key issue.

# 6 Solutions

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | Key Issues | | |
|  | 1 | 2 | 3 |
| #1: Edge computing handling by I-SMF | X |  |  |
| #2: Edge computing handling by local SMF | X |  |  |
| #3: Reducing impact of DNS message handling on central SMF for EAS (re)discovery based on offload to L-SMF | X |  |  |
| #4: Enhanced EC Architecture with SMF selecting local SMF storing EC related information | X |  |  |
| #5: Enhanced EC architecture with AMF selecting local SMF | X |  |  |
| #6: Local management of EAS Deployment Information with local SMF | X |  |  |
| #7: EAS deployment information report from L-UPF | X |  |  |
| #8: Selecting an EAS server leveraging analytics |  | X |  |
| #9: Solution of local UPF and EAS (re)selection jointly considering N6 delay and EAS load |  | X |  |
| #10: L-PSA and EAS (re)selection based on N6 one-way and two-way delay measurement |  | X |  |
| #11: Provision weight factor of DNAIs from AF |  | X |  |
| #12: NWDAF and SMF-based EAS and local UPF (re)selection |  | X |  |
| #13: EAS Discovery taking account of EAS load in EASDF |  | X |  |
| #14: EAS selection considering DNS historical handling records |  | X |  |
| #15: The local EASDF assist for the EAS and local UPF (re)selection based on the AF provided N6 delay and EAS load information |  | X |  |
| #16: Local UPF and EAS (re)selection considering access network delay and N6 delay information by 5GC or AF |  | X |  |
| #17: EC Traffic Routing between local part of DN and central part of DN with IP replacement in EAS |  |  | X |
| #18: Supporting traffic routing between local DN and central DN within a PDU Session |  |  | X |
| #19: Traffic Routing between local DN and central DN over session breakout model |  |  | X |
| #20: EC Traffic Routing between local part of DN and central part of DN via PDU session |  |  | X |
| #21: Solution to traffic routing between local and central part of DN via tunnel(s) |  |  | X |
| #22: Establishment of connectivity between the local DN and central part of DN based on OAM |  |  | X |
| #23: Traffic steering between different parts of a DN |  |  | X |
| #24: Support traffic routing between local-DN and central-DN via the existing UP path of the PDU session and IP replacement |  |  | X |
| #25: EC Traffic Routing between local part of DN and central part of DN with UE IP address within IP header |  |  | X |
| #26: Solution on Enhancements for EAS (re)discovery and UPF (re)selection with reducing impact on central 5GC NFs | X |  |  |

## 6.1 Solution #1: Edge computing handling by I-SMF

### 6.1.1 Key Issue mapping

This solution is related to the KI#1.

### 6.1.2 Functional Description

The architecture of this solution is described as Figure 6.1.2-1.



Figure 6.1.2-1: Architecture assumption

In this solution, I-SMF is used to handle the edge computing related traffic to be offloaded into local DN, EDI management, DNS message handling rules configuration or update, and UL CL/BP or L-PSA insertion. Therefore, the impact on central SMF is reduced.

In this solution, the I-SMF, ULCL/BP UPF and Local PSA UPF are introduced with reusing mechanism described in clause 5.34 of TS 23.501 [2]. The difference from the ETSUN mechanism is that, SMF also sends the address of I-SMF to PCF. When traffic offload policy or edge computing related policy is updated, the PCF sends the policy update to I-SMF, with SMF forwarding transparently, which also reduces the edge computing handling impact to central SMF.

### 6.1.3 Procedures

##### 6.1.3.a I-SMF Insertion Procedure

UL CL

UE

(R)AN

AMF

SMF

UPF

I-SMF

PCF

UDM

4. Npcf\_SMPolicyControl\_Update

5. Npcf\_PolicyAuthorization\_Update

6. Nsmf\_PDUSession\_Update

EASDF

NEF

1. Steps 1-10 of Addition of PDU Session Anchor and Branching Point or UL CL controlled by I-SMF procedure, clause 4.23.9.1 of TS 23.502

2. I-SMF obtains EDI for local network, clause 6.1.3.e

3. Neasdf\_DNSContext\_Update

Figure 6.1.3.a-1: Procedure of I-SMF Insertion

1. I-SMF invoke the SMF service to sends the I-SMF supported DNAI(s) to SMF in Node Level Alternatively, the I-SMF supported the DNAI(s) can be configured in the SMF.

1. Steps 1-10 of Addition of PDU Session Anchor and Branching Point or UL CL controlled by I-SMF procedure is performed as described in clause 4.23.9.1 of TS 23.502 [3], with the following changes:

- During the PDU Session Establishment, the SMF selects EASDF, and then SMF sends the EASDF IP address as DNS server address to the UE via PCO.

- As described in clause 6.2.3.2.2 of TS 23.548[5], based on EAS information received from the EASDF, SMF may determine the DNAI, and trigger the I-SMF insertion. In order to avoid the impact, the SMF may send the target DNAI information to AMF and trigger the AMF to select the I-SMF as described in clause 4.23.5.4 of TS 23.502[3].

- SMF sends the EASDF IP address to I-SMF, to help the direct interaction between I-SMF and EASDF.

2. I-SMF obtains EDI for local network, as described in clause 6.1.3.c.

3. I-SMF invokes Neasdf\_DNSContext\_Update with the updated DNS message handling rules based on the EDI for local network.

4. SMF sends the address of I-SMF to PCF via Npcf\_SMPolicyControl\_Update service, as well as the indication of supporting local handling of Edge Computing from SM subscription data.

The following steps 5-6 will be performed when traffic offload policy (e.g. forwarding local traffic to the L-PSA) is to be updated.

5. When PCF gets the I-SMF address and the indication of supporting local handling of Edge Computing, PCF based on the DNN/S-NSSAI, or local configuration, may send policy container to SMF by invoking Npcf\_PolicyAuthorization\_Update service. The traffic offload policy or edge computing related policy is encapsulated in the policy container, as described in clause 6.1.3.b.

6. The SMF forwards the policy container transparently to I-SMF via Nsmf\_PDUSession\_Update service. The I-SMF performs EAS (re)discovery and UPF (re)selection based on the traffic offload policy or edge computing.

##### 6.1.3.b Processing AF requests for offloading policy create/update for I-SMF

UDR

PCF

NEF

AF

2.Nnef\_TrafficInfluence\_Create/Update

1. Creation of the AF request

SMF

I-SMF

3a. Storing/Updating the information

3b.Nnef\_TrafficInfluence\_Create/Update Response

4.Nudr\_DM\_Notify

5.Npcf\_PolicyAuthorization\_Update

6.Nsmf\_PDUSession\_Update

Figure 6.1.3.b-1: Procedure of processing AF requests for offloading policy create/update for I-SMF

1-4. Steps 1-4 of the procedure is the same as steps 1-4 of clause 4.3.6.2 of TS 23.502 [3], with the following change:

- AF provides requested policy related parameters with the indication for Local DN (in step 1-2). And the requested policy related parameters and the indication for L-DN is stored in UDR(in step 3a) and sent to PCF(in step 4).

5. If received the indication for L-DN, the PCF puts the traffic offload policy into a container and send to SMF.

6. The SMF forwards the policy container transparently to I-SMF via Nsmf\_PDUSession\_Update service, in order to achieve that the L-DN related traffic offloading policy do not impact the SMF.

##### 6.1.3.c EDI for local network Management in the I-SMF

The EDI for local network provisioned from AF to 5GC, i.e. UDR, is same as the procedure defined in clause 6.2.3.4.2 of TS 23.548 [5].

The I-SMF subscribes to EDI for local network Change Notification from the NEF using the procedure same as one defined in clause 6.2.3.4.3 of TS 23.548 [5].

### 6.1.4 Impacts on existing services, entities and interfaces

**I-SMF:**

- Handling the edge computing related traffic to be offloaded into local DN, EDI management, DNS message handling rules configuration or update, and UL CL/BP or L-PSA insertion. and control the edge computing handling for ULCL/BP;

- Receiving the policy from PCF;- Receiving EDI for local network directly from NEF.

**SMF:**

- Determining the target DNAI and triggering AMF to do the I-SMF selection and insertion based on the EAS information received from the EASDF.

- Forwarding traffic offload policy or edge computing related policy transparently to I-SMF.

**PCF:**

- Providing traffic offload policy or edge computing related policy in policy container and sending to I-SMF.

**NEF:**

- Sending EDI for local network to I-SMF.

## 6.2 Solution #2: Edge computing handling by local SMF

### 6.2.1 Key Issue mapping

This solution is related to the KI#1.

### 6.2.2 Functional Description

The architecture of this solution is described as Figure 6.2.2-1.



Figure 6.2.2-1: Network Architecture for the L-SMF

In this solution, UL CL/BP controlled by local SMF (L-SMF) can offload edge computing related traffic to local DN. The L-SMF is responsible for EDI management, DNS message handling rules configuration or update, and UL CL/BP or L-PSA insertion, and central SMF is not involved for the above information.

During PDU Session Establishment procedure, SMF decides to trigger the local-SMF selection based on SM subscription data. The SMF sends the indication of L-SMF selection to AMF, as well as the selected PCF ID/address.

The tunnels between AN, ULCL/BP UPF, central PSA UPF are setup by the following: UL N3 tunnel is setup by AMF provides UL CL/BP UPF CN Tunnel Info received from L-SMF to (R)AN, DL N3 tunnel is set up by AMF provides AN Tunnel Info received from (R)AN to UL CL/BP, UL N9 tunnel between UL CL/BP UPF and central PSA UPF is setup by AMF provides PSA CN Tunnel Info received from SMF to L-SMF, DL N9 tunnel between UL CL/BP UPF and central PSA UPF is setup by AMF provides UL CL/BP UPF CN Tunnel Info received from L-SMF to SMF.

### 6.2.3 Procedures



Figure 6.2.3-1: Procedure of edge computing handling by local SMF

1. Steps 1-11 of the UE-requested PDU Session Establishment procedure is performed as described in clause 4.3.2.2.1 of TS 23.502 [3], with the following change:

- In step 4, the central SMF retrieves indication of L-SMF selection from the Session Management Subscription data.

- In step 11, the central SMF response with the indication of L-SMF selection, and selected PCF ID or PCF address, selected EASDF address to AMF.

2. AMF selects the L-SMF with considering the UE location.

3. AMF triggers another PDU session establishment and sends the PCF address or PCF ID, selected EASDF address to the L-SMF by invoking Nsmf\_PDUSession\_CreateSMContext Request service.

4. L-SMF obtains offloading policy from PCF via SM Policy Association Establish procedure as described in clause 4.16.4 of TS 23.502 [3].

5. L-SMF selects UL CL/BP and optionally L-PSA as described in clause 6.3.3 of TS 23.501 [2].

6. Steps 9-14 of the UE-requested PDU Session Establishment procedure is performed as described in clause 4.3.2.2.1 of TS 23.502 [3], with the following changes:

- SMF is replaced by L-SMF.

- CN Tunnel Info is UL CL/BP CN Tunnel Info.

- The L-SMF configures the selected EASDF with DNS message handling rules, as described in step 2 of clause 6.2.3.2.2 of TS 23.548 [5]. In this step, the (R)AN obtains the CN Tunnel Info of the UL CL/BP UPF.

7. Steps 15-17 of the UE-requested PDU Session Establishment procedure is performed as described in clause 4.3.2.2.1 of TS 23.502 [3], with the following change:

- AN Tunnel Info is replaced by UL CL/BP CN Tunnel Info.

- SMF is replaced by L-SMF.

- In step 15, AMF also sends PSA CN Tunnel Info to the L-SMF.

- In step 16a, L-SMF also provides PSA CN Tunnel Info to the UL CL/BP.

### 6.2.4 Impacts on existing services, entities and interfaces

**AMF:**

- L-SMF selection indicated by DNN of the PDU Session Establishment Request.

- Providing the PCF address and EASDF address from Central SMF to L-SMF.

- Providing the PSA CN Tunnel Info to L-SMF.

- Providing the UL CL/BP CN Tunnel Info to SMF.

**SMF:**

- Providing PCF address and EASDF address to AMF.

**PCF:**

- Providing Offloading policy to L-SMF.

- Support the communication with L-SMF.

**L-SMF:**

- Support the communication with PCF.

## 6.3 Solution #3: Reducing impact of DNS message handling on central SMF for EAS (re)discovery based on offload to L-SMF

### 6.3.1 Key Issue mapping

This solution is proposed to solve KI#1.

### 6.3.2 General Description

The existing EASDF based EAS (re-)discovery mechanism requires the SMF to select and determine the suitable EDNS Client Subnet option or Local DNS server, and DNAI information during the DNS message handling procedure. To support this work, the SMF need be aware several information, e.g. the EAS deployment information, L-UPF (i.e. UPF to access EAS) information and manage the DNS handling rule accordingly. For example, if a new EAS is first time deployed at network and applied to any UE, the SMF need add one related DNS handling rule for all related UE DNS context at the EASDF. This also applies to the case if this EAS is removed from the network.

To mitigate the burden of the central SMF, it is proposed that the existing architecture is enhanced to avoid the SMF always need be updated/synchronized with the latest DNS message handling related information. The enhanced architecture can be depicted as Figure 6.3.2-1.



Figure 6.3.2-1: Support EAS (re)discovery and UPF (re)selection locally

This principle of the EAS (re)discovery based on this architecture can be summarized as below:

1. A new NF, i.e. L-SMF, is introduced. The L-SMF, which are deployed in the local area, selects and determines the suitable EDNS Client Subnet option or Local DNS server, and target DNAI during the DNS message handling procedure. The L-SMF register its service area to the NRF. As usual the UE SM NAS message is terminated at the SMF.

2. The EAS Deployment Information/Local UPF information is managed by L-SMF. L-SMF interact with the EASDF to provision the BaselineDNSPatten information via existing N88a interface. The DNS message detection template within the BaselineDNSPattern includes the additional information on this DNS message detection template is applied to which target of UE.

3. The SMF installed the DNS context at the EASDF as usual. The DNS handling rule within the DNS context include an information on which type of DNS message detection template is applied. After the DNS message handling, SMF may update the DNS handling rule to include the concrete FQDN/IP address detection template and handling action information.

4. EASDF combine the information provisioned from SMF and L-SMF, it can generate the detail DNS message detection template in the DNS context of UE.

5. The EASDF notifies the matched DNS query/response to SMF. And SMF forwards the related information to the related L-SMF. The L-SMF selects the EAS and L-PSA per the managed EDI and L-UPF information.

6. Per the selected EAS information, the SMF insert ULCL/BP and configure traffic filter to route the traffic either to PSA or to L-PSA. Hence the L-SMF only need manage the traffic related to local DN.

### 6.3.3 Procedures

#### 6.3.3.1 EAS Deployment Information and BaselineDNSPattern Management in the EASDF by L-SMF

The EAS deployment information provisioned from AF to 5GC, i.e. UDR, is same as the procedure defined in clause 6.2.3.4.2 of TS 23.548 [5].

The L-SMF subscribes to EAS Deployment Information Change Notification from the NEF using the procedure same as one defined in clause 6.2.3.4.3 of TS 23.548 [5].

The L-SMF manages the BaselineDNSPattern at the EASDF as following.



Figure 6.3.3.1-1: BaselineDNSPattern Management in the EASDF procedure

The procedure defined in clause 6.2.3.4.4 of TS 23.548 [5] is reused with the following difference:

1. The BaselineDNSPattern is enhanced with two additional information, i.e. Associated L-SMF information and Target UE, as following,

**- DNS handling rule associated information:**

- Target UE Group, this DNS pattern is applied to which target UE group, e.g. "Any UE" or "Internal Group ID".

NOTE 1: The Target UE group information is used to associate the BaselineDNSPattern with the DNS handling rule.

*- Baseline DNS message detection template.*

*- Baseline DNS handling actions information.*

NOTE 2: For the Baseline DNS message detection template or Baseline DNS handling actions temple, the Baseline DNS message detection template ID and the Baseline DNS handling actions ID is used for BaselineDNSPattern update and deletion. The uniqueness of the ID is per L-SMF set when a L-SMF set controls an EASDF and per L-SMF otherwise.

- **Association between L-SMF/DNAI/IP address range information:** For each DNAI derived from the EAS deployment Information, one supported L-SMF is included. Then this DNAI/(EAS) IP address range is associated with one L-SMF NF ID.

2. The L-SMF discover the related EASDF(s) for the indicated DNN/S-NSSAI, which are to be selected by the central SMF for DNS message handling. When the EASDF receive the BaselineDNSPattern from L-SMF, EASDF categorize the DNS pattern per which target UE group it is applied.

#### 6.3.3.2 EAS discovery procedure with EASDF



Figure 6.3.3.2-1: EAS discovery procedure with EASDF

The EAS Discovery with EASDF, i.e. option A/B type discovery, is executed as following:

1. L-SMF has created BaselineDNSPattern at the EASDF using the procedure as defined in clause 6.3.3.1.

2. Except the enhancement of DNS context, DNS context creation Procedure is same as defined in step 1~4 in Figure 6.2.3.2.2-1 of TS 23.548 [5].

The SMF creates the DNS context at EASDF. The DNS detection template includes the DNS message detection associated information, e.g. the associated target UE group. Per the DNS message detection associated information, i.e. same target UE group information as indicated in the DNS handling rule associated information within the BaselineDNSPattern, the DNS detection template is linked to the DNS message detection template included in the DNS pattern. Hence the EASDF can combine two information to generate related dedicated DNS template information, e.g. FQDN or IP address range, to be detected. For the DNS handling action, it includes the action to report the DNS message content to SMF, no other action is configured. For these DNS handling rule, it can be called as default handling rule, e.g. default handling rule for Any UE, at the DNS context of UE.

3. If the existing DNS context configured at EASDF does not applied, e.g. due to the condition same as defined step 5 in clause 6.2.3.2.2 of TS 23.548 [5], the SMF may update the DNS context, e.g. removing one dedicated DNS handling rule which is configured at the EASDF in step 10 or 20.

4. Same as step 7 in clause 6.2.3.2.2 of TS 23.548 [5].

5/6, The EASDF notifies the matched DNS query message and include the candidate L-SMF NF ID(s) per the provisioned BaselineDNSPattern information. The SMF responds back to EASDF.

7. The SMF select a L-SMF per the UE location and the candidate L-SMF(s) information.

8/9. The SMF query the L-SMF by N16b interface to determine how to populate the EDNS Client Subnet option or get the local DNS server information. The Query parameter include the UE location information and FQDN information reported from EASDF. The L-SMF select a suitable EDNS Client Subnet option or Local DNS server and responds it to SMF.

10. Per the query result from L-SMF, the SMF update the DNS handling rule. The DNS handling rule update is same as the step 10/11 in clause 6.2.3.2.2 of TS 23.548 [5]. The SMF may determine the DNS handling rule for the FQDN received in the report need to be updated. If yes, the SMF configure the related dedicated handling rule with the EDNS Client Subnet option or local DNS server information.

11. Same as step 12/13 in clause 6.2.3.2.2 of TS 23.548 [5].

12/13. The EASDF notifies the matched DNS response message and include the additional L-SMF information for each candidate EAS addresses per the provisioned BaselineDNSPattern information. The SMF responds back to EASDF.

14. The SMF select a L-SMF per the UE location and the candidate L-SMF(s) information.

15. The SMF invokes a Nsmf\_PDUSession\_CreateSMContext Request (SUPI, DNN, S-NSSAI, SMF ID (SMF Instance ID), SM context ID in SMF, RAT Type, PDU Session Id, UE location information, DNS message) to establish the UE context at the selected L-SMF. The DNS message notified by EASDF are also included and sent to the L-SMF.

16. The L-SMF selects the L-UPF and EAS. For the detail L-UPF and EAS selection refer to solution in KI#2.

17. The L-SMF invokes a Nsmf\_PDUSession\_CreateSMContext Response (Result Indication, PDU Session ID, CN N9 tunnel info) to the SMF. The CN N9 Tunnel Info is the UL Tunnel Info of the new I-UPF.

18. The SMF perform UL CL/BP selection and configure traffic routing rule on the UL CL or the BP to forward UE packets destined to the L-DN to the Local PSA.

19. The SMF communicates with L-SMF to establish the tunnel between ULCL/BP and Local PSA for DL direction, i.e. the SMF send the DL N9 tunnel info of the UL-CL to L-SMF.

20. Same as the step 17/18 in clause 6.2.3.2.2 of TS 23.548 [5], the SMF may determine the DNS handling rule for the FQDN received in the report need to be updated. If yes, the SMF configure the related dedicated handling rule associated with the indicated DNS response message, e.g. not need send further DNS Response message(s) corresponding to FQDN ranges and/or EAS IP address ranges to SMF.

21. Same as step 21 in clause 6.2.3.2.2 of TS 23.548 [5].

Before the DNS query, i.e. step 4, SMF can also select the L-SMF as described in clause 6.4.3.1. When the SMF receives the PCC rule related to the AF traffic influence and/or allowed by the subscription data as described in clause 6.4, the SMF may select the L-SMF which serves that DNAI as indicated in the PCC rule even the DNS query has not been triggered. If the L-SMF has been selected, the selection of L-SMF in step 7 and 14 can be skipped.

#### 6.3.3.3 EAS discovery procedure with Local DNS Server/Resolver



Figure 6.3.3.3-1: EAS Discovery Procedure with Local DNS Server/Resolver

The EAS Discovery Procedure with Local DNS Server/Resolver, i.e. option C/D type discovery, is executed as following:

1. Same as step 1 in clause 6.2.3.2.3 of TS 23.548 [5].

2. The SMF selects L-SMF:

- The SMF may select the L-SMF before the UE sends out any DNS query, e.g. during the PDU session establishment procedure. In this case the SMF select L-SMF per UE location; or

- The SMF select the L-SMF after the DNS query. Then the SMF selects L-SMF as described in clause 6.3.3.2.

3. The SMF invokes a Nsmf\_PDUSession\_CreateSMContext Request () to establish the UE context at the selected L-SMF. It includes the address of UE location, e.g. TAI, and an indication to acquire the local EHE information.

4. The L-SMF selects a L-UPF per UE location information if it is selected before DNS query. Otherwise the L-SMF select the L-UPF as described in clause 6.3.3.2.

5. The L-SMF invokes a Nsmf\_PDUSession\_CreateSMContext Response (Local DNS server) to the SMF. Per the EHE acquirement indication from SMF, the IP address of Local DNS Server is also returned back to the SMF.

6. The SMF perform UL CL/BP insertion and configure traffic routing rule on the UL CL or the BP to forward UE packets destined to the L-DN to the Local PSA.

7. The SMF communicates with L-SMF to establish the tunnel between ULCL/BP and Local PSA for DL direction.

8. Same as step 2~6 in clause 6.2.3.2.3 of TS 23.548 [5].

#### 6.3.3.4 EAS rediscovery at Edge Relocation

This procedure is used by the SMF to trigger the EAS rediscovery procedure when a new connection to EAS need to be established. This rediscovery can be triggered in three cases:

- **SMF triggered:** SMF determines that L-PSA relocation/removal may be needed, e.g. UE moves out of the service area of one L-SMF. The SMF queries serving L-SMF to confirm whether the L-PSA relocation is needed or not.

- **L-SMF triggered:** Per the network condition change as described in KI#2, the L-SMF may determine that EAS rediscovery is required.

- **AF triggered:** Due to the serving EAS is not suitable, e.g. it is to be turned off due to maintenance, the AF notifies the SMF to reselect EAS.



Figure 6.3.3.4-1: EAS rediscovery procedure at Edge relocation

1a. The SMF determines that L-PSA relocation/removal may be needed, e.g. UE moves out of L-SMF service area. The SMF queries the serving L-SMF with the UE location information and FQDN information. The L-SMF per the EAS deployment information determines whether the L-PSA need be relocated/removed or not. If the L-PSA need be relocated/removed, the L-SMF confirms to the SMF.

1b. The L-SMF determines to EAS rediscovery is needed as discussed in KI#2. The L-SMF notifies this to the SMF.

1c. The AF triggers EAS relocation e.g. due to EAS load balance or maintenance. The AF notifies the SMF via the PCF.

2. Same as step 2 in clause 6.2.3.3.3 of TS 23.548 [5].

If the L-SMF is reallocated/removed due to EAS rediscovery, after some local configured time, the SMF may release the UE context at the old L-SMF. The old L-SMF in turn release the related L-PSA. After that the SMF update the ULCL/BP to remove the related filter. The detailed removal procedure can refer to clause 6.4.3.2.

#### 6.3.3.4 Mobility Handling

The L-SMF is located after the anchor SMF. Hence the mobility handling does not need the L-SMF reallocation. After UE mobility, SMF evaluation whether the L-SMF need reallocated or removed. If it is need, the EAS rediscovery can be triggered.

### 6.3.4 Impacts on services, entities and interfaces

**EASDF**

- Receive enhanced BaselineDNSPatterns information from the L-SMF.

- Associate the DNS handling rule with the enhanced BaselineDNSPattern information to generate the concrete DNS detection template.

- Notify the candidate L-SMF to SMF when it notifies the matched DNS message to SMF. This requires the EASDF to be aware of L-SMF deployment information.

**L-SMF:**

- Provision the enhanced BaselineDNSPatterns to the EASDF.

- Select the L-UPF and EAS.

**SMF**

- Selects a L-SMF per received DNS message notification from EASDF and UE location.

- Create UE context at L-SMF to manage the traffic to L-PSA.

## 6.4 Solution #4: Enhanced EC Architecture with SMF selecting local SMF storing EC related information

### 6.4.1 Key Issue mapping

This solution addresses following aspects of KI#1:

- Whether and which edge computing related information (e.g. UPF and EAS deployment information, DNAIs) can be locally managed to support EAS (re)discovery and UPF (re)selection.

- How to manage the above identified edge computing related information, e.g. locally, centrally or in both places.

- Whether existing procedures (e.g. discovery, ULCL/BP, mobility and influence/exposure related procedures) suffice. If not, how to address the gap when the above identified edge computing related information is handled locally or both locally and centrally.

### 6.4.2 Description



Figure 6.4.2-1: Enhanced architecture with Local SMF

A Local SMF is introduced to manage the Local PSA UPF locally, it stores following EAS discovery related information:

- ECS (EDNS Client Subset) option;

- Local configuration associated with the (DNN, S-NSSAI, Internal Group Identifier) of the PDU Session;

- EAS Deployment Information provided by the AF or preconfigured in the L-SMF;

- Information derived from the UE location such as candidate L-PSA(s);

- PDU Session information, like PDU Session L-PSA(s).

In this enhanced system architecture, the Local SMF is responsible for Local PSA management, the central SMF is responsible for UL CL UPF management. The central SMF is responsible for Local SMF discovery and selection.

The Baseline DNS pattern can be created/updated to EASDF by Local SMF.

The interface between SMF and L-SMF is as defined in clause 6.3.

### 6.4.3 Procedures

#### 6.4.3.1 Local SMF and Local PSA insertion procedure (new)



Figure 6.4.3.1-1: Local SMF and Local PSA insertion procedure

1. SMF determines to add Local SMF for a UE's PDU Session based on the UE Requested DNN/selected DNN and S-NSSAI, or based on the AF influence information, which can happen during Application Function influence procedure (clauses 4.3.6.2 and 4.3.6.4 of TS 23.502 [3]), PDU Session Establishment procedure (clause 4.3.2 of TS 23.502 [3]) or PDU Session Modification procedure (clause 4.3.3 of TS 23.502 [3]).

2-3. SMF checks whether a Local SMF is authorized in user subscription information by retrieving the subscription information from UDM. UE's SUPI, serving PLMN ID and PDU Session parameters such as DNN and S-NSSAI may be included in the Subscription Retrieval Request message. If authorized, the User subscription information includes a Local SMF authorized indication and the corresponding DNNs and S-NSSAIs.

4. SMF discovers proper Local SMFs by querying NRF and selects one most suitable Local SMF, a PDU Session Create or Update Request is sent to the Local SMF. The PDU Session Create Request/Response message may include the similar Information Elements (i.e. PDU Session parameters and User Plane tunnel information of UL CL UPF) as Nsmf\_PDUSession\_Create\_Request/Response as defined in clause 5.2.8.2.2 of TS 23.502 [3], the PDU Session Update Request/Response message may include the similar parameters as Nsmf\_PDUSession\_Update\_Request/Response as defined in clause 5.2.8.2.3 of TS 23.502 [3].

5-6. The Local SMF selects a suitable Local PSA UPF based on the received PDU Session parameters (e.g. DNN, S-NSSAI, SSC mode, Requested PDU Session type, etc.). The User Plane tunnel information of Local PSA UPF is included in the N4 Session Establishment Response message. The N4 Session Establishment Request/Response procedure is as defined in clause 4.4.1.2 of TS 23.502 [3].

7. A PDU Session Create/Update Response is sent from Local SMF to SMF. The User Plane tunnel information of Local PSA UPF is included in the Response message.

8-9. SMF sends the User Plane tunnel information of the local PSA UPF to the UL CL UPF.

#### 6.4.3.2 Local SMF and Local PSA Removal procedure (new)



Figure 6.4.3.2-1: Local SMF and Local PSA Removal procedure

1. The SMF determines to remove the Local SMF and Local PSA UPF, which can happen during Application Function influence procedure (clause 4.3.6.2 and 4.3.6.4 of TS 23.502 [3]), PDU Session Establishment procedure (clause 4.3.2 of TS 23.502 [3]) or PDU Session Modification procedure (clause 4.3.3 of TS 23.502 [3]).

2. PDU Session Modification Request is sent from SMF to Local SMF including an indication of removing Local SMF and Local PSA UPF.

3-4. The Local SMF releases the N4 Session towards Local PSA UPF.

5. A PDU Session Modification Response is sent from Local SMF to SMF including an indication of result of Local PSA UPF removal.

6-7. The SMF updates the UL CL UPF to remove the User Plane tunnel towards the Local PSA UPF.

#### 6.4.3.3 EAS Discovery with EASDF procedure



Figure 6.4.3.3-1: EAS Discovery with EASDF procedure (clause 6.3.2.2.2 of TS 23.548 [5])

In step 8, after receiving the Neasdf\_DNSContext\_Notify Request message, the SMF needs to forward the received DNS message report from EASDF to Local SMF to retrieve the EAS discovery related information from Local SMF:

- ECS (EDNS Client Subset) option;

- Local configuration associated with the (DNN, S-NSSAI, Internal Group Identifier) of the PDU Session;

- EAS Deployment Information provided by the AF or preconfigured in the L-SMF;

- Information derived from the UE location such as candidate L-PSA(s);

- PDU Session information, like PDU Session L-PSA(s).

#### 6.4.3.4 EAS Rediscovery procedure

The EAS rediscovery procedure depicted in clause 6.3.3.4 can be applied to this solution.

### 6.4.4 Impacts on services, entities and interfaces

**Local SMF (new entity):**

- Stores the EAS discovery related information and provides the EAS discovery related information to SMF when receives the request from SMF.

- Selects the Local PSA UPF for a PDU Session and sends the User Plane tunnel information to SMF.

- Trigger the EAS rediscovery procedure.

**Impact to SMF:**

- Retrieves Local SMF authorized information from UDM.

- Retrieves the EAS discovery related information from Local SMF.

- Discovers and selects the Local SMF.

- Adds/removes the Local SMF for the PDU Session.

- Forward the received DNS message report from EASDF to Local SMF.

**Impact to UDM:**

- Stores the Local SMF authorized information in the subscription information.

- Provides the Local SMF authorized information in the subscription information to SMF after receiving the subscription retrieval request.

## 6.5 Solution #5: Enhanced EC architecture with AMF selecting local SMF

### 6.5.1 Key Issue mapping

Key issue #1.

### 6.5.2 Description

This solution corresponds to Key Issue #1 and addresses the following aspects:

- How to establish PDU Session that supports local offloading control including (i) how to decide the need of the local offloading control (how to decide to insert local SMF), and (ii) how to authorize the PDU Session to support local offloading control via local SMF.

- How to support Rel-17/18 edge computing related procedure, i.e. EAS discovery.

It is assumed that the OAM configures within AMF or SMF information for local offloading control service area, which represents the area where the local offloading control or local session management is supported

This solution is proposed based on the assumed architecture shown as in Figure 6.5.2-1 that includes local SMF that performs local offloading control based on the instruction from the SMF.

The SM NAS message is delivered to SMF via local SMF in the proposed architecture, where a single EASDF is used.



Figure 6.5.2-1: Architecture for local offloading control with ULCL/BP

The SMF provides the local SMF with the local offloading management policy, which contains the following information: FQDN or IP range allowed for the local offloading control, and the information related to AF influence on traffic routing enforcement control (e.g., DNAI(s) as identifier(s) of the target data network access, Information on AF subscription to UP change events, NEF information as notification endpoint).

The local SMF manages the AF subscription to UP change events if it is provided via the local offloading management policy. If the Information on AF subscription to UP change events AF subscription to UP change events in the local offloading management policy contains Indication of “AF acknowledgment to be expected”, the runtime coordination between 5GC and AF is enabled and managed by the local SMF, and occasionally by interaction between the local SMF and SMF as follows:

a) Case 1: Due to UE mobility, the selected target DNAI is still under the local SMF’s management. The local SMF sends UP change event notification (e.g., via Nnef\_TrafficInfluence\_Notify) to the AF and manage the runtime coordination with the AF by deciding to wait for an Acknowledgement as a positive response from the AF before configuring and/or activating the new UP path toward the target DNAI.

b) Case 2: Due to UE mobility, when the SMF is notified that the UE moves outside of service area of the local SMF, the SMF selects the target DNAI and UPF which are NOT in the service area of the local SMF. However, because the local SMF has managed the AF subscription to UP path change, the local SMF needs to send UP change event notification (e.g., via Nnef\_TrafficInfluence\_Notify) to the AF. If the runtime coordination is also the part of the AF subscription to UP path change, then the runtime coordination is performed among L-SMF, SMF, and the AF to wait for an Acknowledgement as a positive response from the AF before configuring and/or activating the new UP path toward the target DNAI with the followings:   
(i) The SMF needs to provide the local SMF with the selected target DNAI, which may be contained in the UP path change related notification message from the local SMF to the AF.  
(ii) The local SMF informs that the SMF needs to wait before configuring and/or activating the new UP path toward the target DNAI if Indication of “AF acknowledgment to be expected” is given. Accordingly, the SMF wait for a positive response from local SMF.   
(iii) The SMF informs the local SMF that the UP path toward the target DNAI is configured/activated.   
(iv) The local SMF sends to the AF the late notification upon receiving the information for the UP path configured/activated form the SMF.

### 6.5.3 Procedures

#### 6.5.3.1 PDU Session Establishment/EAS discovery with local offloading control and local SMF



Figure 6.5.3.1-1: PDU Session Establishment with supporting local offloading control

1. During the Registration procedure, the AMF gets the Local Offloading Control allowed indication from the UDM

2-3. During the PDU Session Establishment procedure, if the AMF receives the Local Offloading Control allowed indication, the AMF decides to insert and select local SMF considering DNN/S-NSSAI, UE location, locality information of candidate local SMFs, and local offloading control service area information. Even if the service area of the selected SMF includes the current UE location, but the UE location is in the area of the local offloading control service area, the AMF may decide to insert and select local SMF. The SMF selection may be performed via the NRF. For this, local SMF needs to register to the NRF or local SMF information needs to be configured in the NRF.

4-5. The AMF sends the Local Offloading Control Indication and SMF information to the selected local SMF. The local SMF provides response to the AMF.

6. The local SMF selects and configures the UPF for local offloading control.

7. The local SMF sends the Local Offloading Control Request Indication to the SMF. Also, the local SMF provides a list of DNAIs that supports the local offloading control.

8. The SMF decides whether to support the local offloading control based on, for example, the SM subscription data, UE location, and local offloading control service area for a given PDU Session.

9-10. During the SM policy association between the SMF and PCF, the SMF requests local offloading management policy by sending Local Offloading Control Policy Request Indication. If authorized by PCF successfully, the PCF provides the local offloading management policy that may include FQDN or IP range allowed for the local offloading control, and additionally the information related to AF influence on traffic routing enforcement control (e.g., DNAI(s) as identifier(s) of the target data network access, Information on AF subscription to UP change events, NEF information as notification endpoint).

11. The SMF selects and configures the UPF.

12. The SMF sends the Local Offloading Control allowed information, local offloading management policy information, and EASDF information to the local SMF.

The SMF selects the EASDF for local offloading control as described in clause 6.3.23 of 3GPP TS 23.501[2].13. The local SMF performs N4 Session Modification to configure the UP path according the information received form the SMF. The local SMF may decide to insert ULCL/BP.

14-17. The rest of steps for PDU Session Establishment procedures are performed. The N1N2 message sent from the SMF to AMF via the L-SMF.

18. The local SMF configures the EASDF based on the local offloading management policy received from the SMF. When the DNS query occurs, the local SMF and EASDF handles the DNS message according to the local offloading management policy. When the local SMF receives the notification for the DNS response from the EASDF, the local SMF may decide to insert ULCL/BP.

#### 6.5.3.2 Handling local SMF notification service toward the AF



Figure 6.5.3.2-1: Notification of user plane management event when local SMF is used

The Figure 6.5.3.2-1 shows the procedure for a notification of UP management event for case 2 in clause 6.5.2 when runtime coordination is enabled.

1. A condition for a notification to the AF (e.g., DNAI change is needed) has been met.

2. The SMF request the SM context in the local SMF and provides the selected target DNAI information, which is not under the local SMF’s management.

3. The local SMF provides the information for the AF subscription to corresponding UP management event, which may include notification target address and information for the Indication of “AF acknowledgment to be expected”.

4-5. The local SMF sends the Early UP path management event notification, which may include the target DNAI received from the SMF and old DNAI.

6-7. The AF provides Acknowledgement containing positive/negative response to the local SMF.

8. The local SMF informs the SMF that positive/negative response from the AF is received.

9. For the early notification, the SMF performs UP path configuration for the target DNAI.

10. The SMF informs the local SMF that UP path configuration for the target DNAI is completed.

11-12. The local SMF sends the Late UP path management event notification. The AF response with providing Acknowledgement.

13. The local SMF informs the SMF that the positive/negative response from the AF is received. If positive response received, the SMF activates the configured UP path, and the removal of the old UP path and local SMF are performed.

### 6.5.4 Impacts on services, entities and interfaces

AMF may be configured with the local offloading control service area

If the service area of the selected SMF includes the current UE location, but the UE location is in the area of the local offloading control service area,

**AMF**

- checks if the local offloading control is allowed, and if allowed, selects the local SMF.

- sends the Local Offloading Control Indication and SMF information to the selected local SMF.

**SMF**

- decides to support local offloading control and selects the local SMF.

- requests the local offloading management policy to the PCF, and if received from the PCF, provides the local offloading management policy to the local SMF.

- interacts with local SMF for the runtime coordination among local SMF, SMF, and AF for the UP path change.

- retrieves and considers EDI for the UP path change management.

**Local SMF**

- configures EASDF and UPF based on the information received form the SMF.

- receives the notification for the DNS response from the EASDF and decides to insert ULCL/BP.

- register to NRF with its locality information.

- manages notification event(s) subscribed by the AF and, if required, manage the runtime coordination among local SMF, SMF, and AF for the UP path change

**PCF**

- provides the local offloading management policy to the SMF/Local-SMF.

## 6.6 Solution #6: Local management of EAS Deployment Information with local SMF

### 6.6.1 Key Issue mapping

Key issue #1.

### 6.6.2 Description

This solution is for Key Issue #1, which addresses how to locally manage the edge computing related information.

This solution assumes the deployment scenario where SMF is deployed in a central data centre while NEF and a NF (in this solution, the NF refers to local SMF) locally manages edge computing related information is located in a local data centre nearby an edge hosting environment.

This solution proposes to handle EAS deployment information among NFs located in the above mentioned local data centre as much as possible.

### 6.6.3 Procedures

#### 6.6.3.1 Provisioning EAS Deployment Information to local SMF without involvement of SMF



Figure 6.6.3.1-1: Provisioning EAS Deployment Information to local SMF without involvement of SMF

Precondition: Local SMF and SMF are set up to decide to support local offloading control.

1-2. Local SMF subscribes EAS Deployment Information Change Notification from the NEF by providing information (e.g. DNN and/or S-NSSAI and/or application identifier) received from the SMF.

3. The AF invokes the Nnef\_EASDeployment\_Create/Update/Delete service operation.

4. The NEF checks whether the AF is authorized to perform the request, and authorised to provision the EAS Deployment Information based on the operator policies. If the NEF receives the subscription request for the EAS Deployment Information Change Notification, the NEF decides not to store the information in the UDR based on the locally configured operator policy.

NOTE: The NEF can be configured with the operator policy (e.g. per AF), which instructs the NEF to manage the EDI locally without storing the information to the UDR.

5. The NEF provides response to the AF.

6. The NEF sends the notification message including EAS Deployment Information to the local SMF.

7. The local SMF invokes Neasdf\_BaselineDNSPattern or Neasdf \_DNSContext based on the information received from the information obtained from the NEF and the SMF. The local SMF obtains EASDF information from the SMF in advance or use the locally configured EASDF information.

#### 6.6.3.2 Provisioning EAS Deployment Information to local SMF with involvement of SMF



Figure 6.6.3.2-1: Provisioning EAS Deployment Information to local SMF with involvement of SMF

Precondition: Local SMF and SMF are set up to decide to support local offloading control.

1-2. The SMF subscribes EAS Deployment Information Change Notification from the NEF by providing information (e.g. DNN and/or S-NSSAI and/or application identifier).

3. The AF invokes the Nnef\_EASDeployment\_Create/Update/Delete service operation.

4. The NEF checks whether the AF is authorized to perform the request, and authorised to provision the EAS Deployment Information based on the operator policies.

5. The NEF invokes the Nudr\_DM service operation to store/update/delete EAS Deployment Information.

6. The NEF provides response to the AF.

7. The NEF sends the notification message including EAS Deployment Information to the SMF.

8. The SMF provides the notified EAS Deployment Information to the local SMF if local offloading control is decided. The SMF may provide the local SMF with Indication to modify the subscription related to EAS Deployment Information Notification, and the information required to modify the existing subscription information for the notification of the EAS Deployment Information (e.g. subscription correlation ID, corresponding NEF information).

NOTE: The SMF does not need to perform additional local SMF discovery for this procedure. As described in the precondition, it is assumed that the SMF is already aware of the Local SMF information.

9. Option A: The SMF modifies the existing the existing subscription information for the notification of the EAS Deployment Information by replacing the notification target address with the local SMF address.

Option B: The local SMF modifies the existing the existing subscription information for the notification of the EAS Deployment Information by utilizing the information received from the SMF.

NOTE: If it is necessary to terminate the modified subscription between NEF and local SMF, either the SMF or the local SMF will terminate the subscription as follows: for Option A, the SMF will terminate the subscription, and for Option B, the local SMF terminate the subscription.

10. The local SMF invokes Neasdf\_BaselineDNSPattern or Neasdf \_DNSContext based on the information received from the information obtained from the NEF and the SMF. The local SMF obtains EASDF information from the SMF in advance or use the locally configured EASDF information.

NOTE: It will be evaluated whether the respective procedures in clauses 6.5.3.1 and 6.5.3.2 are applicable for which architecture having a local SMF (e.g. an architecture where SM NAS message go through local SMF and to SMF, or architecture where SM NAS message does not go through the local SMF)

### 6.6.4 Impacts on services, entities and interfaces

**SMF:**

- Delegates EASDF and local UPF configuration related to DNS handling to the local SMF.

- Modifies the existing subscription to EDI notification to delegate EDI management to the local SMF.

**Local SMF newly introduced:**

- Handles EDI locally, and configures EASDF and local UPF based on the locally managed EDI

**NEF:**

- Decides whether to store the EDI in the UDR or locally manage and directly provide the EDI to the local SMF.

The interface between the SMF and L-SMF will have a new reference point and be used for transmitting edge-related information such as EDI between them or for delivering SM NAS message for an architecture proposed in clause 6.5.2.

## 6.7 Solution #7: EAS deployment information report from L-SMF/L-UPF

### 6.7.1 Description

This solution is for key issue 1.

This solution is enhancement of Option D in TS 23.548 [5]. The current Option D is quoted below:

**- Option D:** If the SMF has been configured that DNS Queries for an FQDN (range) query can be locally routed on the UL CL, then the subsequent DNS Queries for the FQDN (range) will be locally routed to a Local DNS server.

In this option the SMF has been preconfigured with the FQDN (range) that can be locally routed on the ULCL. The AF can invoke AF influence procedure or provide the EAS Deployment Information to SMF, with FQDN(s) for applications deployed in the Local part of the DN. In order to reduce the impact on SMF, this solution proposes that these information can be provided from the Local part of the DN directly towards the SMF, e.g. the L-SMF/L-UPF in the Local part of the DN provides the FQDN (range) towards the SMF. After the detection of the FQDN in the DNS Query message the SMF can insert the I-UPF and L-PSA and route the DNS Query message towards the Local DNS server via L-PSA.

This solution is applicable for Session breakout connectivity model.

Editor note: It is FFS how this solution can be applicable for the Multiple PDU Sessions connectivity model and Distributed Anchor connectivity model.

### 6.7.2 Procedures

#### 6.7.2.1 No L-SMF insertion



Figure 6.7.2.1-1: No L-SMF insertion

0. The N4 Node level Association is established between the SMF and the L-PSA. During this procedure, the L-PSA provides the S-NSSAI, DNN, FQDN(range) that can be served by the L-PSA, Local DNS server address and associated DNAI.

1. The UE establishes a PDN session towards the SMF. In this procedure the SMF configures the EASDF to detect the FQDN range of the DNS Query request message.

2. The UE sends DNS Query Request message with the target FQDN over the user plane of the PDU session.

3. The EASDF detects that the DNS Query message with the target FQDN.

4. The EASDF forwards the DNS Query Request message with the target FQDN to the SMF and notifies that the FQDN is detected.

5-6. The SMF determines that the DNS query can be routed to an Local DN, it selects target DNAI. If the SMF determines that it can support the DNAI, the SMF selects the L-PSA based on the target DNAI. , The SMF inserts an ULCL/BP and L-PSA associated with that Local DNS server for the PDU Session.

7. The SMF forwards the DNS Query Request towards the ULCL/BP, and ULCL/BP forwards the DNS Query Request to Local DNS server via the L-PSA, similar as Option D in TS 23.548 [5].

#### 6.7.2.2 L-SMF insertion after the I-SMF



Figure 6.7.2.2-1 L-SMF insertion after the I-SMF

Step 1, The SMF subscribes the notification of new L-SMF serving the target S-NSSAI and DNN newly registered in the NRF, or L-SMF profile has been updated.

Step 2, The L-SMF is registered in the NRF. The NF profiles includes the S-NSSAI, DNN, FQDN(range) that can be served by the L-SMF, Local DNS server address and associated DNAIs. When new L-UPF is deployed the L-UPF establishes N4 Node Association and the L-UPF provides the FQDN(range), Local DNS server address and associated DNAI. The L-SMF then update the NF profile stored in the NRF.

Step 3, The NRF notify the SMF about the NF profiles of the newly registered L-SMF , or the updated NF profile of L-SMF.

Step 4, The SMF generates/updates the BaselineDNSPattern based on the NF profiles of the new registered L-SMF and invokes Neasdf\_BaselineDNSPattern\_Create/Update service operation of the EASDF to create/update the BaselineDNSPattern.

Step 5, the UE establishes a PDN session towards the SMF. In this procedure the SMF configures the EASDF to detect the FQDN range of the DNS Query request message. An I-SMF is inserted for the PDU session.

Step 6, The UE sends DNS Query Request message with the target FQDN over the user plane of the PDU session.

Step 7, The EASDF detects that the DNS Query message with the target FQDN.

Step 8, The EASDF forwards the DNS Query Request message with the target FQDN to the SMF and notifies that the FQDN is detected.

Step 9, The SMF determines that the DNS query can be routed to an Local DN, it selects target DNAI. The SMF may determine that the I-SMF can support the DNAI, then the SMF sends Nsmf\_PDUSession\_Update Request to the I-SMF, including the DNS Query Request message and the target DNAIs.

Step 10, The I-SMF selects L-SMF based on the target DNAI.

Step 11, The I-SMF invokes Nsmf\_PDUSession\_Create Request (SUPI, GPSI(if available), SMF SM Context ID, CN-Tunnel-Info, etc.) towards the L-SMF to establish user plane tunnel between the I-UPF and L-PSA controlled by the L-SMF.

Step 12, The L-SMF establishes N4 session with the L-PSA.

Step 13, The L-SMF sends Nsmf\_PDUSession\_Create Response(CN-Tunnel-Info, etc.) to the I-SMF.

Step 14, The I-SMF forwards the DNS Query Request towards the I-UPF, and the I-UPF forwards the DNS Query Request to Local DNS server via the L-PSA, similar as Option D in TS 23.548.

#### 6.7.2.3 L-SMF insertion after the SMF



Figure 6.7.2.3-1 L-SMF insertion after the SMF

Step 1, The SMF subscribes the notification of new L-SMF serving the target S-NSSAI and DNN newly registered in the NRF, or L-SMF profile has been updated.

Step 2, The L-SMF is registered in the NRF. The NF profiles includes the S-NSSAI, DNN, FQDN(range) that can be served by the L-SMF, Local DNS server address and associated DNAIs. When new L-UPF is deployed the L-UPF establishes N4 Node Association and the L-UPF provides the FQDN(range), Local DNS server address and associated DNAI. The L-SMF then update the NF profile stored in the NRF.

Step 3, The NRF notify the SMF about the NF profiles of the newly registered L-SMF, or the updated NF profile of L-SMF.

Step 4, The SMF generates/updates the BaselineDNSPattern based on the NF profiles of the new registered L-SMF and invokes Neasdf\_BaselineDNSPattern\_Create/Update service operation of the EASDF to create/update the BaselineDNSPattern.

Step 5, the UE establishes a PDN session towards the SMF. In this procedure the SMF configures the EASDF to detect the FQDN range of the DNS Query request message.

Step 6, The UE sends DNS Query Request message with the target FQDN over the user plane of the PDU session.

Step 7, The EASDF detects that the DNS Query message with the target FQDN.

Step 8, The EASDF forwards the DNS Query Request message to the SMF and notifies that the FQDN is detected.

Step 9, The SMF determines that the DNS Query Request can be routed to an Local DN, it selects a target DNAI. The SMF may determine that SMF/I-SMF cannot support the DNAI, then the SMF selects L-SMF based on the target DNAIs.

Step 10, The SMF invokes Nsmf\_PDUSession\_Create Request(SUPI, GPSI(if available), SMF SM Context ID, CN-Tunnel-Info, etc.) towards the L-SMF to establish user plane tunnel between the PSA and L-PSA controlled by the L-SMF.

Step 11, The L-SMF establishes N4 session with the L-PSA.

Step 12, The I-SMF sends Nsmf\_PDUSession\_Create Response(CN-Tunnel-Info, etc.) to SMF.

Step 13, The SMF forwards the DNS Query Request towards the PSA, and the PSA forward the DNS Query Request to Local DNS server via the L-PSA.

### 6.7.3 Impacts on services, entities and interfaces

L-PSA:

* The L-PSA is enhanced to reports the FQDN range that can be handled by the L-PSA, the associated Local DNS Server address and associated DNAI to L-SMF.

L-SMF(New NF):

- The L-SMF is introduced to control the L-PSA.

- L-SMF registers the FQDN range, the associated Local DNS Server address and associated DNAI in the NRF.

NRF:

- The NF profile of L-SMF is based on SMF profile, and further include the FQDN range, the associated Local DNS Server address and associated DNAI.

SMF:

- Subscribe the notification on the NF profile change of L-SMF serving the S-NSSAI and DNN.

- Receives the NF profile of the L-SMF and update the BaselineDNSPattern in the EASDF.

- The SMF is enhanced to insert the ULCL/BP/L-PSA or insert L-SMF/L-PSA after the SMF/I-SMF based on the detection of the FQDN and forward the DNS Query towards the ULCL/BP/L-PSA.

## 6.8 Solution #8: Selecting an EAS server leveraging analytics

### 6.8.1 Key Issue mapping

Editor's note: This clause lists the key issue(s) addressed by this solution.

This solution addresses the objectives of Key Issue #2 and in particular selecting the most suitable local UPF and EAS considering end to end delay.

### 6.8.2 Description

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

Currently, TS 23.548 [5] specifies how a UE DNS request can be routed via EASDF. The procedure to route UEs DNS request is as follows (as described in Figure 6.2.3.2.2-1 of TS 23.548 [5]).:

1.- When the UE establish a PDU session the SMF may selects an EASDF and provides the EASDF with DNS message handling rules. The rule includes actions on how to handle DNS requests and DNS responses.

3.- When the UE sends a DNS request the EASDF determines how to route the DNS request according to the DNS message handling rules. At this point the EASDF may determine that the request may need to be sent to an L-DNS.

4. When the EASDF receives a DNS response from an L-DNS server the response may contain a list of EAS IP addresses or a list of FQDNs.

5. The EASDF may report the list of EAS IP addresses or list of FQDNs to the SMF so as the SMF to determine the DNAI and associated N6 traffic routing information for the DNAI and whether a local PSA will need to be inserted.

6. The EASDF then forwards the DNS response to the UE.

7. At this point the UE selects an EAS server. If the UE has received multiple EAS IP addresses or the FQDN corresponds to multiple EAS server the UE may not know which EAS server has the best performance.

In order to ensure optimal EAS server selection it is proposed that when the EASDF reports the list of EAS IP addresses or list of FQDNs to the SMF, the SMF to leverage the NWDAF analytics to determine the EAS application server instance that offers the "best" performance. In this way the UE (at step 7) will receive only the EAS server address that offers the best performance (i.e. lowest end-2-end latency).

There are two Analytics IDs that the SMF can leverage when selecting an Edge Application Server:

- Service Experience Analytics that indicate an average of observed Service MoS and/or variance of observed Service MoS indicating service MOS distribution for services such as audio-visual streaming as well as services that are not audio-visual streaming such as V2X and Web Browsing services.

- DN Performance Analytics which provides analytics for user plane performance (i.e. average traffic rate, average packet delay) in the form of statistics or predictions for an Edge Application.

It is noteworthy to state that the NWDAF can also provide such analytics taking into account: Anchor UPF info, DNAI info.

The SMF can request Analytics for an Application over a specific Application Server Instance Address as described in clause 6.4.4 of TS 23.288 [6]. In addition, the SMF can request DN performance Analytics for an application as described in clause 6.14.4 of TS 23.288 [6].

As an example when the SMF receives two EAS IP addresses in the DNS response the SMF can request the following analytics:

- Analytics ID: "DN Performance Analytics" with analytics filters.

- Candidate Anchor UPF info (Identifies the UPF where a UE has an associated PDU session).

- Area of interest.

- EAS IP address(es) received in the response.

- Application ID, DNN, DNAI, S-NSSAI (if applicable).

The NWDAF provides analytics for DN performance analytics via the Anchor UPF which include packet delay information for each EAS server via the same Anchor UPF. In such scenario the SMF will select the EAS server that offer he best performance that guarantees the lowest N6 delay.

Once the SMF selects an EAS IP address based on NWDAF analytics the SMF notifies the EASDF within an Neasdf\_DNSContextUpdate Request, to include the selected EAS IP address in the DNS response to the UE. The EASDF modifies the buffered DNS response including in the response only the EAS IP address provided by the SMF.

### 6.8.3 Procedures

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

The procedure is described below:



Figure 6.8.3-1: Procedure for selecting an EAS server

1. A UE establishes a PDU session as described in TS 23.502 [3]

2. During the PDU session establishment procedure the SMF selects an EASDF to be used as a DNS server for this PDU session. The procedure is described in TS 23.548 [5].

3. The SMF determines initial DNS message handling rules. The initial DNS message handling rules instructs the EASDF to buffer DNS queries received by a UE on this PDU session and forward the contents of the DNS query to the SMF.

4. The SMF provides the DNS message handling rules to the EASDF by invoking an Neasdf\_DNSContext\_Create request.

5. The EASDF creates a DNS context for the UE and stores the DNS message handling rules as described in TS 23.548 [5].

6. The EASDF acknowledge the request

7. An application in the UE request to establish a connection with an EAS server and creates a DNS query.

8. The DNS query is received at the EASDF. The EASDF determines based on the DNS message handling rules that the DNS query needs to be buffered and the contents of the DNS query needs to be forwarded to the SMF.

9. The EASDF invokes an Neasdf\_DNSContext\_Notify request including in the request the contents of the DNS query. The contents of the DNS query may include a range of FQDN or may include an IP address of the DNS server requested by the application. Alternatively the EASDF provides the (list of) EAS IP addresses included in the DNS response from the DNS server.

10. The SMF acknowledges the response.

11. The SMF determines that analytics can be used to determine an EAS IP address.

12. The SMF constructs a request for analytics using: 1) the contents of the DNS query or 2) determines the EAS IP(es) or DNAI(s) based on the FQDN of DNS query and EAS Deployment Information firstly, and uses determined EAS IP address (es) or candidate PSA UPF (selected based on DNAI) or 3) the list of EAS IP address received in a DNS response.

13. The SMF sends an Analytics request including an Analytic ID set to DN Performance (or Service Experience) and include as analytic filters the location of the UE and the FQDN of the DNS query or determined EAS IP address (es) or candidate PSA UPF (selected based on DNAI), or the (list of) EAS IP address.

14. The NWDAF derives analytics.

15. In the analytics response the NWDAF includes a list of EAS server address and its associated performance.

16. The SMF may select the best performing EAS server.

17. The SMF may perform ULCL/PSA insertion based on the selected EAS server.

18. The SMF constructs an action for the EASDF where the action indicates to the EASDF to create a DNS response for the UE including the selected EAS IP address(es).

19. The SMF creates a service operation including an instruction/rule to the EASDF as described in step 19.

20. The EASDF acknowledges the request.

21. The EASDF constructs a DNS response or forwards the DNS response to the UE as instructed in steps 19-20.

22.The EASDF provides the DNS response with the selected EAS IP address(es) to the UE via the existing PDU session.

23. The application in the UE connects to the selected EAS server.

### 6.8.4 Impacts on services, entities and interfaces

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

SMF requesting existing analytics using the information in DNS request or DNS response as input data.

SMF selects an EAS based on the analytics response (i.e. a list of EAS server address and its associated performance) from NWDAF.

There are no impacts on the DN performance and/or Service Experience analytics as defined in TS 23.288 [6].

## 6.9 Solution #9: local UPF and EAS (re)selection jointly considering N6 delay and EAS load

### 6.9.1 Description

Per existing design of TS 23.548 [5], the (re)selection of the EAS and local PSA by 5GC is based on the UE location and EAS Deployment Information, which only considers the topology information of UE, UPF and EAS. Nevertheless, dynamic information especially the N6 delay between the local PSA and EAS, and EAS load, which contributes to the End to end delay (i.e. between the UE and EAS), are also important factors that should be taken into account.

Some consideration that EAS load has been considered when the DNS server returns the DNS response back to the client. However, these parameters are considered separately. It is better to have one NF jointly consider these parameters and also get the real time measurement.

Comparing to the solution discussed for KI#1, this solution focus on how the N6 delay and EAS load is used for L-PSA/EAS (re)selection.

### 6.9.3 Procedures

#### 6.9.3.1 Enhancement on EAS Deployment Information Management

The EAS deployment information provisioned from AF to 5GC as defined in clause 6.2.3.4 of TS 23.548 [5] is used for local UPF and EAS (re)selection. It is proposed to enhance this information as following:

Table 6.9.3.1-1: Additional information of EAS Deployment Information

|  |  |
| --- | --- |
| Parameters | Description |
| … | …. |
| Delay-sensitive indication | the application demands end to end delay requirement [optional]. |
| AF/NEF address information | Target Address for event subscription [optional].  (See NOTE 5). |
| NOTE 4: It includes End to end delay, i.e. the sum of N6 delay between local PSA and EAS, delay between UE and local PSA and processing delay for a specific application.  NOTE 5: If the AF is trusted, the AF provides AF address information during the EDI provision process. Otherwise, NEF provides the NEF address information to replace the address information provided by the AF. | |

#### 6.9.3.2 EAS/L-PSA discovery procedure with EASDF

Normally the EAS load can be converted to the processing delay (e.g. https://ieeexplore.ieee.org/abstract/document/9253665). Hence when the EAS reports how much percentage of load EAS reaches, based on the local configuration, the percentage of load can be converted to the how much processing delay the EAS needs.

The procedure of EAS/L-PSA discovery procedure with EASDF is defined as in Figure 6.9.3.2-1. The AF requests End-to-end delay requirement of the application for EAS discovery as described in step 1-5 of figure 4.3.6.2-1 in TS 23.502 [3] before the following procedure.



Figure 6.9.3.2-1: EAS discovery procedure with EASDF

1. Same as step 1 - step 12 of clause 6.2.3.2.2 in TS 23.548 [5].

2. same as step 13 as described in clause 6.2.3.2.2 of TS 23.548 [5].

3. same as step 14/15 as described in clause 6.2.3.2.2 of TS 23.548 [5].

NOTE 1: The SMF can be changed to other NF per the discussion of the KI#1.

4a/4b. If the matched DNS response message corresponding to the delay sensitive application, i.e. which has provisioned the Delay-sensitive indication as part of EDI, SMF subscribe to the EAS load information from AF by sending the received EAS IP (s)/FQDN(s), subscribed event to AF through NEF. The event subscription also includes the Immediate reporting flag and reporting threshold, e.g. load level.

4c. SMF subscribe to the EAS load information (e.g., percentage of the load or EAS processing delay) from AF by sending the received EAS IP (s)/FQDN(s), subscribed event directly. The event subscription also includes the Immediate reporting flag and reporting threshold, e.g. load level.

4d/4e. AF notifies SMF of EAS load information (e.g., percentage of the load or EAS processing delay) corresponding to the received EAS IP (s)/FQDN(s) through NEF immediately. The EAS load is reported as percentage of EAS Instance load.

4f. AF notifies SMF of EAS load information corresponding to the received EAS IP (s)/FQDN(s) immediately. The EAS load is reported as the percentage of EAS Instance load.

NOTE 2: The application service provider may decide the specific format of the provided EAS load information. For example, the application service provider can decide whether to provide percentage of the load or EAS processing delay based on configuration. The EAS itself supports the ability to monitor the percentage of EAS load in real time, and application server can simply send this information to 5GC via AF. However, for EAS processing delay provisioning, the delay statics function needs to be added to the EAS during application running, which may introduce additional system overhead for the EAS.

NOTE 3: The AF can also send a notification when a condition is met, e.g. the load level of the EAS (e.g., percentage of the load or EAS processing delay) meets the reporting threshold. The details are described in clause 6.9.3.3. It is assumed the AF is willing to provide EAS load information (e.g., percentage of the load or EAS processing delay) to use the optimization from 5GC.

5. SMF performs EAS load-Processing delay conversion, i.e. convert the percentage of EAS load to the processing delay.

NOTE 4: The relationship between percentage of EAS load and processing delay can be pre-configured on SMF. Step 5 can be skipped if the AF provides EAS load information with the format of the EAS processing delay directly.

6. SMF informs candidate local PSA(s) to measure the real-time N6 delay between the L-PSA and the reported EAS IP(s). In details, SMF determine the candidate Local PSA(s) base on the reported EAS IP(s) and Local PSA information. Then, the candidate local PSA(s) obtain the N6 delay by using certain Layer 3 measuring mechanisms respectively, e.g. via ICMP as defined in RFC 792 [7].

NOTE 4: Step 6 can be executed in parallel with steps 4 or 5.

7. SMF determines suitable EAS and L-PSA based on the end-to end delay requirement.

NOTE 5: The delay between UE and PSA UPF is controlled by the PDB in the 5QI. Thus only N6 delay and processing delay are measured for EAS and PSA selection.

8. Same as step 16 - step 19 as described in clause 6.2.3.2.2 of TS 23.548 [5].

For EAS/L-PSA discovery procedure with local DNS server mechanism, the L-PSA is inserted either per DNS query or per UE mobility before DNS query. For the L-PSA inserted per DNS query, same procedure (i.e. Step 4 -7) as described above can be executed.

#### 6.9.3.3 EAS/L-PSA rediscovery at Edge Relocation

It is assumed that the SMF, which re-discovers the EAS/L-PSA, can be other NF per the discussion of KI#1.



Figure 6.9.3.3-1: EAS/L-PSA rediscovery procedure at Edge relocation

This procedure is used to trigger the EAS (or L-PSA) rediscovery procedure when a new connection between EAS and L-PSA need to be established. This rediscovery can be triggered in three cases:

- **Case 1:** SMF triggered EAS rediscovery based on reported EAS load (e.g., percentage of the load or EAS processing delay) as the end-to end delay requirement is not satisfied.

- **Case 2:** SMF triggered L-PSA or EAS rediscovery based on measured N6 delay as end-to end delay requirement is not satisfied.

- **Case 3:** AF triggered EAS rediscovery as EAS load balance or maintenance, etc.

1. Perform EAS and L-PSA discovery as described in clause 6.9.3.2.

**Case 1: EAS load trigger EAS rediscovery:**

2. AF notifies SMF of EAS load information (e.g., percentage of the load or EAS processing delay) corresponding to the EAS IP (s) through NEF or directly when the event condition is met, e.g. the EAS load (e.g., percentage of the load or EAS processing delay) exceed the load threshold set by SMF. The SMF sets load threshold based on the end to end delay requirement in the EDI.

3. The same as step 5 of clause 6.9.3.2.

NOTE 1: The step 3 can be skipped if the AF provides EAS load information with the format of the EAS processing delay directly.4. SMF triggers EAS discovery as the end-to end delay requirement are not satisfied.

**Case 2: N6 delay trigger L-PSA or EAS rediscovery:**

5. The SMF subscribes the N6 delay measurement event to L-PSA. This event subscription can be per event threshold or periodically. The UPF report the measured real-time N6 delay to the SMF by using certain Layer 3 measuring mechanisms respectively, e.g. via ICMP as defined in RFC 792 [7]. The SMF judges that the N6 delay exceed the related threshold per end-to-end delay requirement provisioned in EDI.

6. If there are candidate L-PSA(s), e.g. different L-PSA to the same DNAI, the SMF informs the candidate L-PSA(s) to measure the N6 delay to the indicated EAS instance.

7. If the calculated end-to end delay of the candidate L-PSA(s) can fulfil the end-to end delay requirement, the SMF triggers the L-PSA reselection and following steps are skipped, i.e. Step 8-9 are skipped. Otherwise SMF trigger EAS rediscovery as the end-to end delay requirement are not satisfied.

**Case 3: AF trigger EAS rediscovery:**

8. AF trigger EAS rediscovery as EAS load balance or maintenance, etc.

9. Same as step 2 of clause 6.2.3.3.3 in TS 23.548 [5].

### 6.9.3 Impacts on services, entities and interfaces

**AF/NEF:**

- Provide enhanced EDI information as described above.

- Provide the EAS load information (e.g., percentage of the load or EAS processing delay) to SMF per event subscription.

- Provide AF influence related information as described above.

**SMF:**

- Get enhanced EDI information and EAS load information (e.g., percentage of the load or EAS processing delay) from AF.

- Perform EAS load - processing delay conversion.

- Instructs UPF to measure the real-time N6 delay.

- Determine suitable EAS and L-PSA based on the above information.

## 6.10 Solution #10: L-PSA and EAS (re)selection based on N6 one-way and two-way delay measurement

### 6.10.1 Key Issue mapping

This solution is related to the KI#2.

### 6.10.2 Functional Description

This solution is applied in 5GS architecture for non-roaming scenario supporting Edge Computing as Figure 4.2-1 or Figure 4.2-2 of TS 23.548 [5].

In this solution, SMF performs L-PSA UPF and EAS (re)selection based on the measured N6 delay. The measurement of N6 delay is as follows:

- In the case for uplink (UL) N6 delay measurement, SMF requests L-PSA to send a N6 delay measurement packet to EAS, encapsulating local time T1 of sending the packet. The EAS records the local time T2 when receiving the N6 delay measurement packets and calculates the UL N6 delay and responds to the L-PSA. The L-PSA reports the UL N6 delay to the SMF.

- In the case for downlink (DL) N6 delay measurement, SMF requests L-PSA to measure DL N6 delay, and the L-PSA sends a request to EAS. The EAS sends a N6 delay measurement packet to L-PSA, encapsulating local time T3 of sending the packet. The L-PSA records the local time T4 when receiving the N6 delay measurement packets and calculates the DL N6 delay. The L-PSA reports the DL N6 delay to the SMF.

In order to support the synchronization between PSA UPF(s) and EAS(s) to support the one-way delay measurement, the NTP (Network Time Protocol) or PTP (Precise Time Protocol) can be introduced.

- In the case round-trip (RT) N6 delay measurement (without the EAS application part), SMF requests L-PSA to send a N6 delay measurement packet to EAS, encapsulating local time T1 of sending the packet. The EAS records the local time T2 when receiving the N6 delay measurement packets. Then the EAS responds the L-PSA with response packet, encapsulating local time T3, and L-PSA records the local time T4 of receiving the N6 delay measurement packet. The L-PSA calculates the RT N6 delay based on the (T2-T1+T4-T3), and reports the RT N6 delay to the SMF.

The protocols which can be used to support the above N6 delay monitoring, for example, includes:

- RFC 4656: A One-way Active Measurement Protocol (OWAMP).

- RFC 5357: A Two-Way Active Measurement Protocol (TWAMP).

### 6.10.3 Procedures



Figure 6.10.3-1: Procedure of L-PSA and EAS reselection based on N6 delay measurement

1. The EAS discovery procedure is performed as described in clause 6.2.3.2.2 or clause 6.2.2.2 of TS 23.548 [5].

2. PCF based on local configuration, sends N6 delay measurement requirement to AF via NEF, including N6 delay measurement ID, L-PSA address, indication to support UL N6 delay measurement or DL N6 delay measurement or RT N6 delay measurement, optionally including reporting frequency. PCF may also send protocol indication of OWAMP alignment with UL/DL N6 delay measurement, protocol indication of TWAMP alignment with RT N6 delay measurement to NEF/AF. Once the AF find the indicated protocol is not supported, the AF may provide another suggested protocol, and PCF authorizes the requested protocol.

3. PCF reuses steps 3-5 of the SM Policy Association Modification procedure as described in clause 4.16.5.2.1 of TS 23.502 [3] to update PCC rules, including N6 delay measurement policy. The N6 delay measurement policy may include indication for UL N6 delay measurement or DL N6 delay measurement or round-trip (RT) N6 delay measurement, as well as the protocol indication (OWAMP or TWAMP).

NOTE: The AF may indicate EAS to support UL N6 delay measurement, DL N6 delay measurement or round-trip N6 delay measurement. The details are out of SA WG2 scope.

If UL N6 delay measurement is required by PCF, the following steps 4a, 5a, 6a and 7a are performed:

4a. The SMF sends a N6 delay measurement request to the L-PSA via N4 to request the UL N6 delay measurement between L-PSA and EAS, may include the protocol indication of OWAMP. The N6 delay measurement request may contain EAS IP address and measurement parameters determined by SMF based on the authorized N6 delay measurement policy received from the PCF and/or local configuration. The measurement parameter includes UL N6 delay indication and reporting frequency. If the L-PSA does not support OWAMP, it includes failure and "OWAMP is not supported" cause value in the N4 session establishment response message.

5a. The L-PSA creates and sends the N6 delay measurement packet to the EAS in a measurement frequency. The L-PSA encapsulates in the N6 delay measurement packet with UL N6 delay measurement packet indicator (which indicates the packet is used for UL N6 delay measurement) and the local time T1 when the L-PSA sends out the N6 delay measurement packet.

6a. The EAS records the local time T1 received in the N6 delay measurement packet and the local time T2 at the reception of the N6 delay measurement packet. The EAS calculates the UL N6 delay and sends N6 delay measurement response packet. The EAS encapsulates the UL N6 delay measurement packet indicator and the UL N6 delay in the N6 delay measurement response packet.

7a. The L-PSA sends report to SMF, including the UL N6 delay and the EAS IP address.

If DL N6 delay measurement is required by PCF, the following steps 4b, 5b, 6b and 7b are performed:

4b. The SMF sends a N6 delay measurement request to the L-PSA via N4 to request the DL N6 delay measurement between L-PSA and EAS, may include the protocol indication of OWAMP. The N6 delay measurement request may contain EAS IP address and measurement parameters determined by SMF based on the authorized N6 delay measurement policy received from the PCF and/or local configuration. The measurement parameter includes DL N6 delay indication and reporting frequency. If the L-PSA does not support OWAMP, it includes failure and "OWAMP is not supported" cause value in the N4 session establishment response message.

5b. The L-PSA creates and sends DL N6 delay measurement request to the EAS. The L-PSA encapsulates in the N6 delay measurement packet with DL N6 delay measurement packet request indicator (which indicates the packet is used for DL N6 delay measurement request).

6b. The EAS creates and sends the N6 delay measurement packet to the L-PSA in a measurement frequency. The EAS encapsulates in the N6 delay measurement packet with DL N6 delay measurement packet indicator and the local time T3 when the EAS sends out the N6 delay measurement packet.

7b. The L-PSA records the local time T4 received in the N6 delay measurement packet. The L-PSA calculates the DL N6 delay. The L-PSA sends report to SMF, including the DL N6 delay and the EAS IP address.

If RT N6 delay measurement is required by PCF, the following steps 4c, 5c, 6c and 7c are performed:

4c. The SMF sends a N6 delay measurement request to the L-PSA via N4 to request the RT N6 delay measurement between L-PSA and EAS, may including the protocol indication of TWAMP. The N6 delay measurement request may contain EAS IP address and measurement parameters determined by SMF based on the authorized N6 delay measurement policy received from the PCF and/or local configuration. The measurement parameter includes RT N6 delay indication and reporting frequency. If the L-PSA does not support TWAMP, it includes failure and "TWAMP is not supported" cause value in the N4 session establishment response message.

5c. The L-PSA creates and sends the N6 delay measurement packet to the EAS in a measurement frequency. The L-PSA encapsulates in the N6 delay measurement packet with RT N6 delay measurement packet indicator (which indicates the packet is used for RT N6 delay measurement) and the local time T1 when the L-PSA sends out the N6 delay measurement packet.

6c. When receiving an N6 delay measurement packet from L-PSA with RT N6 delay measurement packet indicator, the EAS creates and sends the N6 delay measurement response packet to the L-PSA:

- The EAS encapsulates in the N6 delay measurement response packet with RT N6 delay measurement packet indicator, the time T1 received in the N6 delay measurement packet, the local time T2 at the reception of the N6 delay measurement packet and the local time T3 when the EAS sends out this response packet.

7c. The L-PSA records the local time T4 when receiving the N6 delay measurement response packet and calculates the RT N6 delay based on (T2-T1+T4-T3), and reports the RT N6 delay and the EAS IP address to the SMF.

8. If the SMF determines the N6 delay (UL or DL or RT N6 delay) is exceeded the N6 delay threshold, which may be configured in SMF or provided by PCF, then the SMF sends the N6 delay, L-PSA address and EAS address to PCF by invoking Npcf\_SMPolicyControl\_Update Request.

9. The PCF invokes Npcf\_SMPolicyControl\_Update Response to update the SM Policy to the SMF, including UL/DL/RT N6 delay per L-PSA per EAS, which may be measured based on other traffic flows.

10. The SMF may re-select the L-PSA and EAS, and triggers edge relocation as described in clause 6.2.3.3 or clause 6.2.2.3 of TS 23.548 [5].

### 6.10.4 Impacts on existing services, entities and interfaces

**SMF:**

- Sending N6 delay measurement request to L-PSA to request UL/DL/RT N6 delay measurement.

- Sending request to PCF if determines N6 delay is exceeded N6 delay threshold.

- Performing EAS re-discovery procedure at edge relocation based on N6 delay.

**L-PSA:**

- Sending N6 delay measurement packet or N6 delay measurement request to EAS.

- Calculating DL/RT N6 delay.

- Reporting N6 delay to SMF.

- Sending failure and "OWAMP is not supported" or "TWAMP is not supported" cause value if OWAMP/TWAMP is not supported.

**EAS:**

- Sending N6 delay measurement packet or N6 delay measurement response packet to L-PSA.

- Calculating UL N6 delay.

**PCF:**

- Sending N6 delay measurement requirement to AF via NEF.

- Sending N6 delay measurement policy to SMF.

- Sending N6 delay per L-PSA per EAS to SMF.

## 6.11 Solution #11: Provision weight factor of DNAIs from AF

### 6.11.1 Description

This solution is for key issue #2.

The following NOTE is quoted from TS 23.548 [5]:

*NOTE 12: If multiple candidate DNAIs are available after considering the UE location, network topology and EAS deployment, the SMF selects one DNAI from the multiple ones based on operator's policy. For examples, the SMF can select the DNAI randomly, or based on selection weight factor if provided by AF, or select the DNAI closest to the UE location.*

The SMF may use the selection weight factor for each DNAI to select a target DNAI. It is unclear how the selection weight factor is provided by the AF. This solution propose that the AF can provide the selection weight factor for each DNAI to the SMF in the EAS Deployment information. The following shows example on how the weight factor is set corresponding to the EAS load:

- When the EAS load associated with the DNAI is low, the weight factor of the DNAI can be set to high value, which increases the possibility to select the corresponding DNAI.

- When the EAS load associated with the DNAI increase, the weight factor of the DNAI can be set according to relative capacity of EAS associated with the DNAIs, which ensures the selection of DNAI to be associated with the relative capacity of the EAS associated with the DNAIs.

- When the EAS load associated with the DNAI reaches threshold, the weight factor of the DNAI can be set to low value, which reduce the possibility to select the corresponding DNAI. Value 0 indicates the DNAI is not permitted for the EAS traffic.

NOTE: In order to reduce the signalling load of the providing EDI towards the SMF, it is expected that AF will not change the weight factor of the DNAI very frequently.

In addition, the AF may also provide average delay over N6 interface associated with the DNAI in the EAS Deployment information. The SMF can obtain the delay between the UE and DNAI/UPF by using QoS monitoring. When the SMF receives E2E delay requirements in the PCC rule, the SMF selects DNAI/UPF via which the E2E delay (UE to UPF delay + N6 interface delay) can meet the E2E delay requirements.

### 6.11.2 Procedures



Figure 6.11.2-1: EAS Deployment Information management in the AF procedure

1. The AF invokes the Nnef\_EASDeployment\_Create/Update service operation. This request may contain the following additional information:

- Selection weight factor per DNAI: selection weight for each DNAI when there are more than one DNAIs provided by the AF. The weight factor for each DNAI can be set according to the clause 6.11.1.

- Average delay over N6 interface per each DNAI: the average delay between the UPF and EAS(es) in the Data Network. Each EAS measures N6 delay by using Layer 3 measuring mechanisms respectively, e.g. via ICMP as defined in RFC 792[7]. The AF calculates an average delay over N6 interface for the DNAI by considering the measurement result from all EASs associated with DNAI.

2. NEF checks whether the AF is authorized to perform the request, and authorised to provision the EAS Deployment Information based on the operator policies.

3. The NEF invokes the Nudr\_DM\_Create/Update to the UDR if it is authorized.

4. The UDR stores/updates the corresponding information received from the AF. And responds a Nudr\_DM\_Create/Update Response to the NEF.

5. The NEF sends Nnef\_EASDeployment\_Create/Update Response to the AF.

### 6.11.3 Impacts on services, entities and interfaces

The EAS Deployment information is enhanced to include the selection weight factor per DNAI, average delay over N6 interface per DNAI.

The SMF is enhanced to use the new information in the EAS Deployment information to select DNAI.

## 6.12 Solution #12: NWDAF and SMF-based EAS and local UPF (re)selection

### 6.12.1 Key Issue mapping

The following solution corresponds to the key issue key issue #2 on enhancement of EAS and local UPF (re)selection.

### 6.12.2 Description

The AF may request EAS discovery based on N6 delay and/or EAS load. The SMF determines the N6 delay between each candidate PSA UPF and EAS via indicating PSA UPF to report the N6 delay measurements or receives delay analysis information from NWDAF, or determines the EAS load based on the information received from NWDAF. The SMF selects a target EAS and a local PSA UPF based on the determined N6 delay and/or EAS load, and indicates the selected EAS IP address to EASDF via DNS message handling rule.

### 6.12.3 Procedures

#### 6.12.3.1 NWDAF and SMF-based EAS and local UPF (re)selection



Figure 6.12.3.1-1: Procedure for NWDAF and SMF-based EAS and local UPF (re)selection

1. [Optional] The AF request in step 1 of figure 4.3.6.2-1 in TS 23.502 [3] is used to request EAS discovery based on N6 delay and/or EAS load. The AF request may include Indication for N6 delay based EAS discovery, Indication for EAS load based EAS discovery. In step 5 of figure 4.3.6.2-1 of TS 23.502 [3], the PCF creates PCC rule with Indication for N6 delay based EAS discovery, Indication for EAS load based EAS discovery.

2. The UE triggers PDU session establishment procedure and sends DNS query to EASDF, and EASDF retrieves the DNS response (including EAS information, e.g. one or more EAS IP addresses) from DNS server and notifies the DNS message reporting to SMF as shown in step 1-15 of figure 6.2.3.2.2-1.

3. Based on the local policy or PCC rule received from PCF in step 2, the SMF determines the N6 delay or EAS load should be taken into consideration for EAS and local UPF selection.

Based on EAS information received from the EASDF in Neasdf\_DNSContext\_Notify of step 2 and other UPF selection criteria, the SMF determines one or more candidate PSA UPF(s). The SMF also receives one or more candidate EAS(s) as indicated in EAS information.

The SMF determines the N6 delay between each candidate PSA UPF and EAS via following step 3a and/or 3b, and SMF may receive EAS load via step 3b.

3a. [Optional] The procedure described in clause 6.12.3.2 is triggered to perform N6 delay measurement and reporting. The SMF sends Session Reporting Rule to each candidate PSA UPF, which includes the EAS information to indicate the PSA UPF to report the N6 delay (between PSA UPF and EAS) measurements.

The UPF measures the UL and/or DL N6 delay (e.g. via RTT measurement) and sends N4 Session Report to SMF to report the N6 delay measurements. The SMF responds with an N4 session report ACK message.

3b. [Optional] The SMF sends Nnwdaf\_AnalyticsInfo\_Request or Nnwdaf\_AnalyticsSubscription\_Subscribe to request NWDAF to provide delay (e.g. UL/DL Average Packet Delay) and/or EAS load. The SMF receives the delay and/or EAS load from NWDAF via Nnwdaf\_AnalyticsInfo\_Request response or Nnwdaf\_AnalyticsSubscription\_Notify.

For the N6 delay case:

The request sent by SMF includes Analytics ID = "DN Performance", Analytics Filter Information = Application Server Address(es) (i.e. list of EAS IP addresses receives in step 2), Target of Analytics Reporting= SUPI of target UE, a list of analytics subsets are requested = "Average Packet Delay" and/or "Maximum Packet Delay". The response sent by NWDAF includes "Average Packet Delay" and/or "Maximum Packet Delay". The procedure described in clause 6.14.4 of TS 23.288 [6] is used.

Then the SMF determines the UL/DL N6 delay by subtracting the UL/DL PDB (delay between UE and PSA UPF) from UL/DL Average Packet Delay (delay between UE and EAS).

For the EAS load case:

The AF provides original EAS load to NWDAF (via NEF) as input data for load analytics, and the EAS load statistics and predictions can be provided by NWDAF as output analytics. The request sent by SMF includes Analytics ID = "NF load information", Analytics Filter Information = EAS instance ID(s) (e.g. determined based on the list of EAS IP addresses receives in step 2), Target of Analytics Reporting= SUPI of target UE, a list of analytics subsets are requested = "EAS load". The response sent by NWDAF includes "EAS load".

4. The SMF selects an EAS and a local PSA UPF based on the N6 delay and/or EAS load determined in step 3a and/or 3b.

5. The SMF inserts the Local PSA UPF.

6a. The SMF sends the updated DNS message handling rule to EASDF via Neasdf\_DNSContext\_Update Request. The DNS message handling rule includes the selected EAS IP address.

6b. The EASDF responds with Neasdf\_DNSContext\_Update Response.

7. The EASDF sends the DNS Response with selected EAS IP address to the UE as indicated in the DNS message handling rule.

#### 6.12.3.2 N6 delay measurement and reporting



Figure 6.12.3.2-1: procedure for N6 delay measurement and reporting

The steps 1-2 of Figure 6.12.3.1-1 are performed.

1. TSMF sends the N4 message to the PSA UPF with the EAS information (e.g. list of EAS IP addresses), which indicates the PSA UPF to measure the N6 delay between the UPF and each EAS.

2. The UPF receives the N4 request, and then it generates ICMP Echo message [8] and sends it to EAS.

NOTE: By configuration, the UPF knows the EAS support the ICMP.

3. The UPF receives the ICMP Echo response [y] from EAS and measures the time that elapses between the transmission of Request message and the reception of Response message. The PSA UPF computes an accumulated packet delay by adding RTT/2 and processing time (if available).

4. The UPF reports the N6 delay to SMF via N4 report.

### 6.12.4 Impacts on services, entities and interfaces

**SMF:**

1. Determines the N6 delay or EAS load should be taken into consideration for EAS and local UPF selection based on local policy or PCC rule.

2. Determines one or more candidate PSA UPF(s) and EAS(s), and configures PSA UPF to report the N6 delay between each candidate PSA UPF and EAS, and/or retrieves delay information or EAS load from NWDAF.

3. Selects a target EAS and a local PSA UPF based on the determined N6 delay and/or EAS load, and indicates the selected EAS IP address to EASDF via DNS message handling rule.

4. Determines the UL/DL N6 delay by subtracting the UL/DL PDB (delay between UE and PSA UPF) from UL/DL Average Packet Delay (delay between UE and EAS).

**UPF:**

1. Measures and reports the N6 delay (between PSA UPF and EAS).

**NWDAF:**

1. Provides analytics/predictions on the EAS load information.

**AF:**

1. Provides the EAS load to NWDAF for EAS.

2. Provides “Indication for N6 delay based EAS discovery” and “Indication for EAS load based EAS discovery” via AF request.

**NEF:**

1. Receives the EAS load from AF and provides to NWDAF.

## 6.13 Solution #13: EAS Discovery taking account of EAS load in EASDF

### 6.13.1 Key Issue mapping

This solution addresses EAS Discovery considering EAS load aspects of KI#2.

### 6.13.2 Description

The EAS load information can be known by AF (Application Function), AF can update the EAS load information to EASDF or DNS Server in some interval or range threshold which can be configured in AF. Then during the EAS discovery procedure (in Figure 6.13.2-1), the EASDF can discover and select a suitable EAS by taking account of the EAS load information.



Figure 6.13.2-1: EAS Discovery using EASDF procedure (clause 6.3.2.2.2 in TS 23.548 [5])

AF is supposed to store the latest EAS load information, ESADF can subscribe to AF for EAS load information update, then AF can notify the EASDF with the latest EAS load information. The subscription can be per FQDN(s), FQDN range, IP address(es), IP range. The AF can be configured to report in some interval or percentage change range of EAS load.

The EAS load information includes one or more of following:

- load percentage of general resource;

- load percentage of memory resource;

- load percentage of storage resource;

- load percentage of processor resource;

- load percentage of network resource.

### 6.13.3 Procedures

#### 6.13.3.1 EAS load subscription and notification procedure



Figure 6.13.3-1: EAS load subscription and notification procedure

1. EASDF subscribes to AF for EAS load change notification per EAS identifier. The operator can configure the EASDF to serve a list of AFs and EASs, the EASDF subscribes to the selected AFs based on the configured list of AFs.

2. AF is configured with notification condition/trigger which can be time interval or EAS load change range.

3. AF notifies EASDF the latest EAS load per subscribed EAS identifier.

The EAS identifier can be EAS FQDN(s), FQDN range, IP address(es), IP range.

### 6.13.4 Impacts on services, entities and interfaces

**Impact to EASDF:**

- EASDF subscribes to AF for EAS load notification per EAS identifier.

- EASDF stores the EAS load information and selects a suitable EAS for the received EAS Discovery request from UE taking account of EAS load information.

**Impact to AF:**

- AF collects and stores EAS load information.

- AF notifies EASDF about latest EAS load with configured notification trigger.

## 6.14 Solution #14: EAS selection considering DNS historical handling records

### 6.14.1 Key Issue mapping

Key issue #2.

### 6.14.2 Description.

This solution is for Key Issue #2 to address the issue on how to consider EAS load for enhanced EAS selection.

This solution proposes to consider DNS historical handling records by enhancing EASDF. As EAS load information itself is dynamic and resides in the management system of EAS, it would be hard and burdensome for 5G NF to obtain such information in real time. Thus, it is necessary to utilize alternative information that can represent the EAS load status and that can be easily available at the NF. The DNS historical handling records, which can be tracked and stored by the EASDF, is one of such alternative information representing the EAS load status.

This solution proposes to enhance the EASDF to store the DNS resolution records and provides the information to the SMF, so that the SMF can provide guide for EAS selection considering such information.

For example, the DNS historical handling records is defined as in the following table.

Table 6.14.2-1: DNS historical handling records

|  |  |
| --- | --- |
| Information | Description |
| FQDN | FQDN in the DNS query. |
| > List of DNS handling records (1,… , max) | List of the recorded number of for each EAS IP address in the DNS response forwarded to the UE. |
| … | … |

### 6.14.3 Procedures

This solution addresses a scenario where the EASDF receives multiple EAS IP addresses from the DNS system.



Figure 6.14.3-1: EAS selection considering DNS historical handling records

1. The EASDF performs the DNS resolution as described in TS 23.548 [5]. The EASDF creates the DNS historical handling records by storing the result of the DNS resolution for a given period.

The DNS historical handling records contains the number of DNS responses, which were decided to forward to the UE, with respect to the given EAS IP address or FQDN.

NOTE: If the DNS response contains multiple IP addresses, the EASDF can generate records for all the IP addressed or choose one of them to be recorded and reported to the SMF based on the local configuration.

NOTE: It will be evaluated how accurately DNS historical records collected at EASDF can represent the EAS load.

2. The EASDF reports the DNS historical handling records as the estimated EAS load information to the SMF.

3. A DNS query is sent to the EASDF after the DNS historical handling records is created, and the EASDF receives the DNS Response including multiple EAS IP addresses determined by the DNS system.

4. The EASDF sends to the SMF the notification related to the DNS response with providing EAS IP addresses while buffering the DNS response.

5. The SMF performs EAS selection considering the DNS historical handling records, if available for the EAS IP addresses included in the notification from the EASDF.

6. The SMF provides the selected EAS to the EASDF by invoking Neasdf\_DNSContext\_Update service operation.

7. The EASDF sends the DNS response containing the selected EAS.

### 6.14.4 Impacts on services, entities and interfaces

**EASDF:**

- creates and provides DNS historical handling records to the SMF.

**SMF:**

- performs EAS selection considering DNS historical handling records received from the EASDF.

## 6.15 Solution #15: The local EASDF assist for the EAS and local UPF (re)selection based on the AF provided N6 delay and EAS load information

### 6.15.1 Description

The 5GC not considering the network metrics(e.g. N6 delay) and the compute metrics(e.g. EAS load) has the possibility to provide suboptimal EAS address to the UE and result in redundant EAS rediscovery or Edge relocation.

The N6 delay for each DNAI which is not constant and the EAS load status information subject for frequent update needs consideration for the signalling and computation overhead aspect to be managed by the SMF having heavy impact for the centralized control in the current design.

This solution proposes the local EASDF to support EAS and local UPF (re)selection based on the N6 delay and the EAS load information from the AF. This assumes the AF can provide the N6 delay between candidate local PSA UPF(s) and EAS in the local DN and the EAS load information to be taken into account for the SMF to perform EAS and local UPF (re)selection with following enhancement:

- The AF registers its available data to the EASDF via OAM configuration at NEF including the N6 delay and the EAS load information and notifies the information conditionally or periodically to the EASDF via NEF.

- The local EASDF is configured to manage the N6 delay and the EAS load information and subscribes to the AF to get notified with the N6 delay and the EAS load information and may also be pre-configured or instructed by the SMF with condition to request EAS re-discovery to the SMF upon the updates from the AF.

### 6.15.2 Procedures



Figure 6.15.2.1: EAS re-discovery based on the N6 delay and the EAS load information

1. The AF registers its available data (i.e. N6 delay and the EAS load information) to the NEF via OAM and the NEF updates its NF Profile to the NRF to register that it supports exposure of AF available data (i.e. N6 delay and EAS load information).

2-4. The local EASDF is configured to manage the metric information and with necessary information to subscribe to the AF for the N6 delay and the EAS load information.

The local EASDF discovers the AF available data using the AF ID and the NEF to which the AF available data can be provided and subscribes to the AF via NEF to be notified for the N6 delay and the EAS load information.

5-6. Based on the subscription in the step 3, the AF notifies the local EASDF conditionally or periodically for the event related to the N6 delay and the EAS load and provides the following information:

- N6 delay information per DNAI.

- EAS load information:

- Indication for the EAS in overload status.

- IP address of the EAS.

The AF is configured with the information needed for the measurement or has the knowledge for the EAS load and the measures the N6 delay of candidate DNAI(s) with the existing traffic flows between candidate L-PSA(s) and the EAS in the local part of the DN and provides information to the local EASDF.

7-9. During PDU Session Establishment, the SMF selects the local EASDF and EAS Discovery Procedure with EASDF is performed taking into account the N6 delay and the EAS load information available in the local EASDF.

Upon reception of the DNS response message from the UE, the EASDF reports EAS information to the SMF together with N6 delay and EAS load information if available to be taken into account for EAS discovery.

10-11. The AF notifies the local EASDF for the event related to the N6 delay and the EAS load information.

12-13. The EASDF can be pre-configured or instructed from the SMF to request for the EAS re-discovery jointly considering the updated N6 delay and EAS load information from the AF using Neasdf\_DNSContext\_Notify with extension to include target UE information.

The SMF sends PDU Session Modification Command to the UE for the EAS re-discovery.

### 6.15.3 Impacts on Existing Nodes and Functionality

**AF:**

- Registers its available data at the NEF including the N6 delay and the EAS load information.

- Sends notification to the EASDF via NEF for the event with the N6 delay and the EAS load information.

**SMF:**

- Instructs the local EASDF to subscribe and manage the N6 delay and the EAS load information to be taken into account for EAS (re)discovery and provides necessary information for AF discovery and subscription.

- Initiates the EAS re-discovery procedure and local UPF (re)selection by the request from the EASDF.

**EASDF:**

- Discovers the AF available data via NEF to which the AF available data can be provided.

- Subscribes to the AF via NEF to be notified for the N6 delay and the EAS load information as instructed by the SMF.

- Receives notification from the AF with the N6 delay and the EAS load information and manage the information locally to be kept updated.

- Requests the SMF to perform the EAS re-discovery for the UEs served by the EAS based on pre-configuration or instruction with conditions upon updates from the AF for the N6 delay and EAS load information .

**NEF:**

- Subscribes for the N6 delay and EAS load information to the AF based on the EASDF subscription information.

- Provisions the N6 delay and EAS load information provided by the AF to the EASDF.

## 6.16 Solution #16: Local UPF and EAS (re)selection considering access network delay and N6 delay information by 5GC or AF

### 6.16.1 Key Issue mapping

This solution addresses Key Issue #2: Enhancement of EAS and local UPF (re)selection and proposes enhancements on Local UPF/DNAI and EAS (re)selection considering access network delay and N6 delay information.

### 6.16.2 Description

In Rel-18, QoS Monitoring for packet delay can be used to determine the access delay in 5GS. QoS Monitoring for packet delay can be applied based on AF request or PCF policy control or both (see clause 5.33.3 of TS 23.501 [2]). The measurement of the UL/DL packet delay between NG-RAN and PSA UPF can be performed on different levels of granularities, i.e. per QoS Flow per UE level, or per GTP-U path level, subject to the operators' configuration. The SMF can request to activate QoS monitoring for the GTP-U path(s) between all UPF(s) and the (R)AN based on locally configured policies (see clause 5.33.3.3 of TS 23.501 [2]).

**Case 1: 5GC performs N6 delay measurements**

Based on the need to select an appropriate UPF for traffic offloading or based on an AF request, the SMF may control an UPF for delay monitoring related with N6 delay between an UPF and one or more EAS(s). As part of AF request, AF may provide an assistance information such as protocol specific configuration parameters.

Based on AF request or OAM, 5GC/SMF can configure UPF(s) to perform measurements and report results for N6 delay information with the following parameters:

- the (list of) target EAS identified by their IP address or FQDN(s);

- measurement type i.e. N6 delay (between UPF and EAS(s)) or combined delay (from a UE to EAS);

- Application ID;

- Measurement protocol to be used to monitor N6 delay along with the protocol-specific configuration parameters based on AF-provided assistance information;

NOTE 1: In case more than one measurement protocol such as STAMP [RFC 8792], TWAMP [RFC 5357], ICMP and/or HTTP is supported by the UPF, a list of protocols in priority order can be provided.

NOTE 2: Protocol-specific configuration parameters may include port number of the remote N6 entity for the measurement protocol, measurement role such as session-sender for STAMP, operation mode, security information, etc.

- Reporting frequency and/or reporting threshold;

- Reporting target: notification URI.

When UPF receives an application ID, UPF performs N6 delay measurements when UPF detected usage of this application.

**Case 2: AF performs N6 delay measurements**

AF can request both access network delay and N6 delay related information from 5GC via NEF.

The access network delay and N6 delay related information include:

- requirements and/or reporting results for QoS monitoring packet delay in N3/N9 access network delay (as in clause 5.33.3 of TS 23.501 [2]);

- requirements and/or reporting results for QoS monitoring over N6 delay, which may include AF-provided assistance information that includes N6 measurement configuration information related to EAS(es) on the data network (measurement endpoint(s), protocol, keys, etc.). 5GS measurement endpoint(s) can use to perform N6 delay measurements based on the AF-provided assistance information; or

- 5GC N6 measurement assistance information including 5GC N6 interface related measurement configuration information (measurement endpoint address(es), protocol, keys, etc.), which the AF and/or N6 measurement endpoint(s) on the data network side can use to perform N6 delay measurements when 5GC reporting for N6 delay information is not required.

When AF provides a list of DNAI(s) and/or EAS IP address(es), it may include access network delay and N6 delay related information in Nnef\_TrafficInfluence\_Create/Update service operation. SMF can use Rel-18 QoS Monitoring for packet delays to obtain access network delay information for each DNAI(s) and either obtain measurement results over N6 delay information for each DNAI (as described in Figure 6.16.3-1) or provide 5GC N6 measurement assistance information to AF (as described in Figure 6.16.3-2), depending on the AF request.

For the case where AF performs measurements, when a measurement endpoint in (local) data network perform N6 measurements between one or more UPF(s) and EAS, UPF(s) can act in the measurement role of receiver/reflector endpoint. In this case, based on AF request or OAM/SLA, (authorized) 5GC/UPF configuration information for QoS monitoring over N6 can be provided to AF as a 5GC assistance information.

This solution is based on following principles:

- 5GC/SMF configures UPF to perform measurements and report results on N3/N9 and N6 delay information as described in Figure 6.16.3-1. This is the case 1 where UPF has a measurement role as the session-sender.

- Enhancement on Application Function influence on traffic routing procedure for AF to request/subscribe for each DNAI and/or EAS IP address(es):

- associated requirements and/or reporting results for QoS monitoring packet delay over N3/N9 access network which can be used in both case 1 and 2;

- for case 1, associated requirements and/or reporting results for QoS monitoring over N6 delay and/or associated N6 measurement configuration information related to EAS(es) on the data network for QoS monitoring over N6 delay or;

- for case 2, 5GC N6 measurement assistance information for QoS monitoring over N6 delay. This is the case where UPF has a measurement role as the receiver/reflector;

- Enhancement on exposure of User Plane Management Events (Early Notification) for SMF to provide EAS IP address(es), reporting results for QoS monitoring packet delay over N3/N9 access network (for case 1 and 2) and reporting results for QoS monitoring over N6 delay (for case 1), which can be the sum of the measured delays, or 5GC N6 measurement assistance information for QoS monitoring over N6 delay (for case 2), for each candidate DNAI(s).

- Enhancement on exposure of User Plane Management Events for AF to confirm/select the target DNAI based on above information provided by SMF or direct reporting by UPF(s).

NOTE: AF can additionally consider EAS load information available at compute-site level for DNAI/EAS selection transparently to 5GC.

**Case 3: SMF N6 delay measurements**

In the existing mechanism in Rel-18 5G system, the estimated user plane latency between the UE and the potential PSA-UPF is known to the SMF and the 5GC supports the AF influence to consider the user plane latency requirements requested by the AF. This enables SMF to select the PSA-UPF based on the AF requested requirements. However, user plane latency between the UE and the potential PSA UPF cannot represent the end-to-end delay between the EAS and the UE as it cannot include N6 delay (delay between the potential PSA UPF and EAS). To address this, it is proposed to provide enhancement of UPF selection considering N6 delay and AF request to include N6 delay requirement or end-to-end delay requirement.

### 6.16.3 Procedures

In case 1 (5GC performs N6 delay measurements), AF-provided assistance information that includes N6 measurement configuration information related to EAS(es) on the data network (measurement endpoint(s), protocol, keys, etc.) can be provided via EAS Deployment Information service or AF Traffic Influence service.

In case 2 (AF performs measurements), the need of 5GC-provided assistance information that includes 5GC N6 interface related measurement configuration information (measurement endpoint address(es), protocol, keys, etc.) can be provided via EAS Deployment Information service or AF Traffic Influence service.

**Case 1: 5GC performs N6 delay measurements**

Figure 6.16.3-1 shows the enhancement on Procedure for AF requests to influence traffic routing in order to include monitoring over N6. For this given procedure, 5GC/UPF performs measurement over N6.



Figure 6.16.3.1: Procedure on AF request on monitoring over access and data network delays where data network delay measurement is performed by 5GC/UPF

0. This call flow assumes that the UE has already established a PDU session.

1. AF creates a request for 5GC to monitor N3/N9 delays as well as N6 delay. As part of this request, AF may also include AF-provided assistance information for QoS monitoring over N6 as described as part of case 1 in clause 6.16.2.

2. The AF sends its request to the NEF. NEF performs necessary authorization control of the AF request, and, if necessary, maps the information provided by the AF.

3. The same step 3 as in Figure 4.3.6.2-1 of TS 23.502 [3] where additionally, storing/updating the information includes monitoring over N6 request as well as AF-provided assistance information for QoS monitoring over N6.

4. The same step 4 as in Figure 4.3.6.2-1 of TS 23.502 [3].

5. The same step 5 as in Figure 4.3.6.2-1 of TS 23.502 [3] where additionally, PCF provides QoS monitoring over N6 related rules to SMF.

6. SMF determines the impacted UPF(s) to perform QoS monitoring i.e. N6 delay measurements between the determined UPF(s) and the data network endpoints. SMF can make use of EAS IP address and DNAI mapping and determines the impacted UPF(s) according to the candidate DNAI(s) which are selected as described in 6.2.3.2.2 of TS 23.548 [5]. SMF optionally determines the protocol-specific configuration parameters based on the received AF-provided assistance information.

7. SMF provides N4 session rules that includes the configuration of QoS monitoring over N6 which includes all or part of the parameters listed in clause 6.16.2 as part of case 1.

8. UPF(s) performs QoS monitoring over N6 using the configuration sent by SMF.

9. UPF(s) reports QoS monitoring results to SMF.

10. SMF obtains QoS monitoring results and calculates the sum of the delays, i.e. the total delay including access network (N3/N9) and data network (N6) delays.

11. While constructing the list of candidate DNAIs/EASs, SMF takes into account either the sum of the delays or N6 delay monitoring results for each candidate DNAI/EAS.

12. The procedure defined for notification of user plane management event described in clause 4.3.6.3 of TS 23.502 [3] is followed. When SMF sends the notification, SMF includes the respective delay measurement result along with each candidate DNAI/EAS.

**Case 2: AF performs N6 delay measurements**

Figure 6.16.3-2 shows the enhancement on Procedure for AF requests to influence traffic routing in order to include monitoring over N6. For this given procedure, AF performs measurement over N6.



Figure 6.16.3.2: Procedure on AF request on monitoring over access and data network delays where data network delay measurement is performed by AF based on 5GC-provided assistance information

0. This call flow assumes that the UE has already established a PDU session.

1. AF creates a request for 5GC to monitor N3/N9 delays and to provide an assistance information. The AF uses the 5GC-provided assistance information as described as part of case 2 in clause 6.16.2 to perform N6 delay measurements.

2. The AF sends its request to the NEF. NEF performs necessary authorization control of the AF request, and, if necessary, maps the information provided by the AF.

3. The same step 3 as in Figure 4.3.6.2-1 of TS 23.502 [3] where additionally, storing/updating the information includes the requirement for 5G-provided assistance information for monitoring over N6.

4. The same step 4 as in Figure 4.3.6.2-1 of TS 23.502 [3].

5. The same step 5 as in Figure 4.3.6.2-1 of TS 23.502 [3] where additionally, PCF provides QoS monitoring over N3/N9 related rules to SMF along with the requirement for 5G-provided assistance information to be sent to AF.

6. SMF determines the impacted UPF(s) to perform QoS monitoring over N3/N9. SMF can make use of EAS IP address and DNAI mapping and determines the impacted UPF(s) according to the candidate DNAI(s) that are selected as described in 6.2.3.2.2 of TS 23.548 [5].

7. The SMF sends the request to the UPF(s) via N4 session establishment/update.

8. UPF reports QoS monitoring results to SMF.

9. SMF obtains QoS monitoring results and determines the list of candidate DNAI(s)/EAS(s).

10. The procedure defined for notification of user plane management event described in clause 4.3.6.3 of TS 23.502 [3] is followed where additionally, when SMF sends the notification, SMF includes the respective N3/N9 delay measurement and 5GC-provided assistance information to AF in order to AF to perform N6 delay measurements over each candidate DNAI/EAS.

11. AF performs N6 delay measurements based on the information provided by SMF. Then, AF performs EAS (re)selection. AF may additionally consider the EAS load information available at compute-site level when confirming/selecting the Target DNAI from the list of candidate DNAI(s)/EAS(s).

**Case 3 SMF performs UPF/EAS selection considering N6 delay**

The procedure is to address case 3 in clause 6.16.2 based on the existing procedure described in the clause 4.3.6.2 of TS 23.502 [x] with additional parameters sent via the AF request and its corresponding SMF behaviour.



Figure 6.16.3.3: AF request with N6 delay requirement and UPF/EAS selection (case 3)

1. The AF (e.g. EAS or EES) decides to sends AF traffic influence request. In addition to the input parameters described in TS 23.502 [3], clause 5.2.6.7, this request includes the user plane latency requirements. The user plane latency requirement may include the following information:

- N6 delay requirement: The value of this information is the delay between the potential PSA UPF and EAS. The SMF uses this value to ensure N6 delay between the PSA UPF and EAS. The SMF uses this value to perform UPF selection and further EAS selection. This value can be jointly provided with the existing user plane latency requirement.

- Minimum N6 delay preference indication: This indication denotes the preference of the AF for the shortest N6 delay. Based on this, t the SMF (re)selects the PSA UPF with the minimum N6 delay.

- End-to-end delay requirement: The value of this information is the delay between the UE and EAS. The SMF uses this value to ensure the delay between the PSA UPF and UE. The SMF uses this value to perform UPF selection and further EAS selection.

- Minimum End-to-end delay preference indication: This indication denotes the preference of the AF for the shortest end-to-end delay. Based on this, the SMF (re)selects the PSA UPF with the minimum end-to-end delay.

- Delay requirement class information: This information denotes either assured class or best effort class.

2-4. The steps 2-4 of Figure 4.3.6.2-1 in clause 5.2.6.7 of TS 23.502 [x] are performed.

5. In addition to the existing PCC rule information, the N6 delay requirement and/or end-to-end delay requirement is/are sent to the SMF.

6. When the PCC rule information is received from the PCF, the SMF may take appropriate actions to configure the user plane path of the PDU Session, including UPF selection considering the provided N6 delay requirement and/or end-to-end delay requirement.

7-8. The SMF configures the EASDF with the DNS handling rule. After that, when the UE sends the DNS query and the EASDF gets the corresponding DNS response including EAS IP address(es), the EASDF notifies the SMF with the EAS IP address(es).

9. If the notification from the EASDF contains a single EAS IP address, the SMF performs UPF selection for the EAS IP address considering the N6 delay requirement and/or end-to-end delay requirement received from the PCF in step 5. For this purpose, the SMF considers the measured/estimated N6 delay, if available (e.g., by utilizing the measurement at UPF or NWDAF-provided analytics as in clause 6.12.3.1).

If the notification from the EASDF contains multiple EAS IP addresses, the SMF jointly performs UPF selection and EAS selection considering the N6 delay requirement and/or end-to-end delay requirement received from the PCF in step 5. For this purpose, the SMF considers the measured/estimated N6 delay, if available (e.g., by utilizing the measurement at UPF or NWDAF-provided analytics as in clause 6.12.3.1).

### 6.16.4 Impacts on services, entities and interfaces

**Application Function (AF):**

- (for the case where 5GC performs measurements) provides requirements for reporting results for QoS monitoring over N6 delay.

- (for the case where 5GC performs measurements) provides assistance information related to data network endpoints for N6 delay measurement.

- (for the case where AF performs measurements) receives 5GC-provided assistance information on N6 delay measurement.

- (for the case where AF performs measurements) selects Target DNAI considering delay information (N3/N9 delay as well as N6 delay) and potentially locally available compute-site level EAS load information.

**Network Exposure Function (NEF):**

- may authorize AF provided requirements and configuration information for QoS monitoring over N6 delay

- (if necessary) maps the AF provided requirements and/or assistance information.

- (for case 3) exposes an API for AF to provide N6 delay requirement or end-to-end delay requirement, and optionally its related information (minimum delay preference and Delay requirement class).

**Session Management Function (SMF):**

- (for the case where 5GC performs measurements) determines UPF(s) to perform QoS monitoring over N6 (e.g. N6 delay measurements) and optionally determines the protocol-specific configuration parameters.

- (for the case where 5GC performs measurements) configures UPF(s) to perform QoS monitoring over N6 (e.g. N6 delay measurements).

- (for the case where 5GC performs measurements) receives reports on QoS monitoring over N6 from UPF.

- (for the case where 5GC performs measurements, optionally) calculates the sum of the measured delay of N3/N9 delay (between the UE and PSA UPF) and N6 delay (between the PSA UPF and EAS/DN).

- (for the case where AF performs measurements) provides 5GC-assistance information on N6 delay measurements to AF.

- (for case 3) performs UPF (re)selection considering N6 delay requirement or end-to-end delay requirement.

- (for case 3) performs EAS (re)selection considering N6 delay requirement or end-to-end delay requirement.

**Policy Control Function (PCF):**

- (for the case where AF performs measurements) provides the rule to SMF regarding 5GC-provided assistance information to be sent to AF.

- (for the case 3 where AF provides requirements for delay) creates and provides the SMF with the PCC including N6 delay requirement or end-to-end delay requirement, and its related information (minimum delay preference and Delay requirement class).

**User Plane Function (UPF):**

- receives measurement parameters/configuration from SMF on QoS monitoring over N6.

- (for the case where 5GC performs measurements) QoS monitoring over N6 (e.g. N6 delay measurements).

- (for the case where 5GC performs measurements) includes QoS monitoring over N6 (e.g. N6 delay measurement) results to QoS monitoring report.

- (if authorized for the case where AF performs measurements) responds to AF delay measurement messages.

## 6.17 Solution #17: EC Traffic Routing between local part of DN and central part of DN with IP replacement in EAS

### 6.17.1 Key Issue mapping

This solution addresses following aspects of KI#3:

- How to determine and route the application traffic between the EAS in the local part of DN and the Application Server in the central part of DN for both UL and DL in case there is no direct connectivity between the local DN and central part of DN.

- How is the 5GC aware of the application traffic is required to be processed at different locations? and by what order? including how to distinguish the UL/DL traffic traversing through the PSA.

- How to guarantee the QoS when the traffic transmission between local and central parts of DN.

- Whether and what information is required to be provided to make the final destination (e.g. UE, server in central part of DN) be aware of the traffic being processed by Edge Hosting Environment.

### 6.17.2 Description

Per current 5G system design, the UL CL (Uplink Classifier) User Plane Function (UPF) decides whether to route uplink traffic to local PDU Session Anchor (PSA) UPF based on the Destination IP address and/or Port number of the uplink traffic from the Next Generation Radio Access Network (NG-RAN) node based on the routing rule which is configured in the UL CL UPF by the Session Management Function (SMF). Then after being processed by the local EAS, the traffic is sent back to UE via UL CL UPF. The UL CL UPF today forwards all the traffic arriving from the local PSA UPF towards the NG-RAN node transparently.

In contrast, according to the scope of the Rel-19 study on Edge enhancements, the traffic injected by the Local EAS into the UL CL UPF could go either to the UE (as in Rel-18 specifications) or could be forwarded towards an AS in a central location for further processing.



Figure 6.17.2-1: Application traffic processing in UL/DL CL and local EAS

**UL:**

- Packet from UE to local EAS: the Destination IP address is either the IP address of central AS or the IP address of local EAS, the Source IP address is the UE IP address.

- Packet from local EAS to UL/DL CL: the Destination IP address is the central AS IP address, the Source IP address is the UE IP address.

**DL:**

- Packet from UL/DL CL to local EAS: the Destination IP address is the UE IP address, the Source IP address is the central AS IP address.

- Packet from local EAS to UE: the Destination IP address is the UE IP address, the Source IP address is either the central AS IP address or local EAS IP address.

**Assumption of traffic processing by EAS:**

- For the IP packets sent by the local EAS towards the central AS via UL CL, the Source IP address is the UE IP address, the Destination IP address is the IP address of central AS. If the Destination IP address of the uplink traffic from UE is the IP address of the local EAS, destination IP address replacement happens at EAS. If the Destination IP address of the uplink traffic from UE is the IP address of central AS, the EAS doesn't need to do destination IP address replacement.

- For the IP packets sent by the local EAS towards the UE, the Source IP address is the same as the Destination IP address (i.e. IP address of central AS or local EAS) of the uplink traffic received from the UE. If the Destination IP address of the uplink traffic from UE is the IP address of the local EAS, source IP address replacement happens at EAS. If the Destination IP address of the uplink traffic from UE is the IP address of central AS, the EAS doesn't need to do source IP address replacement.

To support this new requirement from the Rel-19 study, the following enhancement to UL CL UPF is required:

- The UL CL becomes Uplink/Downlink Classifier (UL/DL CL) because it needs to inspect both uplink and downlink traffic, as well as traffic injected by the local EAS. The SMF configures the UL/DL CL UPF with packet filters not only for uplink traffic arriving from the UE side, but also for traffic arriving from the EAS side, as well as for the downlink traffic arriving via the central PSA UPF.

- Supporting enhanced traffic routing rule:

- For the traffic received at the UL/DL CL UPF from the local PSA UPF:

a) If the Destination IP address and/or port number matches the UE's IP address as indicated in the traffic routing rule configured in UL/DL CL UPF, the traffic is forwarded to UE via the NG-RAN node.

b) If the Destination IP address and/or port number matches the central AS's IP address as indicated in the traffic routing rule configured in UL/DL CL UPF, the traffic is routed to the central AS. The Source IP address in the forwarded packets identifies the UE-specific User Plane tunnel between the UL/DL CL and the PSA UPF on which the packets are forwarded towards the PSA UPF. If the UL/DL CL UPF cannot identify a UE based on the Source IP address in the traffic received from the local PSA UPF or local EAS, the traffic is discarded.

- For the downlink traffic received from the PSA UPF, if the Source IP address and/or port number matches the IP address of the central AS as indicated in the traffic routing rule configured in the UL/DL CL UPF, the traffic is routed towards the local EAS over the User Plane tunnel towards the local PSA UPF.

By using the UE's User Plane tunnel for traffic routing, the QoS applied to the corresponding PDU Session can guarantee the QoS aspect of traffic being routed between local part of DN and central part of DN.

NOTE: For the traffic forwarded to local EAS, if the Destination IP address of the packet is a central AS IP address and the traffic is encrypted, local EAS may not be able to process the traffic and will send the encrypted traffic back to UL CL, then the UL CL sends the traffic to central AS over PSA UPF.

### 6.17.3 Procedures

During the currently defined AF influence or UL CL addition procedure, the enhanced traffic routing rule may have been configured in UL CL by SMF. Below figure shows an example procedure of AF triggered routing rule configuration or update procedure.



Figure 6.17.3-1: Example procedure for supporting traffic routing between local DN and central DN

0. UE establish a PDU Session as described in clause 4.3.2.2.1 of TS 23.502 [3].

1. The SMF configures ULCL, L-PSA to perform local traffic routing based on existing AF influence or Addition of UL CL procedure.

2. User plane data from UE are routed to EAS via ULCL/BP and L-PSA.

3. The AF sends a request to PCF (optionally via NEF) to configure a traffic routing path between local DN and central DN. The AF request includes UE IP address as target UE, DNAI of the EAS, QoS requirement and related filter of the traffic to be routed between local DN and central DN (e.g. EAS IP/port number, central AS IP/port number). The DNAI of the EAS is used to indicate the traffic is routed via which L-PSA.

NOTE: Step 3 can be executed before UE sends out the data packet, i.e. Step 2.

4. The PCF generates PCC rule for traffic routing between local DN and central DN based on AF request. The PCF sends the PCC rule to SMF.

5. The SMF configures the traffic routing rule in ULCL/BP to detect and forward traffic between local DN and central DN as follows:

- For the traffic received at the UL/DL CL UPF from the local PSA UPF:

- If the Destination IP address and/or port number matches the UE's IP address as indicated in the traffic routing rule configured in UL/DL CL UPF, the traffic is forwarded to UE via the NG-RAN node.

- If the Destination IP address and/or port number matches the central AS's IP address as indicated in the traffic routing rule configured in UL/DL CL UPF, the traffic is routed to the central AS. The Source IP address in the forwarded packets identifies the UE-specific User Plane tunnel between the UL/DL CL and the PSA UPF on which the packets are forwarded towards the PSA UPF. If the UL/DL CL UPF cannot identify a UE based on the Source IP address in the traffic received from the local PSA UPF or local EAS, the traffic is discarded.

- For the downlink traffic received from the PSA UPF, if the Source IP address and/or port number matches the IP address of the central AS, as indicated in the traffic routing rule configured in the UL/DL CL UPF, the traffic is routed towards the local EAS over the User Plane tunnel towards the local PSA UPF.

6. The SMF indicates to AF the traffic routing path between L-DN and central DN has been configured, possibly via PCF and/or NEF.

7. Traffic from L-DN (i.e. after processed by EAS) is sent to central DN via L-PSA, ULCL/BP and PSA.

8. Traffic from central DN (i.e. after processed by cloud server) sent to L-DN via PSA, ULCL/BP and L-PSA.

9. Traffic sent from EAS to UE.

### 6.17.4 Impacts on services, entities and interfaces

**Impact to UL CL UPF:**

- The UL CL becomes Uplink/Downlink Classifier (UL/DL CL) because it needs to inspect both uplink and downlink traffic, as well as traffic injected by the local EAS. The SMF configures the UL/DL CL UPF with packet filters not only for uplink traffic arriving from the UE side, but also for traffic arriving from the EAS side, as well as for the downlink traffic arriving via the central PSA UPF.

- Supporting enhanced traffic routing rule:

- For the traffic received at the UL/DL CL UPF from the local PSA UPF or local EAS:

a) If the Destination IP address and/or port number matches the UE's IP address as indicated in the traffic routing rule configured in UL/DL CL UPF, the traffic is forwarded to UE via the NG-RAN node.

b) If the Destination IP address and/or port number matches the central AS's IP address as indicated in the traffic routing rule configured in UL/DL CL UPF, the traffic is routed to the central AS. The Source IP address in the forwarded packets identifies the UE-specific User Plane tunnel between the UL/DL CL and the PSA UPF on which the packets are forwarded towards the PSA UPF. If the UL/DL CL UPF cannot identify a UE based on the Source IP address in the traffic received from the local PSA UPF or local EAS, the traffic is discarded.

- For the downlink traffic received from the PSA UPF, if the Source IP address and/or port number matches the IP address of the central AS as indicated in the traffic routing rule configured in the UL/DL CL UPF, the traffic is routed towards the local EAS over the User Plane tunnel towards the local PSA UPF.

## 6.18 Solution 18: Supporting traffic routing between local DN and central DN within a PDU Session

### 6.18.1 Description

This solution resolves KI#3 about traffic routing between L-DN and central DN based on the scenario that the application traffic is required to be processed at different locations. The following aspects are included:

1) UL/DL traffic handling

For the UL traffic, after receiving traffic from the UE, the traffic is routed to EAS to be processed firstly. Then EAS generates its own traffic and send it to the cloud server, i.e. the AS located at central DN. For the DL traffic, the cloud server generates its own traffic and send it back to the EAS and UE. Thus, in details, the traffic will have following characteristics:

- The traffic between local DN and central DN is preferred to be sent within the PDU session (i.e. via a QoS Flow) to guarantee the related QoS requirement.

- UL: Packets sent by UE have UE IP as source IP address and EAS IP as target IP address.

- UL: The traffic after processed by EAS have EAS IP as source IP address and AS (cloud server) IP as target IP address. However, when the UL traffic sent from PSA to cloud server, the network needs to change the source IP address to an IP address assigned by PSA as source IP address. This is to ensure the DL traffic sent back from cloud server can be routed to PSA. The L-PSA detects the traffic is corresponding to the PDU session based on the IP 5-tuple of the traffic indicated by SMF in the PDR.

- DL: The traffic after processed by cloud server have AS IP as source IP address and the received UL packet source IP address as target IP address, i.e. the IP address assigned by PSA, when the DL traffic sent from L-PSA to EAS, PSA (or L-PSA) need change the target IP address to the EAS IP address. The PSA detects the traffic is corresponding to the PDU session based on the IP 5-tuple of the traffic indicated by SMF in the PDR.

- DL: The traffic after processed by EAS have EAS IP as source IP address and UE IP as target IP address.

- DL: UE does not need to be aware whether the traffic has been processed by EHE.

NOTE 1: It is assumed that a tunnel is configured between the L-PSA and EAS.

NOTE 2: It is assumed that the EAS and/or AS will use a unique port number to generate traffic between EAS and AS for a specific traffic from UE identified by a UE address. Then the source or target port numbers in the IP 5-tuple as described above can be used by 5GC to differentiate traffics belong to multiple PDU Sessions.

2) Enable traffic routing between local part of DN and central part of DN

To enable the traffic routing via the tunnel of PDU session, the AF provides the following information:

- Traffic routing enable indicator which indicates the corresponding traffic requires traffic routing between local part of DN and central part of DN;

- Traffic flow description for UL and/or DL (e.g. IP 5 tuples) as described in clause 5.6.7 of TS 23.501 [2].

The IP 5-tuple is corresponding to the traffic sent by UE to EAS and need be routed between local DN and central DN (e.g. EAS IP, AS IP).

- Target UE Identifier

- QoS requirement of the indicated traffic flow

### 6.18.2 Procedures



Figure 6.18.2-1: Procedure for supporting traffic routing between local DN and central DN

0. UE establish a PDU Session as described in clause 4.3.2.2.1 of TS 23.502 [3]. For the UP path of the PDU Session, two scenarios are described as following:

- The PDU Session accesses the local part of DN, e.g. for Distributed Anchor model.

- The PDU Session accesses the central part of DN, e.g. for Session Breakout model before UL CL/BP inserted.

1. After EAS discovery as described in clause 6.2 of TS 23.548 [5], UE send traffic to EAS. User plane data from UE are routed to EAS via ULCL/BP and L-UPF for Session Breakout model. The SMF configures ULCL/BP, L-PSA to perform local traffic routing.

User plane data from UE are routed to EAS via ULCL/BP and L-PSA for Session Breakout model.

User plane data from UE are routed to EAS via L-PSA for Distributed Anchor model.

2. The AF sends a request to PCF (optionally via NEF) by invoking Npcf\_PolicyAuthorization service to configure a traffic routing path between local DN and central DN. The AF request includes Traffic routing enable indicator, UE IP address as target UE, QoS requirement and related IP 5-tuple of the traffic to be routed between local DN and central DN (e.g. EAS IP, cloud server IP).

3. The PCF generates PCC rule for traffic routing between local DN and central DN based on AF request. The PCF sends the PCC rule to SMF.

4. For Distributed Anchor model, the SMF selects and inserts a central UPF and UL CL/BP for the traffic routing between local DN and central DN via the PDU Session.

4. The SMF requests the PSA to allocate an IP address, which is used to replace the EAS IP address when the UL packet sent to cloud server. The allocated IP address is different comparing to the IP address allocated to the PDU session. The IP replacement can be done by either by PSA (step 6) or L-PSA (step 7). If the IP replacement is executed at the L-PSA, the allocated IP address also need be notified to L-PSA.

NOTE 1: Using a new allocated IP address rather than UE IP address is to differentiate the traffic from EAS to cloud server and the traffic from UE to cloud server, i.e. the traffic to UE and traffic to EAS can be transmitted simultaneously.

6. To support the DL traffic from cloud server to EAS:

- The SMF configures the N4 rule on PSA to guarantee QoS based on dynamic or preconfigured policy (e.g. bind to a new QoS flow or an existing QoS flow as described in clause 6.1.3.2.4 of TS 23.503 [4]).

If PSA performs IP replacement, the SMF configures the PSA to perform IP replacement:

- For UL traffic from EAS to cloud server, the source IP address (i.e. EAS IP address) is replaced with an IP address allocated by PSA.

- For DL traffic from cloud server to EAS, the target IP address is replaced back with the EAS IP address.

7. To support the UL traffic from EAS to cloud server:

- The SMF configures the N4 rule on L-PSA to guarantee QoS based on dynamic or preconfigured policy (e.g. bind to a new QoS flow or an existing QoS flow as described in clause 6.1.3.2.4 of TS 23.503 [4]).

If L-PSA performs IP replacement, the SMF configures the L-PSA to perform IP replacement:

- For traffic from EAS to cloud server, the source IP address (i.e. EAS IP address) is replaced with an IP address assigned by PSA in step 5.

- For traffic from cloud server to EAS, the target IP address is replaced back with the EAS IP address.

8. The SMF configures the traffic routing rule in ULCL/BP to detect and forward traffic between local DN and central DN as follows:

- For UL traffic from EAS to cloud server, forward to PSA. This can be done per traffic target address to differentiate, i.e. the target IP address is UE IP address or cloud server IP address.

- For DL traffic from cloud server to EAS, forward to L-PSA. This can be done per traffic target address to differentiate, i.e. the target IP address is UE IP address, or EAS IP address when PSA performs IP replacement, or IP address assigned by PSA when L-PSA performs IP replacement.

9. The SMF indicates to AF the traffic routing path between L-DN and central DN has been configured, possibly via PCF and/or NEF.

10. Traffic from L-DN (i.e. after processed by EAS) is sent to central DN via L-PSA, ULCL/BP and PSA.

11. Traffic from central DN (i.e. after processed by cloud server) sent to L-DN via PSA, ULCL/BP and L-PSA.

12. Traffic sent from EAS to UE.

NOTE 2: All the traffic is within the PDU Session, thus operators can identify it with SDF template in a PCC rule and apply appropriate charging key and charging method (e.g. neither of online or offline charging) as described in clause 6.6 of TS 23.503 [4]. There can also be Sponsor Identifier if it is charging for 3rd party as described in clause 6.6 of TS 23.503 [4].

### 6.18.3 Impacts on services, entities and interfaces

**SMF:**

- For Distributed Anchor model, the SMF may insert a central UPF and UL CL/BP for the PDU Session.

- Generate traffic routing rule as described above.

**UPF:**

- Detect traffic between local DN and central DN and route the traffic to L-PSA or PSA.

- Perform IP replacement of the source IP address for UL traffic and target IP address for DL traffic.

**AF:**

- Inform 5GC to configure the traffic between local DN and central DN.

## 6.19 Solution #19: Traffic Routing between local DN and central DN over session breakout model

### 6.19.1 Key Issue mapping

This solution is proposed to address Key Issue #3: EC Traffic Routing between local part of DN and central part of DN.

### 6.19.2 Description

As proposed in key issue, the following two cases should be considered to support EC Traffic Routing between local part of DN and central part of DN:

- UL traffic related to an application first routed over EC to Application Server(s) for local-processing, and then further forwarded to a remote Application Server(s) in central part of DN.

- DL traffic related to an application first routed over central part of DN for processing, then forwarded to Application Server(s) in local EC for local-processing, and finally provided to the UE.

To guarantee the policy and charging control from end to end, the solution proposes to reuse the Session breakout model as described in TS 23.548 [5] to build a single PDU Session with multiple PDU Session Anchor(s) (UL CL / IP v6 multi-homing) and further support traffic routing between local DN and central DN on the basis of enabling Edge Computing.

In this solution, the UE IP address is always kept as source IP or destination IP in each data packet to make sure UPF can correlate the traffic into the same PDU session. The EAS and AS use different IP address for the traffic going through two DNs and the normal traffic to distinguish these two kinds of traffic and the AF will notify the 5GC about this information. The detail replacement is shown as below:



Figure 6.19.2-1: Traffic Routing among UE and Local DN and Central DN

In the case of UL, as shown in Figure 6.19.2-1, the traffic from UE to local DN and the traffic from local DN to central DN should be delivered via the same PDU session, namely, SDF1 and SDF2 are required to be correlated to the same PDU session serving the UE. According to existing mechanism, SDF1(SA: UE IP, DA: EAS IP) is able to be correlates to the PDU Session and route to the local DN without any other enhancement. For SDF2, this solution proposes to perform IP replacement at UL CL/BP UPF and the SDF2-1(SA: EAS IP1, DA: UE IP) will be changed to SDF2-2 (SA: UE IP, DA: AS IP). The EAS IP 1 is allocated by the EAS and will be provided to 5GC by AF influence mechanism as described in clause 6.19.3. The local PSA distinguishes the data packets of SDF2-1 by traffic description and correlates these data packets to the PDU session by UE IP address, after that, the data packets can be routed towards ULCL or BP UPF based on current mechanism. When the ULCL or BP UPF receive the data packets of SDF2-1, the ULCL or BP UPF replaces the source IP address from the IP address of local EC application server to the UE IP address and replaces the destination IP address from the UE IP address to the IP address of central application server, so that the packets of SDF2-2 are able to be further forwarded to the central DN via the PDU Session.

In the case of DL, similar principle applies. As shown in Figure 6.19.2-1, traffic distinguishing and routing of SDF4 can be regards as usual case which is able to be satisfied by existing mechanism. For SDF3, similar as UL case, IP replacement can be performed at UL CL/BP UPF and the SDF3-1(SA: AS IP1, DA: UE IP) will be changed to SDF3-2 (SA: UE IP, DA: EAS IP). the central PSA distinguishes the data packets of SDF3-1 by traffic description and correlates these data packets to the PDU session by UE IP, and then, it forwards these data packets to ULCL or BP UPF. When the ULCL or BP UPF receive the data packets of SDF3-1, the ULCL or BP UPF replaces the source IP address from the AS IP address 1to the UE IP address and replaces the destination IP address from the UE address to the IP address of EC application server, so that the packets of SDF3-1 are able to be further forwarded to the local DN via the PDU Session.

The traffic routing rule configured at ULCL/BP is shown in Table 6.19.2-1.

Table 6.19.2-1 Traffic routing rule configured at ULCL/BP

|  |  |  |
| --- | --- | --- |
| Options | Traffic from L-PSA | Traffic from C-PSA |
| **UL CL/BP perform IP replacement** | Target IP is UE IP address: Route to UE (RAN).  Others:  Route to PSA. | Target IP is UE IP address: Route to UE (RAN).  Others:  Route to L-PSA. |

NOTE 1: It is required to have UE IP NAT address to make sure the traffic can be routed to its corresponding PSA.

NOTE 2: It is assumed that after the traffic being processed by local EAS, the UE IP address is NATed back to the same private UE IP address as the source IP address of the traffic before being processed.

On the other hand, this solution reuses the Application Function influence on traffic routing mechanism as described in TS 23.501 [2] to indicate which traffic should be influenced and by what order of the function should be routed, and the PCF might generate the PCC rules providing to SMF for building or updating suitable PDU session. The AF re

quest contains the traffic description (e.g. application identifier), potential prior-processing locations of applications and potential post-processing locations of applications which are used to indicate the function order to be routed, e.g. a list of local DNAI(s), a list of central DNAI(s). The detail procedures are described in clause 6.19.3.

### 6.19.3 Procedures

Figure 6.19.3-1 illustrates the procedure for AF influence on traffic routing between local DN and central DN.



Figure 6.19.3-1: AF influence on traffic routing between local DN and central DN

1. The AF sends the request to NEF by invoking Nnef\_TrafficInfluence\_Update service. The AF request contains the traffic description (identifies the application traffic to be processed in both of local DN and central DN), potential prior-processing locations of applications (indicates the first location that application traffic is required to be routed for initial processing), potential post-processing locations of applications (indicates the later location that application traffic is required to be routed for further processing), Target UE Identifier(s), AF transaction identifier and other necessary parameters as described in Table 5.6.7-1 of TS 23.501 [2].

2. The PCF creates or updates PCC rules based on the AF request . For influenced PDU Sessions, the PCF may create or update the PCC rule information including service data flow template, data network access identifier for prior-processing, data network access identifier for post-processing, per DNAI: Traffic steering policy identifier and other necessary parameters as described in Table 6.3.1 of TS 23.503 [4].

The PCF sends the new policy to SMF by invoking Npcf\_SMPolicyControl\_UpdateNotify service.

3. The SMF may take appropriate actions to reconfigure the user plane of the PDU Session. The actions may include:

- Reselect UL CL or BP UPF which has the capability of replacing the IP address of data packets.

- Reselect PSA which has the capability of correlating the SDF with the single PDU Session (to the local DN and the central DN in order).

- Creates or updates PDR and FAR and sends the PDR and FAR to related UPF(s).

4. The PSA identifies the SDF(s) by traffic description and correlates them with the single PDU session for traffic routing. The UL CL/BP UPF performs IP address replacement for the data packets of the identified SDF(s) and forwards the data packets to next destination.

### 6.19.4 Impacts on services, entities and interfaces

**AF:**

- AF request enhancement to contain potential post-processing locations of applications and potential prior-processing locations of applications.

**PCF:**

- PCC policy enhancement to contain DNAI(s) for prior-processing and DNAI(s) for post-processing.

**SMF:**

- creates a single PDU Session to local DN and central DN, and supporting the traffic routing between local DN and central DN.

**UPF:**

- Correlates data packets with the given PDU session.

- Replaces the IP address of the data packets for the given data traffic.

## 6.20 Solution #20: EC Traffic Routing between local part of DN and central part of DN via PDU session

### 6.20.1 Key Issue mapping

The following solution corresponds to the key issue #3 on EC Traffic Routing between local part of DN and central part of DN.

### 6.20.2 Description

This solution is applicable for both Session Breakout Connection Model and Distributed Anchor Point Model.

As described in clause 5.3, the UL traffic is first routed over EC to Application Server(s) for local-processing, and then further forwarded to a central AS(s), and the DL traffic is first routed over central part of DN for processing, then forwarded to AS(s) in local EC for local-processing, and finally provided to the UE. To support such scenario, the following aspects are included:

- The AF requests the order of traffic routing, which indicates if application identifier or traffic filtering information (e.g. IP 5 Tuple) is matched, then first routing the UL/DL traffic to the specific IP address (i.e. EAS IP address).

- Based on the PCC rule or local policy, the SMF configures the UPF (i.e. UL CL/BP, PSA UPF) with traffic filters to enable traffic routing between local part of DN and central part of DN.

- In case of session breakout connectivity model, the UL CL/BP UPF Encapsulates in the IP header with the EAS IP address and sends the packets to the EAS via local PSA.

- In case of distributed anchor connectivity model, the central PSA reports the event to SMF (if the application identifier or IP 5 Tuple is matched and/or the PDU session tunnel can't be mapped), then the SMF establishes the forwarding tunnels for transferring packets from central PSA to local PSA based on the event report from central PSA.

- The EAS processes packets and sends the packets using the original destination address (e.g. UE IP, central AS IP).

For the UL traffic:

- The packets sent by UE use the UE IP as source address and the central AS IP or EAS IP as destination address.

- When the packets received by UL CL/BP UPF, if the destination address is central AS IP, then UL CL/BP UPF uses the EAS IP as the destination address by IP replacement and routes to the local EAS.

- The local EAS replaces the destination address by central AS IP address (i.e. uses the UE IP address as the source address and the central AS IP address as the destination address).- The UL CL/BP UPF sends the packets to central AS based on the destination address (central AS IP address).

For the DL traffic:

- The packets sent by central AS use the central AS IP as source address and the UE IP as destination address.

- When the packets received by UL CL/BP UPF, the UL CL/BP UPF uses the EAS IP as the destination address by IP replacement and routes to the local EAS (The original destination address is UE IP address, and this address is kept in the packet send to EAS).

- The local EAS replaces the destination address by UE IP address (i.e. uses the central AS IP address as the source address and the UE IP address as the destination address).

- The UL CL/BP UPF sends the packets to UE based on the destination address (UE IP address).

### 6.20.3 Procedures

#### 6.20.3.1 EC traffic Routing for UL traffic



Figure 6.20.3.1-1: EC traffic routing for UL traffic

1. [Optional] The AF request in step 1 in Figure 4.3.6.2-1 of TS 23.502 [3] is used to request the traffic routing between local part of DN and central part of DN. The AF request may include order of traffic routing (e.g. indicates the specific IP address for first routing for uplink traffic), application identifier or traffic filtering information (e.g. IP 5 Tuple), which indicates if application identifier or traffic filtering information (e.g. IP 5 Tuple) is matched, then first routing the uplink traffic to the specific IP address (i.e. EAS IP address).

In step 5 in figure 4.3.6.2-1 of TS 23.502 [3], the PCF creates PCC rule with order of traffic routing traffic, application identifier or traffic filtering information (e.g. IP 5 Tuple).

2. Based on local policy and/or PCC rule received from PCF in step 1, the SMF configures the UPF (i.e. UL CL/BP, PSA UPF) with traffic filters correspondingly.

2a. (In case of session breakout connectivity model) SMF configures UL CL/BP UPF and local PSA with PDR and FAR. If the application identifier or IP 5 Tuple is matched (e.g. for UL CL case, the destination IP address or destination port number is matched with the central AS IP address/port number or EAS IP address /port number, and for BP case, IP prefix@central PSA is matched), the UL CL/BP UPF should forward the traffic to the EAS (i.e. using the IP address indicated in "order of traffic routing" of step 1) via local PSA. If the destination address is central AS IP address, then local PSA forwards the traffic from EAS to the UL CL/BP UPF.

2b. (In case of distributed anchor connectivity model) SMF configures central PSA with event reporting. If the application identifier or IP 5 Tuple is matched (e.g. source address (UE IP address) is matched) and/or the packets can't be routed to the destination (i.e. local EAS), then central PSA reports the event to SMF.

3. UE sends UL traffic, and the destination is central AS IP address or IP prefix @ central PSA, or local EAS IP address or IP prefix @ local PSA.

3a. (In case of session breakout connectivity model) The UL CL/BP UPF receives the UL packets and determines to forward the traffic to the EAS via local PSA based on configured PDR and FAR. If the destination address is central IP address or IP prefix @ central PSA, UL CL UPF enforces the "Outer Header Creation" to replace the destination address by EAS IP address and sends the packets to EAS via local PSA. If the destination address is local EAS IP address or IP prefix @ local PSA, the UL CL/BP UPF sends the packets to the EAS via local PSA directly.

3b. (In case of distributed anchor connectivity model) The central PSA receives the UL packets and reports event to the SMF. The SMF determines the UL packets need to be forwarded to EAS firstly. Based on the EAS IP address, the SMF determines the DNAI (e.g. based on IP address range(s) per DNAI included in the EAS Deployment Information) and selects the local PSA UPF per DNAI. Then SMF establishes the BP or UL CL for the PDU Session, and indicates to establish the forwarding tunnels for transferring packets from central PSA to local PSA using the procedure described in steps 3 to 8 in Figure 4.3.5.4-1 of TS 23.502 [3].

4. The EAS receives and processes packets. The EAS determines the original destination is central AS, and then sends the processed packets back to UL CL/BP via local PSA. The EAS keeps UE IP address as source IP address and removes the Outer Header to revert the central AS IP address as destination IP address.

5. The UL CL BP UPF sends the traffic to the central PSA based on the destination address (IP address of central AS).

#### 6.20.3.2 EC Traffic Routing for DL traffic



Figure 6.20.3.2-1: EC traffic routing for DL traffic

1. [Optional] The AF request in step 1 in Figure 4.3.6.2-1 of TS 23.502 [3] is used to request the traffic routing between local part of DN and central part of DN. The AF request may include order of traffic routing (e.g. indicates the specific IP address for first routing for downlink traffic), application identifier or traffic filtering information (e.g. IP 5 Tuple), which indicates if application identifier or traffic filtering information (e.g. IP 5 Tuple) is matched, then first routing the downlink traffic to the specific IP address (i.e. EAS IP address).

In step 5 in Figure 4.3.6.2-1 of TS 23.502 [3], the PCF creates PCC rule with order of traffic routing traffic, application identifier or traffic filtering information (e.g. IP 5 Tuple).

2. Based on local policy and/or PCC rule received from PCF in step 1, the SMF configures the UPF (i.e. UL CL/BP, PSA UPF) with traffic filters correspondingly.

2a. (In case of session breakout connectivity model) SMF configures UL CL/BP UPF and local PSA with PDR and FAR. If the application identifier or IP 5 Tuple is matched (e.g. for UL CL case, the destination IP address or destination port number is matched with UE IP address or port number, and for BP case, IP prefix@local PSA is matched), the UL CL/BP UPF should forward the traffic to the EAS (i.e. using the IP address indicated in "order of traffic routing" of step 1) via local PSA. If the destination address is UE IP address, then local PSA forwards the traffic from central AS to the UL CL/BP UPF.

2b. (In case of distributed anchor connectivity model) SMF configures central PSA with event reporting. If the application identifier or IP 5 Tuple is matched (e.g. destination address (UE IP address) is matched) and/or the packets can't be routed to the destination (i.e. local EAS), then central report the event to SMF.

3. The Central AS sends DL traffic, and the destination is UE IP address or IP prefix @ local PSA.

3a. (In case of session breakout connectivity model) The UL CL/BP UPF receives the DL packets and determines to forward the traffic to the EAS via local PSA based on configured PDR and FAR. The UL CL/BP UPF enforces the "Outer Header Creation" to replace the destination address by EAS IP address and sends the packets to the EAS via local PSA.

3b. (In case of distributed anchor connectivity model) The central PSA receives the DL packets and reports event to the SMF. The SMF determines the DL packets need to be forwarded to EAS firstly. Based on the EAS IP address, the SMF determines the DNAI (e.g. based on IP address range(s) per DNAI included in the EAS Deployment Information) and selects the local PSA UPF per DNAI. Then SMF establishes the BP or UL CL for the PDU Session, and establishes the forwarding tunnels for transferring packets from central PSA to local PSA using the procedure described in steps 3 to 5 in figure 4.3.5.4-1 of TS 23.502 [3].

4. The EAS receives and processes packets. The EAS removes the Outer Header and determines the original destination is UE IP address, and then sends the processed packets back to UL CL/BP via local PSA using the original destination address (UE IP address).

5. The UL CL BP UPF sends the traffic to the UE based on the destination address (UE IP address).

### 6.20.4 Impacts on services, entities and interfaces

**AF:**

- Requests the order of traffic routing and indicates if application identifier or traffic filtering information (e.g. IP 5 Tuple) is matched, then first routing the UL/DL traffic to the specific IP address (i.e. EAS IP address).

**SMF:**

- SMF configures the UPF (i.e. UL CL/BP, PSA UPF) with traffic filters to enable traffic routing between local part of DN and central part of DN.

- Receives event report from UPF and determines to establish the BP or UL CL for the PDU Session, and establishes the forwarding tunnels for transferring packets from central PSA to local PSA based on the event report from central PSA.

**UL CL/BP:**

- Enforces the "Outer Header Creation" to replace the destination address by EAS IP address and sends the packets to the EAS via local PSA.

**Central PSA:**

- Reports the event to SMF, if the application identifier or IP 5 Tuple is matched (e.g. source address (UE IP address) is matched) and/or the PDU session tunnel can't be mapped.

## 6.21 Solution #21: Solution to traffic routing between local and central part of DN via tunnel(s)

### 6.21.1 Description

#### 6.21.1.1 Overall architecture of the solution

The architecture provides connectivity between the local and central parts of the DN ("L-DN" and "C-DN" as depicted in Figure 6.21.1-1), so that traffic can be exchanged between different parts of the DN e.g. between a L-DN part and the C-DN part. This allows EASs in different parts of a DN to communicate with each other.



Figure 6.21.1-1: Connectivity between the local and central parts of the DN

NOTE 1: In the above figure, even though a single Local PSA UPF (L-PSA UPF) interfacing a DN part has been represented, the L-PSA UPF terminating the PDU Session may be different from the L-PSA UPF allowing to interface the L-DN part with other parts of the DN.

This solution proposes to establish below two data paths:

1 a data path per PDU session between the UE and a L-PSA UPF interfacing the L-DN part.

2. a tunnel between the two parts of the DN (i.e. a L-DN part and a C-DN part in Figure 6.21.1-1).

The tunnel between L-PSA UPF(s) interfacing the two parts of the DN is independent from the data path established per PDU session between the UE and the L-PSA UPF. The data path per PDU session between the UE and the L-PSA UPF interfacing the L-DN part is established as part of the PDU session establishment or update procedures as defined in TS 23.502 [3]. The tunnel between the L-PSA UPF(s) interfacing two parts of the DN can be shared by all PDU sessions whose traffic requires joint handling by the L-DN and the C-DN part. The solution focuses on the establishment and usage of the tunnels between the L-PSA UPF(s) interfacing two parts of the DN.

NOTE 2: Handling of the charging of the traffic through the tunnel(s) between the local and central parts of a DN can be achieved via existing mechanisms e.g. based on an SLA between the PLMN and the application provider or as part of sponsored data connectivity. Further details on charging aspect needs alignment with SA5.

The Application Function (AF) may request 5GC to establish the tunnel between the two parts of the DN based on the extended Data Network Access Identify (DNAI) related information in EAS Deployment Information (EDI).

One of the major problems of any solution that needs to tunnel traffic between 2 separate IP network, is how to deal with the routing. In the IP network routers exchange information about how to reach a destination via routing protocols. Now if the 2 IP network are disjoint, no routing information will flow between these networks. And thus, one cannot use an IP address of another network if there is no connection between them. This means that additionally, tunnels on N6 between the L-EAS and L-PSA UPF. need be established based on the L-EAS andUPF supported tunnel mechanisms, so that packets can be routed between the L-EAS and L-PSA UPF. In addision depending on IP address allocation in the C-PSA UPF, there may also be need for a tunnel between the C-EAS and C-PSA UPF.

#### 6.21.1.2 AF control of the connectivity between different DN parts

The solution updates EDI in Table 6.2.3.4-1 of TS 23.548 [5] with following information:

- an indicator whether the DNAI is to be considered as local or central;

- an indicator whether connectivity to central DNAI(s) is needed;

- tunnelling mechanisms at N6 supported by the EAS, and other relevant information.

For the AF, to create, update, or delete the information described above, the existing procedure defined in clause 6.2.3.4.2 of TS 23.548 [5] "EAS Deployment Information Management in the AF Procedure" apply. SMF may receive the information as part of the EDI from NEF via the existing procedure defined in clause 6.2.3.4.2 of TS 23.548 [5] "EAS Deployment Information Management in the SMF".

There may be two ways of establishing the tunnel either use EDI or by means of AF requesting the tunnels to be established.

### 6.21.2 Procedures

#### 6.21.2.1 Procedure to establish the tunnel between different DN parts using EDI

Based on the AF control of the connectivity between different DN parts as defined in clause 6.21.1.2, the 5GS establishes the tunnel between the different parts of the DN as described in this clause.

When SMF receives DNAI information requiring setting up connectivity between different DN parts, the SMF:

1. selects a L-PSA UPF based on the received DNAI of the L-DN and a Central PSA UPF (C-PSA UPF) based on the received DNAI of the C-DN.

NOTE: L-PSA UPF that is selected for the UE PDU session and the L-PSA that establishes the tunnel to the C-PSA can be different.

2. via existing N4 session signalling (providing PDRs and FARs) to the PSA UPF(s) to generate an Up Link Terminal Endpoint Identify (UL TEID) in C-PSA UPF and a Down Link Terminal Endpoint Identify (DL TEID) in L-PSA UPF, so that a tunnel can be established between L-DN and C-DN.

3. Configures the L-PSA UPF with PDR(s) and FAR(s) as defined below.

Figure 6.21.2-1 depicts the call flow of the establishing a tunnel to provide connectivity between the local and central parts of DN.



Figure 6.21.2-1: Procedure of establishing a tunnel between local and central parts of DN

The steps in the call flow are as follows:

1. AF provides 5GC with information to provide connectivity between the local and central part of DN and optionally, the tunnelling mechanism at N6, for example, the AF invokes the Nnef\_EASDeployment\_Create/Update/Delete service operation as the step 1 defined in clause 6.2.3.4.2 of TS 23.548 [5].

2. SMF is triggered to retrieve AF provided information. The trigger can be a NEF notification (related with EDI), or a 5GC event (e.g. PDU session establishment/modification, EAS (re-)discovery). SMF retrieves EDI, which includes information as defined in the above Clause 6.21.1.2. This information is conveyed from NEF to SMF via EDI based on EAS Deployment Information Management in the SMF defined in clause 6.2.3.4.3 of TS 23.548 [5]. The SMF determines to establish the tunnel based on this information received from the AF.

Steps 3 to 11 may take place for each pair of DNAIs (local/central) where the SMF is to establish a tunnel.

3. The SMF selects two UPFs as the L-PSA UPF and the C-PSA UPF, based on the two retrieved DNAIs.

4. The SMF initiates a N4 Session Establishment procedure with the selected C-PSA UPF. The N4 message contains PDR-1 and FAR-1 defined in the below Table 6.21.2-1 for UL traffic. C-PSA UPF performs the session configuration and UL TEID selection. During the session configuration, UL TEID (i.e. UL TEID of the tunnel) is used for L-PSA UPF to forward L-DN's UL traffic to C-DN via C-PSA UPF. If provided by the AF, the SMF selects one of the tunnelling mechanisms at N6 and establishes the tunnel at N6 towards C-EAS.

5. The C-PSA UPF responses SMF by sending an N4 Session Establishment Response, including the UL TEID of the C-DN tunnel which is a part of CN tunnel information, and optionally, sending information about the established N6 tunnel via N4, including the selected tunnelling mechanism at N6, the N6 tunnel endpoint address, and the N6 tunnel specific information if needed.

6. The SMF responds to the NEF with the received information about the established N6 tunnel, and the NEF forwards the information to the AF.

7. SMF initiates a N4 Session establishment procedure with the selected L-PSA UPF, to provide UL TEID of the tunnel to L-PSA UPF, as well as PDR-2 and FAR-2 defined in Table 6.21.2-1 for UL traffic. L-PSA UPF performs the tunnel configuration and DL TEID of C-DN tunnel/LL-DN tunnel selection. During the tunnel configuration, DL TEID of the tunnel is selected for L-PSA UPF to forward UL traffic to C-DN via C-PSA UPF. The SMF selects one of the tunnelling mechanisms at N6 provided by the AF and establishes the tunnel at N6 towards L-EAS.

8. L-PSA UPF provides SMF with the DL TEID of the C-DN tunnel which is a part of CN tunnel information. And optionally, provides information about the established N6 tunnel via N4, including the selected tunnelling mechanism at N6, the N6 tunnel endpoint address, and the N6 tunnel specific information if needed.

9. The SMF responds to the NEF with the received information about the established N6 tunnel, and the NEF forwards the information to the AF.

10. SMF initiates a N4 Session Update procedure with the selected L-PSA UPF and provide PDR-3 and FAR-3 defined in Table 6.21.2-1 for DL traffic.

11. L-PSA UPF responses SMF by sending an N4 Session Update Response.

12. SMF initiates a N4 Session Update procedure with the selected C-PSA UPF and provides DL TEID of the tunnel to C-PSA UPF, as well as PDR-4 and FAR-4 defined in Table 6.21.2.1-1 for DL traffic.

13. C-PSA UPF responses SMF by sending an N4 Session Update Response.

Table 6.21.2.1-1 shows PDRs and FARs for L-PSA UPF and C-PSA UPF configuration.

Table 6.21.2.1-1: PDRs and FARs for L-PSA UPF and C-PSA UPF

|  |  |  |
| --- | --- | --- |
| UPF | Rule | Description |
| C-PSA UPF (UL) | PDR-1 | Source Interface = access (N9)  Packet Filter Set (optional): Incoming Tunnel ID, IP DA = C-EAS IP (range)  GTP-U outer header removal  FAR ID = FAR-1’s ID |
|  | FAR-1 | Rule ID  C-PSA UPF’s N6 tunnel outer header adding  Action = forward  Destination interface = N6 |
| L-PSA UPF (UL) | PDR-2 | Source Interface = N6 (optional)  Packet Filter Set: Incoming L-PSA UPF’s N6 tunnel info  L-PSA UPF’s N6 tunnel outer header removalFAR ID = FAR-2’s ID |
|  | FAR-2 | Rule ID  Action = forward  Destination interface = N9  GTP-U outer header adding: GTP-u header that the SMF has received from the C-PSA |
| L-PSA UPF (DL) | PDR-3 | Source Interface = access N9 (optional)  Packet Filter incoming GTP-U tunnel  GTP-U outer header removal  FAR ID = FAR-3’s ID |
|  | FAR-3 | Rule ID  L-PSA UPF’s N6 tunnel outer header adding  Action = forward  Destination interface = N6 |
| C-PSA UPF (DL) | PDR-4 | Source Interface = N6 (optional)  Packet Filter Set: Incoming C-PSA UPF’s N6 tunnel info  C-PSA UPF’s N6 tunnel outer header removal  FAR ID = FAR-4’s ID |
|  | FAR-4 | Rule ID 004  Action = forward  Destination interface = access (N9)  GTP-U outer header adding: GTP-U header that the SMF has received from the L-PSA |

Once a packet is processed by the L-EAS and is to be sent to the C-EAS for further processing, the L-EAS setups L-EAS’s overlay address as the source IP address and C-EAS’s overlay address as the destination IP address of the packet. Using the established N6 tunnel, the L-EAS adds another N6 tunnel outer header, in which the L-EAS’s overlay address is the source address and L-PSA UPF’s tunnel endpoint address is the destination address. By receiving the packet from the L-EAS, the L-PSA UPF applies the defined PDRs and FARs. For packets generated by the C-EAS and to be routed to C-PSA UPF, same approach applies.

#### 6.21.2.2 Procedure to establish the tunnel between different DN parts using request by AF.

UPF2

UPF1

SMF

NEF

AF/EAS

1. Get tunnel req. (DNAIs, supported tunneling mech).

2. Get tunnel req. (dito)

3. set-up tunnel

4. Get tunnel resp. (endpoint, tunnel mechanism)

5. Get tunnel resp. (dito)

+-

AS

Figure 6.21.3-1: Request tunnel over 5GC

1. AF/EAS requests 5GC to set up a tunnel between 2 DNAIs. One could also imagine that the EAS/AF only gives IP address ranges of EAS and AS, or even FQDNs of these. If not DNAIs are provided, NEF needs to translate the provided info to DNAIs. The AF/EAS provides which tunnelling protocol it supports, e.g.. IP in IP, GRE, etc. Also other relevant data related to the specific tunnel, such as e.g. which optional parameters in GRE to be used, and in case this Key in GRE is used, what value. If AF/EAS supports masque e.g. connect IP (IETF RFC 9484 [x], AF/EAS can also indicate this. This step can happen at any time e.g., at EAS boot up or restart, when a UE first access the EAS, or via a management procedure in an AF.

2. NEF finds a SMF supporting both DNAIs and sends a request to this SMF.

3. SMF follows steps 3-6 in clause 6.21.2.1. With the following differences:

- SMF selects one of the tunneling methods provided by the AF/EAS (if 5GC supports at least one of them, else SMF rejects the request)

- PDRs from Solution #21 updated as follows:

PDRs and FARs for UPF1 and UPF2

|  |  |  |
| --- | --- | --- |
| UPF | Rule | Description |
| UPF2 (UL) | PDR-1 | Source Interface = access (N9)  Packet Filter Set (optional): Incoming Tunnel ID / IP SA = L-EAS IP (range), IP DA = C-EAS IP (range)  GTP-U outer header removal  FAR ID = FAR-1’s ID |
|  | FAR-1 | Rule ID  Action = forward  Destination interface = N6 |
| UPF1 (UL) | PDR-2 | Source Interface = N6’ Tunnel outer header removal  Packet Filter Set: Incoming Tunnel ID FAR ID = FAR-2’s ID |
|  | FAR-2 | Rule ID  Action = forward  Destination interface = N9  GTP-U outer header adding: GTP-u header that the SMF has received from the UPF2 |
| UPF1(DL) | PDR-3 | Source Interface = access N9 (optional)  Packet Filter: incoming GTP-U tunnel  GTP-U outer header removal  Tunnel Outer header adding  FAR ID = FAR-3’s ID |
|  | FAR-3 | Rule ID  Action = forward  Destination interface = N6’ |
| UPF2(DL) | PDR-4 | Source Interface = core (N6 (optional))  Packet Filter Set: IP SA = C-EAS IP (range), IP DA = L-EAS IP (range)  FAR ID = FAR-4’s ID |
|  | FAR-4 | Rule ID  Action = forward  Destination interface = access (N9)  GTP-U outer header adding: GTP-U header that the SMF has received from the UPF1 |

4. SMF responds with the selected tunneling mechanism and the tunnel endpoint address of UPF1 and also the tunnel specific information needed, e.g. if Key in GRE is to be used, the Key value. Or if masque is selected, the HTTP proxy address for masque control.

5. NEF forwards the received information from SMF to the AF/EAS

#### 6.21.2.3 QoS handling of the tunnel between different DN parts

The QoS requirement of the tunnel is independent from any UE’s PDU session, the QoS requirement is defined per DNAI or per application (identified by Application ID). The EDI in TS 23.548 [5] Table 6.2.3.4-1 is updated to contain the QoS requirement on a DNAI or application basis.

To guarantee the QoS requirement of the tunnel between the L-PSA UPF and the C-PSA UPF, DSCP approach is used. Specifically, the AF provides to the SMF via NEF on the requested QoS requirement in the EDI. For a given set of QoS parameter values from the QoS requirement, a DSCP value can be mapped which is used by the transport networks between the L-PSA UPF and C-PSA UPF. The SMF configures L-PSA UPF and C-PSA UPF to handling the QoS requirements, by defining the Packet Filter Set in PDRs and the FAR(s) linked to each PDR. With the PDRs, the UPFs are able to classify packets per QoS requirement with a given set of QoS parameter values. With the linked FAR(s), the UPFs are able to set the IE “transport layer marking” to the mapped DSCP value for transport level marking by a FAR.

For example, the following QoS parameters can be supported by the tunnel:

- Maximum Bit Rate (MBR) per DNAI (defined in current EDI), or per given application (based on Application ID);

- Packet Delay Budget (PDB): The delay between two UPFs’ terminating N6;

- Packet Error Rate: Packet sent by a UPF but not successfully received by another UPF.

### 6.21.3 Impacts on existing nodes and functionality

Impacted nodes and functionality are listed as follows:

**AF:**

- provides information to 5GC requesting application data forwarding between two parts of the DN (L-DN and a C-DN) via information described in clause 6.21.1.2.

**SMF:**

- select PSA UPFs (L-PSA UPF and C-PSA UPF), so that two parts of the DN can be anchored and a tunnel can be established in-between.

- configure two PSA UPFs (L-PSA UPF and C-PSA UPF) to send/receive traffic at L-DN or C-DN.

UPF:

- In deployments that would require N6 tunnel between EAS/AS and Local/Central PSA-UPF, support new tunnelling mechanisms, and control thereof by SMF

## 6.22 Solution #22: Establishment of connectivity between the local DN and central part of DN based on OAM

### 6.22.1 Key Issue mapping

The solution applies to Key Issue #3: EC Traffic Routing between local part of DN and central part of DN.

### 6.22.2 Description

Raw data collected by devices is expected to be processed locally (e.g. to remove privacy aspects, or reduce the volume of raw data) and then sent to central application servers for further data processing. On the other hand, the processed data by the central servers may be distributed to the local servers, for example, to control devices. In the context, local and central applications are expected to be configured in advance so that they can work together.

As given in the key issue, there might be a case where there is no direct connectivity between a local DN and central part of DN. In the context, the central part of DN hosts Application Server (AS) and a DNAI connecting with a PSA-UPF. The local part of DN hosts Edge Application Server (EAS) but the local part of DN is not connected to the PSA-UPF connecting to AS. Edge Hosting Environment in the local DN and central part of DN is managed by OAM in Edge Computing Service Provider (ECSP) in TS 28.538 [9]

The following procedure introduce how to deploy the communication link and routing requirements for application traffic between the EAS in the local part of DN and the AS in the central part of DN.

### 6.22.3 Procedures

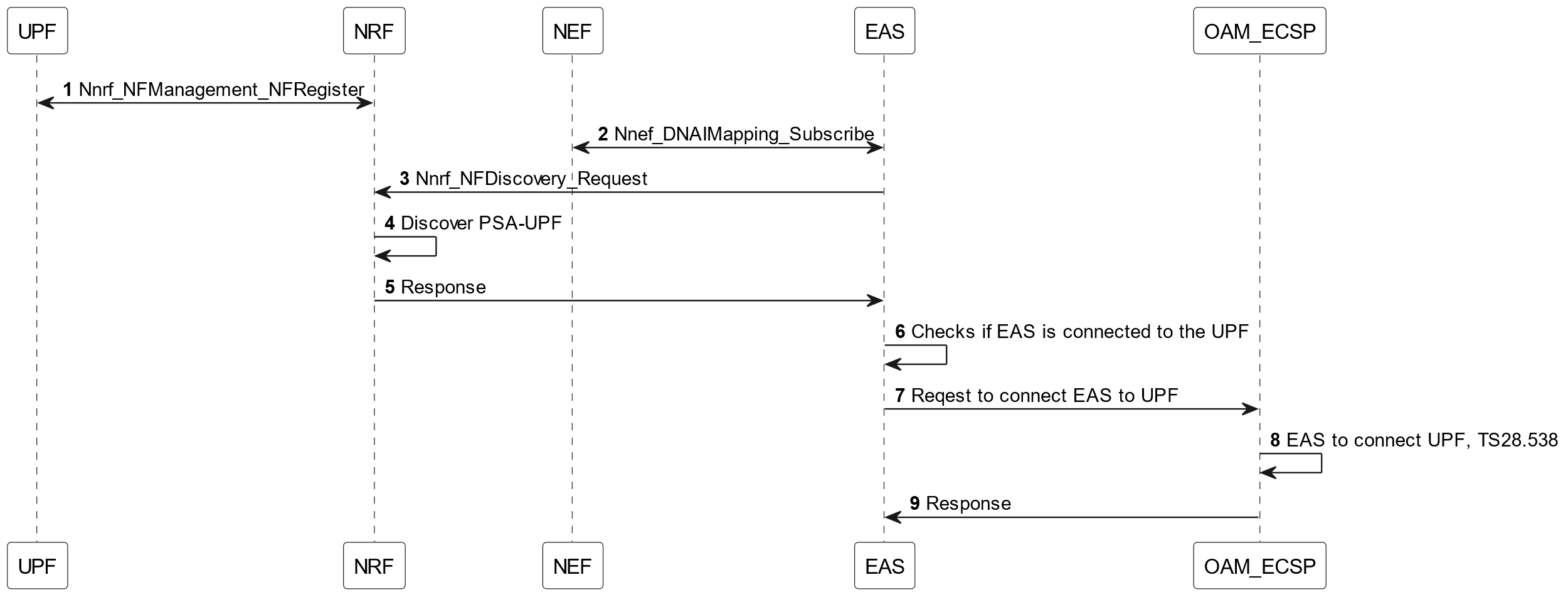


Figure 6.22.3-1: Procedure for connectivity between the local DN and central part of DN

1. UPF invokes Nnrf\_NFManagement\_NFRegister to request NRF to register UPF profile when UPF becomes operative for the first time. The request includes parameters that indicates DNAI(s) hosted by the UPF and supported Transit Gateway functionalities in the UPF. The Transit Gateway is a new capability to support routing between N6 reference points.

NRF responds UPF with an acceptance to Nnrf\_NFManagement\_NFRegister Request when the UPF profile is successfully stored.

2. Through an operation for Nnef\_DNAIMapping service operations in TS 23.502 [3], EAS receives DNAI information by providing specific information of AS such as IP address.

3. EAS invokes Nnrf\_NFDiscovery\_Request to request NRF to discover PSA-UPF(s) connecting to the AS. The request may include DNAI(s) received in the step 2 and supported new functionality, called transit gateway. The transit gateway functionality enables UPF to route traffic between local and central parts of DN(s).

4. NRF discovers a set of PSA-UPF instance(s) matching the Nnrf\_NFDiscovery\_Request.

5. NRF responds EAS with UPF profiles of the discovered PSA-UPF hosting DNAI connecting to AS, as well as supporting transit gateway.

6. EAS checks if EAS is connected to the discovered PSA-UPF. If connected, it is found that the DNAI connecting to EAS is hosted by PSA-UPF connecting to AS.

7. In the case where there is no PSA-UPF or EAS is not connected to the discovered PSA-UPF, connectivity needs to be provisioned. EAS creates N6 traffic routing list that includes DNAI(s) and N6 traffic routing information corresponding to each DNAI for EAS/ AS. As described in the clause 5.4.4, TS28.538 [9], EAS requests OAM\_ECSP to connect EAS to PSA-UPF supporting transit gateway connecting to AS in the central part of DN. The request includes EAS IP addresses and the N6 traffic routing list.

8. OAM\_ECSP works with OAM in the PLMN specified in TS 28.538 [9] in order to find and connect EAS with PSA-UPF supporting transit gateway.

In the case no PSA-UPF is found by OAM in the PLMN, OAM in the PLMN provisions a new PSA-UPF supporting transit gateway connecting to AS in the central part of DN and then connects EAS with the PSA-UPF.

In the case that a PSA-UPF is found but EAS is not connected to the found PSA-UPF by OAM in the PLMN, OAM in the PLMN provisions connectivity to connect EAS with the PSA-UPF.

9. OAM\_ECSP responds EAS with output that includes PSA-UPF information. Transit gateway routes traffic leveraging the N6 traffic routing information for AS and EAS.

### 6.22.4 Impacts on services, entities and interfaces

**UPF:**

- Support transit gateway functionality that enables to route traffic between local and central parts of DN(s).

**NRF:**

- Support NF profile for UPF with transit gateway support.

## 6.23 Solution #23: Traffic steering between different parts of a DN

### 6.23.1 Key Issue mapping

Key issue #3.

### 6.23.2 Description.

This solution addresses a scenario where the traffic steering between different parts of a DN for a given UE.

This solution considers the following cases (i) UL traffic first routed EAS in the local part of DN for local-processing (source IP: UE, destination IP: EAS IP-ue, which is given to UE), and then further forwarded to a remote Application Server in the central part of DN (source IP: EAS IP-steering, assigned to EAS only for the purpose of communicating AS, destination IP: remote AS), and (ii) DL traffic from a remote Application Server in the central part of DN for processing, then forwarded to Application Server(s) in the local part of DN (source IP: remote AS, destination IP: EAS IP-steering), and finally provided to the UE (source IP: EAS IP-ue, destination IP: UE).

NOTE: The solution assumes that EAS and AS uses the EAS/AS IP address assigned for the traffic steering via the UPFs and that the corresponding N6 tunnel is also set up for this purpose. Accordingly, it is assumed that such AS/EAS IP address can be pre-configured in the CN.

### 6.23.3 Procedures

The procedure is based on the existing procedure described in clause 4.3.6.2 of TS 23.502 [3] with additional parameters sent via the AF request and its corresponding SMF behaviour.



Figure 6.23.3-1: UP path configuration for traffic steering between different parts of a DN

1. The AF decides to send AF traffic influence request. In addition to the input parameters described in clause 5.2.6.7 of TS 23.502 [3], this request includes local consecutive steering indication, steering order (UL, DL, or both) local consecutive steering target application target DNAIs/FQDN/IP address, and inter AS latency requirement as local steering requirement information.

2-4. The steps 2-4 of Figure 4.3.6.2-1 in clause 5.2.6.7 of TS 23.502 [3] are performed.

5. In addition to the existing PCC rule information, the PCF sends to the SMF local consecutive steering rule including local consecutive steering target application target DNAIs/FQDN/IP address, steering order, and inter AS latency requirement.

6. Upon receiving the PCC rule information from the PCF, the SMF decides how to re-configure the UP path.

7-8. The SMF configures the EASDF with the DNS handling rule. After that, when the UE sends the DNS query and the EASDF gets the corresponding DNS response including EAS IP address, the EASDF notifies the SMF with the EAS IP address.

9. The SMF checks if the EAS IP address is matched with the local consecutive steering rule. If matched, the SMF utilizes the EAS IP address and the information contained in the local consecutive steering rule (e.g. target DNAI, inter AS latency requirement) to decide how to configure the UP path configuration, including local PSA selection for EAS located in the local part of DN, whether to insert/select a remote PSA selection for consecutive steering target AS located in the central part of DN and ULCL. To configure the UP path (including PSA UPF selection for the local part of DN and the central part of DN), the SMF uses the EAS IP address and the AS IP address in the local consecutive steering target application IP address.

(i) UL traffic first routed to EAS

PDR-1: Source interface = N3 / Packet Filter Set: Source IP: UE, Destination IP: EAS   
FAR-1 Action = forward, Destination interface = N6

(ii) From the EAS to a remote AS

PDR-2: Source interface = N6 / Packet Filter Set: Source IP: EAS, Destination IP: AS   
FAR-2 Action = forward, Destination interface = N9

(iii) From the AS to the EAS

PDR-3-1 (at central PSA): Source interface = N6 / Packet Filter Set: Source IP: AS, Destination IP: EAS   
FAR-3-1 (at central PSA) Action = forward, Destination interface = N9

(iv) From the EAS to the UE

PDR-4: Source interface = N6 / Packet Filter Set: Source IP: EAS, Destination IP: UE   
FAR-4 Action = forward, Destination interface = N3

Based on the above UP path configuration, the traffic between the EAS in the local part of DN and the remote AS in the central part of DN is routed via the selected local PSA, ULCL/BP, and remote PSA.

### 6.23.4 Impacts on services, entities and interfaces

**NEF:**

- exposes an API for AF to provide information for local consecutive steering (including local consecutive steering indication, steering order (UL, DL, or both) local consecutive steering target application target DNAIs/FQDN/IP address, and inter AS latency requirement as local steering requirement information).

**PCF:**

- creates and provides the SMF with the local consecutive steering rule.

**SMF:**

- checks if the EAS IP address, notified from the EASDF, is matched with the local consecutive steering rule.

- configures UP path to support local consecutive steering based on the EAS IP address received from the EASDF and information in the local consecutive steering rule.

## 6.24 Solution #24: Support traffic routing between local-DN and central-DN via the existing UP path of the PDU session and IP replacement

### 6.24.1 Key Issue mapping

This solution is proposed to solve KI#3. It is the merged solution on using the PDU session to convey the traffic between local DN to central DN the existing UP path of the PDU Session.

### 6.24.2 General Description

This solution resolves KI#3 about traffic routing between L-DN and central DN based on the scenario that the application traffic is required to be processed at different locations.

Based on AF traffic influence request information, the 5GC determines to enable the traffic routing between L-DN and central DN via the tunnel of PDU session.

* For the UL traffic, the UE generates traffic and send it to the EAS (i.e. target IP address is EAS IP address), the traffic is routed to EAS to be processed firstly. Then after processed by EAS, the EAS generates the traffic and send it to the AS (i.e. the cloud server) for further processing.
* For the DL traffic, the AS (cloud server) generates traffic based on the received UL traffic and send it back to the EAS.
* For UL/DL traffic between EAS and AS, L-PSA also perform IP replacement (if required).

For the traffic sent from EAS to cloud AS, there are three options (option 1: sol#18; option 2: sol#17; option 3:sol#19) on how to handle the user plane traffic at L-PSA, including the IP replacement as described in Table 6.24.2-1, and traffic rules configured at the UL CL/BP as described in Table 6.24.2-2. UL traffic is the traffic from EAS to AS and DL traffic is the traffic from AS to EAS.

Table 6.24.2-1 Traffic between local DN and central DN for each option

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Options | UL Traffic generated by EAS | How L-PSA associate the UL traffic with PDU session | How L-PSA performs IP replacement for UL traffic | DL Traffic generated by AS | How PSA associate the DL traffic with PDU session | How L-PSA performs IP replacement for DL traffic |
| **Option 1**  **(sol#18)** | Source IP:  EAS IP  Target IP:  AS IP | Based on IP 5-tuple  (NOTE 3) | Replace the source IP to UE IP2.  (NOTE 4) | Source IP:  AS IP  Target IP:  UE IP 2 | Based on UE IP 2  (target IP address) | Replace the target IP to EAS IP. |
| **Option 2**  **(sol#17)** | Source IP:  UE IP  Target IP:  EAS IP or  AS IP | Based on UE IP (source IP address) | None. | Source IP:  AS IP  Target IP:  UE IP | Based on UE IP (target IP address) | None. |
| **Option 3**  **(sol#19)**  (NOTE 1) | Source IP:  EAS IP 2  (NOTE 2)  Target IP:  UE IP | Based on UE IP (target IP address) | Replace the Source IP to UE IP address, and Target IP to AS IP address. | Source IP:  AS IP 2  Target IP:  UE IP | Based on UE IP (target IP address) | Replace the target IP to EAS IP.  Replace the source IP to AS IP. |
| NOTE 1: For option 3, to align with the existing mechanism, it is suggested not to perform IP replacement at ULCL/BP.  NOTE 2: EAS IP 2 is an IP address assigned by EAS, and is different from the IP address EAS used to communicate with UE.  NOTE 3: The IP 5-tuple is the IP 5-tuple of traffic between EAS and AS (i.e. EAS IP address, port number and AS IP address, port number)  NOTE 4: UE IP 2 is an IP address assigned by PSA, and is different from the UE IP included in the UL traffic.  NOTE 5: It is assumed that there is a tunnel configured between the L-PSA and EAS.  NOTE 6: AS IP 2 is an IP address assigned by AS, and is different from the IP address of AS used to communicate with UE. | | | | | | |

Table 6.24.2-2 Traffic routing rule configured at ULCL/BP for each option

|  |  |  |
| --- | --- | --- |
| Options | Traffic from L-PSA | Traffic from PSA |
| **Option 1**  **(sol#18)** | Target IP is UE IP address: Route to UE (RAN).  Others:  Route to PSA. | Target IP is UE IP address: Route to UE (RAN).  Others:  Route to L-PSA. |
| **Option 2**  **(sol#17)** | Target IP is UE IP address: Route to UE (RAN).  Others:  Route to PSA. | Source IP is AS IP:  Route to L-PSA for specific source AS IP  Others:  Route to UE (RAN). |
| **Option 3**  **(sol#19)** | Target IP is UE IP address: Route to UE (RAN).  Others:  Route to PSA. | Source IP is AS IP 2:  Route to L-PSA  Others:  Route to UE (RAN). |

NOTE 1: Option 2 and 3 assume the EAS can do IP replacement for the UL and DL traffic.

NOTE 2: Option 3 assumes the AS can assign two IP addresses, one is for directly communicate with UE and the other is for communicate with EAS.

NOTE 3: Option 3 assumes EAS IP 2 is preconfigured in 5GC for traffic detection.

### 6.24.3 Procedures

2. Packet detection and IP replacement configuration

1. AF request for local traffic routing

UE

SMF

PCF

ULCL/BP

L-PSA

PSA

EAS

AF/NEF

AS

(cloud server)

3. traffic routing rule configuration

5.Traffic from L-DN to central DN

6.Traffic from central DN to L-DN

4. Notify AF the user plane has been configured

0b. Traffic from UE

7.Traffic from EAS to UE

0a. PDU session establishment

Figure 6.24.2-1: High level procedure for supporting traffic routing between local DN and central DN via PDU session

Traffic from UE to EAS via the existing procedure.

1. The UE establishes a PDU Session as described in clause 4.3.2.2.1 of TS 23.502 [3]. The UE does the DNS query and finds the EAS. The UL CL/BP is inserted per existing procedure as defined in clause 6.2.3 of TS 23.548[5]. UE send the traffic to the EAS, i.e. the target IP address is EAS IP address, and UL CL/BP route the traffic to L-PSA.

Traffic from EAS to central AS (i.e. Cloud server) is routed via the tunnel of PDU session

1. The AF requests the SMF to perform traffic routing between local DN and central DN via the existing AF traffic influence procedure.

Following information are included in the information sent from AF to PCF: indication for traffic routing between local DN and central DN, traffic flow description for UL and DL (e.g. IP 5-tuples), target PDU session (e.g. associated UE IP address), QoS requirement of the indicated traffic flow.

Editor’s note: Whether other IEs should also be included in the AF request is FFS.

1. Based on AF request in step 1, the SMF configures UPF(s) (i.e. L-PSA and/or PSA) to detect traffic related to one dedicated PDU session, and performs IP replacement at L-PSA. The information for SMF to instruct to L-PSA/PSA is per the information described in Table 6.24.2-1. This step includes the following handling:

For UL traffic between local DN and central DN sent by EAS:

2a. The SMF configures the L-PSA to detect the indicated traffic flow and associate the indicated the traffic flow with the PDU session per the received traffic flow description and target PDU session information.

2b. The SMF configures the L-PSA to perform IP replacement for UL traffic.

For DL traffic between local DN and central DN sent by AS:

2c. the SMF configures the PSA to detect the indicated traffic flow and associate the indicated the traffic flow with the PDU session per the received traffic flow description and target PDU session information.

2d. The SMF configures L-PSA performs IP replacement for DL traffic.

NOTE 1: If UE IP 2 is used as described in Table 6.24.2-1, SMF also needs to request another UE IP address from PSA before step 2b.

1. The SMF configures the traffic routing rule on ULCL/BP to route traffic between L-DN and central DN. The information for SMF to instruct to UL CL/BP is detailed in Table 6.24.2-2.
2. The SMF notifies AF the traffic routing path between L-DN and central DN has been configured via PCF and/or NEF as described in clause 4.3.6.3 of TS 23.502 [3].
3. Traffic from L-DN (i.e. after processed by EAS) is sent to central DN via the tunnel of PDU session (i.e. via L-PSA, ULCL/BP and PSA).

The L-PSA determines which PDU session to convey the traffic per N4 rule configured in step 2. And the UL-CL/BP routes the traffic to PSA per the N4 rule configured in step 3.

1. Traffic from central DN (i.e. after processed by cloud server) sent to L-DN via the tunnel of PDU session (i.e. via PSA, ULCL/BP and L-PSA).

The PSA determines which PDU session to convey the traffic per the N4 rule configured in step 2. And UL-CL/BP route the traffic to L-PSA per the N4 rule configured in step 3.

1. Traffic sent from EAS to UE.

The L-PSA determines which PDU session to convey the traffic per UE IP address. And UL-CL/BP route the traffic to RAN per the N4 rule configured in step 3.

NOTE 2: All the traffic is within the PDU Session, thus operators can identify it with SDF template in a PCC rule and apply appropriate QoS parameter as described in clause 6.3 TS 23.503 [4]. The PCF can generate QoS parameter considering the QoS requirement required by AF.

NOTE 3: All the traffic is within the PDU Session, thus operators can identify it with SDF template in a PCC rule and apply appropriate charging key and charging method (e.g. neither of online or offline charging) as described in clause 6.6 TS 23.503 [4]. There can also be Sponsor Identifier if it is charging for 3rd party as described in clause 6.6 TS 23.503 [4].

### 6.24.4 Impacts on services, entities and interfaces

**SMF (applies for all three options):**

* Generate traffic routing rule on ULCL/BP and PDR, FAR on L-PSA/PSA based on AF influence as described above.
* Inform AF the routing path has been configured.

NOTE X: Details of the traffic routing rule, PDR, FAR are different for three options and described in UPF impacts.

**L-PSA:**

- detect traffic between local DN and central DN (based on IP 5-tuple for option1, based on UE IP for option 2,3) and route the traffic to ULCL/BP.

- For option 1,3: Perform IP replacement for traffic between local DN and central DN.

**ULCL/BP:**

- Route traffic from EAS to AS based on Table 6.24.2-2.

**PSA:**

- For option 1: assign UE IP 2 for IP replacement.

**AF (applies for all three options):**

- inform 5GC to configure the traffic between local DN and central DN.

6.25 Solution #25: EC Traffic Routing between local part of DN and central part of DN with UE IP address within IP header

### 6.25.1 Key Issue mapping

This solution is for KI #3 EC Traffic Routing between local part of DN and central part of DN.

### 6.25.2 Description

According to KI #3, UL traffic may need to be firstly steered to EAS for first-step processing then to the central AS.DL traffic may need to be firstly steered to EAS then to the UE. However, there may be no direct connectivity between the local DN and central DN.

In this solution,it is proposed the traffic routing as below:

UL:

* UE sends UL packets to EAS. The source IP address is UE IP address, and the destination IP address is EAS IP.
* When EAS sends the UL packets to Central AS(CAS), the source IP address is EAS IP address, and the destination IP address is CAS IP, and EAS adds the UE IP address in the UL packet IP header(e.g. IPv6 Extension Headers).
* Local-PSA UPF identifies the UE IP address in the UL packet IP header and classifies the packet into the target PDU session tunnel.
* ULCL/BP UPF forwards the UL packets to the Central PSA UPF and CAS. The source IP address is EAS IP, and the destination IP address isCAS IP, and the UE IP is included in the UL packet IP header(e.g. IPv6 Extension Headers).

DL:

* CAS sends DL packets to EAS. The source IP address is CAS IP, and the destination IP address is EAS IP, and the UE IP is included in the DL packet IP header(e.g. IPv6 Extension Headers).
* Central PSA identifies the UE IP address in the DL packet IP header and classifies the packet into the target PDU session tunnel.
* ULCL/BP UPF forwards the DL packets to the Local PSA UPF and EAS.
* DL packets from EAS to UE: The source IP address is EAS IP, and the destination IP address is UE IP.

NOTE: This solution is only applied to PDU session with IPv6.

### 6.25.3 Procedures

UE

SMF

ULCL/BP

L-PSA

PCF

C-PSA

NEF

AF

EAS

4. N4 Session Modification

2. AF request for traffic routing between local DN and central DN

Central AS

1. UL CL/BP insertion, clause 4.3.5.4 of TS 23.502

3. PCC rule for traffic routing between local DN and central DN

5. UL traffic

6. UL traffic

7. DL traffic

8. DL traffic

0. PDU Session Establishment procedure, clause 4.3.2.2.1 of TS 23.502

Figure 6.25.3-1: EC Traffic Routing between local part of DN and central part of DN with UE IP address in packet

0. PDU Session Establishment procedure, as described in clause 4.3.2.2.1 of TS 23.502 [3].

1. The SMF inserts ULCL/BP and L-PSA, as described in clause 4.3.5.4 of TS 23.502 [3].

2. The AF sends a request to PCF (optionally via NEF) to configure a traffic routing path between local DN and central DN. The AF request includes UE IP address as target UE.

3. The PCF generates PCC rule for traffic routing between local DN and central DN based on AF request. The PCF sends the PCC rule to SMF.

4. The SMF configures the traffic detecting rule and routing rule in ULCL/BP to detect and forward traffic between EAS and CAS as follows:

- For traffic that UE IP address is included in the IP header (e.g. IPv6 Extension Headers), the UL CL/BP forwards the traffic to the destination IP via the PDU Session related to the UE IP.

For UL traffic:

5. The UE sends UL traffic (src IP: UE IP, dst IP: EAS IP) to UL CL/BP, and UL CL/BP forwards the traffic to L-PSA and then local EAS.

6. After processing, the EAS includes the UE IP address in the IP header (e.g. IPv6 Extension Headers), and sends the packet to L-PSA and then UL CL/BP (src IP: EAS IP , dst IP: CAS IP). Based on the traffic routing rule received in step 4, the UL CL/BP forwards the packet to central PSA and then CAS, via the same PDU Session as UE sends the packet to the local EAS.

For DL traffic:

7. The CAS sends DL traffic (src IP: CAS IP , dst IP: EAS IP) to central PSA via tunnel between CAS and central PSA, then forward to UL CL/BP. UE IP address is included in the DL packet IP header (e.g. IPv6 Extension Headers). Based on the traffic routing rule received in step 4, the UL CL/BP forwards the packet to L-PSA and then local EAS, via the same PDU Session as receives the packet from the local EAS.

8. After processing, the local EAS sends DL packets to L-PSA then the UL CL/BP (src IP: EAS IP , dst IP: UE IP). The UL CL/BP forwards the DL packet to UE.

### 6.25.4 Impacts on services, entities and interfaces

SMF

- Configuring the ULCL UPF, local PSA UPF, central PSA UPF to support the UL/DL traffic processing between local DN and central DN.

## 6.26 Solution #26: Solution on Enhancements for EAS (re)discovery and UPF (re)selection with reducing impact on central 5GC NFs

### 6.26.1 Description

This solution addresses KI#1.

This solution is in particular based on the below main architectural aspects:

- Use URSP to enable UE, while in certain location, initiate a PDU Session establishment with certain DNN, S-NSSAI

- Ensures a “local” SMF is selected as part of initial PDU session establishment. AMF is configured to select “Local” SMF serving the UE location, and for the requested DNN, S-NSSAI. If the UE moves out of certain area and/or not served by this “local” SMF then a PDU session release is initiated by SMF, and UE initiates a new PDU session establishment.

- In case of Session breakout scenarios, an I-SMF is inserted i.e. instead of Releasing the PDU session.

- Support all three connectivity models i.e. Distributed Anchor Point, Multiple PDU Sessions and session breakout models.

#### 6.26.2 Procedures

##### 6.26.2.1 Distributed Anchor Point and Multiple PDU Session models

Procedures defined in clause 6.2.2 of 23.548 on SSC Mode 2/3 and in clause 4.3.5 of 23.502 are used for Distributed Anchor Point and Multiple PDU Session models. An example procedure is given as follows:



Figure 6.26.2.1-1: “Local” SMF selection as part of PDU session establishment

Step 1. UE Registration, as in Clause 4.2.2, TS 23.502

Step 2. UE is configured with URSP Rule in order to support local offloading of some application traffic in a specific area (e.g. enterprise location with DNN/enterprise):

* URSP is provided with RSD (DNN, S-NSSAI) with validity conditions containing location validity (e.g. TAI(s), Cell ID(s))

Step 3. UE sends PDU session establishment request, with specific DNN, S-NSSAI, while in the applicable location, as indicated in the URSP.

Step 4. AMF based on the received subscription information from UDM and configuration information, selects “Local” SMF for this PDU session.

Step 5-6. AMF also provides an indication e.g. Local Offloading indication to the selected SMF that the PDU session is valid only for certain UE’s area.

Step 7. SMF Selects UPF and establishes N4 Session.

Step 8. SMF subscribes to AMF for UE location notification, and thus receives notification.

Step 9. If SMF receives notification on UE being outside the area i.e. TAIs received in step 5, SMF sends PDU session release request.

Step 10-11. UE initiates a new PDU session establishment procedure.

##### 6.26.2.2 Session Breakout model

For Session Breakout model, I-SMF is inserted. I-SMF receives local offloading policy information, as described in Solution #5 in clause 6.5. I-SMF retrieves EDI to configure EASDF and DNS message handling locally.



Figure 6.26.2.2-1: PDU Session Establishment with supporting local offloading control

Step 1. The steps from 1 to 17 in Figure 6.5.3.1-1 are followed in order to insert an I-SMF and enable I-SMF to select local UPF based on offloading policies received from SMF.

Step 2. I-SMF retrieves EAS Deployment Information as defined in clause 6.2.3.4 of TS 23.548.

Step 3. I-SMF configures EASDF for DNS message handling as defined in clause 6.2.3.2.2 of TS 23.548 based on retrieved EDI and local offloading information. Local offloading information is similar to VPLMN specific Offloading Information described in TS 23.548 and TS 23.503, and is used to indicate IP range(s) and/or FQDN(s) allowed to be routed to the local part of DN. I-SMF makes use of the local offloading information together with the retrieved EDI.

Step 4. The steps from 7 to 19 in Figure 6.2.3.2.2-1 of TS 23.548 are followed.

#### 6.26.4 Impacts on services, entities and interfaces

**SMF (for Session Breakout)**

- Receiving local offloading policies from PCF.

- Providing local offloading policy(ies) to I-SMF.

**I-SMF (for Session Breakout)**

- Receiving local offloading policy information from SMF

- Retrieves EDI for offloading information

- configures EASDF, and DNS message handling.

**PCF (for Session Breakout)**

- provides the local offloading management policy to the SMF.

**AMF (for Session Breakout)**

* checks if the local offloading control is allowed, and if allowed, inserts/selects the I-SMF.
* sends the Local Offloading Control Indication to the selected I-SMF.

## 6.X Solution #X: <Solution Title>

### 6.X.1 Key Issue mapping

Editor's note: This clause lists the key issue(s) addressed by this solution.

### 6.X.2 Description

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

### 6.X.3 Procedures

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

### 6.X.4 Impacts on services, entities and interfaces

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

# 7 Overall Evaluation

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

## 7.1 Evaluation for KI#1

There are 7 solution related to KI#1, i.e. solution #1-#7. The solution can be categorized into 4 groups:

* Group 1: I-SMF based offloading solution.
* Group 2: L-SMF based offloading solution.
* Group 3: Two PDU sessions based solution.
* Group 4: EDI provisioned solution.

**G1: I-SMF based offloading solution**

I-SMF based offloading solution is that the SMF which control the offloading traffic is put before the anchor SMF, i.e. I-SMF. The Edge related information and handling, i.e. DNS context management, DNS message handling, UL-CL/BP and L-PSA insertion is handled by I-SMF. This includes the solution#1, #5.

NOTE 1: In this category even it is called as I-SMF based offloading solution, it does not mean the functionalities define in the I-SMF in this category solution is same as existing defined I-SMF.

**G2: L-SMF based offloading solution**

L-SMF based offloading solution is that the SMF which control the offloading traffic is put after the anchor SMF. The Edge related information and handling, i.e. DNS message handling, L-PSA insertion is handled by L-SMF. The DNS context management, UL-CL/BP insertion is handled by SMF. This includes the solution#3, #4.

**G3: Two A-SMF based offloading solution**

Two A-SMF based offloading solution is that the two A-SMF are selected and interact with PCF from SMF/L-SMF separately but combined as one PDU session. The UL CL/BP/L-PSA insertion, interaction with NG-RAN are handled by L-SMF. This includes the solution#2.

**G4: EDI provision solution**

Solution #6 and #7 introduces EDI provision methods.

## 7.2 Evaluation for KI#2

## 7.3 Evaluation for KI#3

There are 7 solutions (Sol#17, 18, 19, 20, 21, 22, 23) in the TR for KI#3. These 7 solutions can be classified into 3 categories from Traffic forwarding perspective:

* CAT-A: Traffic forwarding by reusing the established User Plane path of the PDU Session (Sol#17, 18, 19, 20, 23);
* CAT-B: Traffic forwarding by establishing a new User Plane path between the L-PSA UPF and C-PSA UPF (Sol#21);
* CAT-C: Traffic forwarding by establishing a tunnel between EAS and PSA UPF (Sol#22) based on OAM mechanism, which is out of SA2 scope.

# 8 Conclusions

Editor's note: This clause will list conclusions that have been agreed during the course of the study item activities.

## 8.1 Conclusion for KI#1

The following principles are concluded for the normative work.

Editor’s Note: it is FFS whether the offloading SMF is I-SMF as defined in Group 1 or L-SMF as defined in Group 2 solution.

Editor’s Note: whether the offloading SMF needs to first select DNAI to then select the L-PSA UPF is FFS.

## 8.2 Conclusion for KI #2

The following principles are recommended in normative work for KI #2: Enhancement of EAS and local UPF (re)selection

- SMF selects local PSA UPF considering N6 delay, when available.

Editor’s NOTE: Whether SMF collects N6 delay measurements from the L-PSA UPF or from the AF is FFS

Editor’s NOTE: Whether EAS load can also be used by the SMF/EASDF is FFS.

- N6 delay between L-PSA UPF and EAS is measured by leveraging existing mechanisms (e.g., defined by IETF, PING, TWAMP, OWAMP, etc.)

- Interaction between AF and 5GC may be needed to enable the measurement

Editor’s NOTE: Details of such interaction are FFS.

Editor’s NOTE: Whether the NWDAF should be involved is FFS.

## 8.3 Conclusion for KI#3

**Interim conclusion:**

* The traffic routing rule between local DN and central DN should be controlled by SMF, which can be influenced by AF.
* The requirement of establishing connectivity for traffic routing between local DN and central DN should be provided by AF.
* QoS should be supported for the traffic routed between local DN and central DN.
* Charging should be supported for the traffic routed between local DN and central DN, any charging issue should be verified with SA5.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-01 | SA2#160-Ah Hoc-e |  |  |  |  | Initial TR skeleton. | 0.0.0 |
| 2024-01 | SA2#160-Ah Hoc-e |  |  |  |  | Implementing following approved papers: S2-2400477, S2-2401711, S2-2401712, S2-2401645, S2-2401714, S2-2401715. | 0.1.0 |
| 2024-03 | SA2#161 |  |  |  |  | Implementing following approved papers: S2-2403096, S2-2403358, S2-2403359, S2-2403587, S2-2403588, S2-2403362, S2-2403363, S2-2403366, S2-2403365, S2-2403607, S2-2403369, S2-2403608, S2-2403609, S2-2403372, S2-2403610, S2-2403611, S2-2403612, S2-2403122, S2-2403584, S2-2403582, S2-2403128, S2-2403613, S2-2403585, S2-2403586. | 0.2.0 |
| 2024-03 | SA2#162 |  |  |  |  | Implementing following approved papers: S2-2405588, S2-2405589, S2-2405291, S2-2405293, S2-2405593, S2-2405300, S2-2405594, S2-2404200, S2-2405303, S2-2405595, S2-2405304, S2-2405596, S2-2405306, S2-2405308, S2-2405309, S2-2405310, S2-2405311, S2-2405312, S2-2405313, S2-2405613, S2-2405295, S2-2405296, S2-2405598, S2-2405599, S2-2405614, S2-2405590, S2-2405591 | 0.3.0 |
|  |  |  |  |  |  |  |  |