|  |
| --- |
| 3GPP TS 23.548 V0.1.0 (2021-03) |
| Technical Specification |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;5G System Enhancements for Edge Computing;Stage 2(Release 17) |
|   |
|  |  |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2021, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Abbreviations 6

4 Reference Architecture and Connectivity Models 7

4.1 General 7

4.2 Reference Architecture for Supporting Edge Computing 7

4.3 Connectivity Models 7

5 Functional Description for Supporting Edge Computing 8

6 Procedures for Supporting Edge Computing 8

6.1 General 8

6.2 EAS Discovery and Re-discovery 8

6.2.1 General 8

6.2.2 EAS (Re-)discovery over Distributed Anchor Connectivity Model 8

6.2.2.1 General 8

6.2.2.2 EAS Discovery Procedure 8

6.2.2.3 EAS Re-discovery Procedure at Edge Relocation 8

6.2.3 EAS (Re-)discovery over Session Breakout Connectivity Model 9

6.2.3.1 General 9

6.2.3.2 EAS Discovery Procedure 9

6.2.3.2.1 General 9

6.2.3.2.2 EAS Discovery Procedure with EASDF 9

6.2.3.2.3 EAS Discovery Procedure with Local DNS Server/Resolver 13

6.2.3.3 EAS Re-discovery Procedure at Edge Relocation 15

6.2.4 Support of AF Guidance to PCF Determination of Proper URSP Rules 16

6.3 Edge Relocation 16

6.3.1 General 16

6.3.2 Edge Relocation Triggered by AF 16

6.3.3 Edge Relocation Using EAS IP Replacement 16

6.3.3.1 EAS IP Replacement Procedures 17

6.3.3.1.1 Enabling EAS IP Replacement Procedure 17

6.3.3.1.2 EAS IP Replacement Update upon DNAI and EAS IP Change 18

6.3.3.1.3 Disabling EAS IP Replacement Procedure 19

6.3.3.2 Enhancement to AF Influence 19

6.3.4 Simultaneous Connectivity for Source and Target EASs 19

6.3.5 Packet Buffering for Low Packet Loss 20

6.3.6 Edge Relocation Considering User Plane Latency Requirement 21

6.4 Network Exposure to Edge Application Server 22

6.4.1 General 22

6.4.2 Network Exposure to Edge Application Server via Local NEF 22

6.5 Support of 3GPP Application Layer Architecture for Enabling Edge Computing 24

6.5.1 General 24

6.5.2 ECS Address Provisioning 24

6.5.2.1 ECS Address Provisioning by a 3rd Party AF 25

7 Network Function Services and Descriptions 25

Annex A (Informative): EAS Discovery Using 3rd Party DNS Server 26

Annex B (Informative): Application Layer based EAS (Re-)Direction 27

Annex C (Informative): UE Considerations for EAS (re)Discovery 27

C.1 General 27

C.2 Impact of IP Addresses for DNS Resolver 27

C.3 UE Considerations for EAS Re-discovery 28

C.4 UE Procedures for Session Breakout 28

Annex D (Informative): Examples of AF Guidance to PCF for Determination of URSP Rules 28

Annex E (Informative): Change history 29

# Foreword

This Technical Specification 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.

# 1 Scope

The present document defines the Stage 2 specifications for enhancements of 5G System to support Edge Computing.

# 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; Stage 2".

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

[5] 3GPP TS 23.558: "Architecture for enabling Edge Applications (EA)".

[6] IETF RFC 7871: "Client Subnet in DNS Queries".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP 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 3GPP TR 21.905 [1].

**Edge Application Server:** An Application Server resident in the Edge Hosting Environment.

**Edge Hosting Environment:** An environment providing support required for Edge Application Server's execution.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP 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 3GPP TR 21.905 [1].

C-DNS Central DNS

C-NEF Central NEF

C-PSA UPF Central PSA UPF

EAS Edge Application Server

EASDF Edge Application Server Discovery Function

EHE Edge Hosting Environment

L-DNS Local DNS

L-NEF Local NEF

L-PSA UPF Local PSA UPF

# 4 Reference Architecture and Connectivity Models

Editor’s Note: Bring assumptions, connectivity models and hosting models from the TR clause 4. Privacy considerations in TR clause 7.12. could also considered here.

## 4.1 General

Editor’s Note: This chapter refers to TS 23.501 chapter 5.13 for an overview of the 3GPP specified functions which are part of 5GC Support to Edge Computing

## 4.2 Reference Architecture for Supporting Edge Computing

## 4.3 Connectivity Models

5GC supports the following connectivity models to enable Edge Computing:

- Distributed Anchor Point: The PSA UPF is in a local site, i.e. close to the UE location. The PSA UPF may be changed e.g. due to UE mobility and using SSC mode 2/3.

- Session Breakout: The PDU Session has a C-PSA UPF in a central site and a L-PSA UPF in the local site. The C-PSA UPF provides the IP Anchor Point when UL Classifier is used. The Edge Computing application traffic is selectively diverted to the L-PSA UPF using UL Classifier or multi-homing Branching Point technology. The L-PSA UPF may be changed due to e.g. UE mobility.

- Multiple PDU Sessions: Edge Computing applications use PDU Session with a PSA UPF in the local site. The rest of applications use PDU Session with C-PSA UPF. The L-PSA UPF may be changed due to e.g. UE mobility and using SSC mode 3 with multiple PDU Sessions.

URSP rules, for steering the mapping between applications and PDU Sessions, can be used for any connectivity model and they are required for the Multiple PDU Sessions model.

These three connectivity models are illustrated in Figure 4.3-1:



Figure 4.3-1: 5GC Connectivity Models for Edge Computing

# 5 Functional Description for Supporting Edge Computing

Editor’s Note: EASDF(LDNSR) is specified here: role, functionality and depolyment

Editor’s Note: This clause also brings clarity in the high-level relation between the solutions described in this TS and solutions built on SA6 Architecture for Enabling Edge Applications.

# 6 Procedures for Supporting Edge Computing

## 6.1 General

Editor’s Note: Any requirements on the applications and solution limitations are documented. For the detailed procedures for the management of the connectivity and run-time coordination with the application layer this clause refers to TS 23.502 and to TS 23.503 for the details on the Policy and Charging Control aspects.

## 6.2 EAS Discovery and Re-discovery

### 6.2.1 General

Editor’s Note: This clause describes general parts including e.g. privacy considerations, which DNS properties that are enabling DNS based Edge AS Discovery, recommendations/limitations for cases that OS/user overrides DNS setting.

### 6.2.2 EAS (Re-)discovery over Distributed Anchor Connectivity Model

#### 6.2.2.1 General

#### 6.2.2.2 EAS Discovery Procedure

Editor’s Note: This clause describes the procedure for Edge AS Discovery over Distributed Anchor connectivity model according to the recommendations in the conclusions in the TR clause 9.1.2 (selected parts from Sol 2/4/5/10).

In order to provide a translation of the FQDN of an EAS into the address of an EAS as close as possible to the UE (where closeness relates to IP forwarding distance), the DNS system uses mechanisms described in clause 6.2.1.

For Distributed Anchor Point connectivity model, in order to provide addressing information to the DNS system that is related to the UE topological location, when a DNS request is sent via the Local PSA UPF,

- either the DNS request is resolved by a DNS resolver, which then adds a DNS ECS option that may be built based on a locally pre-configured value or based on the source IP address of the DNS request; then send the DNS Query to the Authoritative DNS server, which may take into account the DNS ECS option, or

- the DNS request is resolved by a DNS server that is close to the PSA UPF: the Authoritative DNS server may take into account the source IP address of the DNS query.

#### 6.2.2.3 EAS Re-discovery Procedure at Edge Relocation

Editor’s Note: This clause also describes rediscovery (UE based), and aspects and assumptions based on applicable clause 9.2.2 in the TR

### 6.2.3 EAS (Re-)discovery over Session Breakout Connectivity Model

#### 6.2.3.1 General

This clause describes the EAS discovery and re-discovery procedures for PDU Session with Session Breakout connectivity model.

Editor's Note: The following C-DNS/L-DNS description will be moved to other more generic clause in future meeting since it applies to all connectivity models.

Central DNS (C-DNS) server is centrally deployed by MNO or 3rd party and is responsible for resolving the UE DNS queries into suitable Edge Application Server (EAS) IP address(es).

Local DNS (L-DNS) resolvers/servers may be locally deployed by MNO or 3rd parties within the Local DN, and is responsible for resolving UE DNS queries into suitable EAS IP address(es) within the local DN. The L-DNS resolvers/servers may or may not have connectivity with C-DNS depending on the deployment.

NOTE 1: The C-DNS server and/or L-DNS resolvers/servers can use an anycast address.

NOTE 2: The C-DNS server or L-DNS resolvers/servers can contact any other DNS servers for recursive queries, which is out of scope of this specification.

Editor's Note: The following Session Break Out model descriptions will be moved to other more generic clause in future.

The following Session breakout models are defined:

- Dynamic Session Breakout: ULCL/BP/Local PSA (and their associated traffic filters and forwarding rules) are inserted based on DNS Response provided by the EASDF.

- Pre-established Session Breakout: ULCL/BP/Local PSA (and their associated traffic filters and forwarding rules) are inserted without dependency on the UE sending out DNS queries or data traffic. They are typically inserted based on local configuration or per AF request.

#### 6.2.3.2 EAS Discovery Procedure

##### Editor’s Note: This clause describes the procedure for Edge AS Discovery over Session Breakout connectivity model according to the recommendations in the conclusions in the TR clause 9.1.4.6.2.3.2.1 General

For PDU Session with Session Breakout connectivity model, based on UE subscription (e.g. DNN) and/or the operator’s configuration, the DNS Query sent by UE may be handled by an EASDF (see clause 6.2.3.2.2), or by a local or central DNS resolver/server (see clause 6.2.3.2.3).

##### 6.2.3.2.2 EAS Discovery Procedure with EASDF

For the case that the UE DNS Query is to be handled by EASDF, the following applies.

- During the PDU Session establishment procedure, the SMF selects an EASDF and provides its address to the UE as the DNS Server to be used for the PDU Session. The UE sends DNS Query to the EASDF. The SMF may configure the EASDF with DNS message handling rules to forward DNS messages of the UE and/or report when detecting DNS messages. The DNS message reporting rule may include DNS message type (i.e. DNS Query or DNS Response), IP address range(s) or FQDN range(s) in DNS Answer field or FQDN range(s) in DNS Query field.

- If the FQDN in a DNS Query matches the FQDN(s) provided by the SMF, based on instructions by SMF, one of the following options is executed by the EASDF:

Editor’s Note: It is FFS how non-UE specific EAS’s FQDN information is configured with the SMF.

- Option A: The EASDF adds the EDNS Client Subnet (ECS) option into the DNS Query message as defined in RFC 7871[6], and sends the DNS Query message to the DNS server. The DNS server resolves the EAS IP address considering the ECS option, and sends the DNS Response to the EASDF.

- Option B: The EASDF forwards the DNS Query message to a suitable Local DNS server which is responsible for resolving EAS within the corresponding Local DN, and receives DNS Response message from Local DNS server.

NOTE 1: Option B does not support the scenario where the EASDF has no direct connectivity with the local DNS servers.

 The SMF instructions for a matching FQDN may as well indicate EASDF to contact SMF. SMF then provides instructions to EASDF to execute one of the above Options (A or B) or to simply forward the DNS Query towards a preconfigured DNS server/resolver for DNS resolution.

- If the DNS Query from the UE does not match a DNS message handling rules set by the SMF, then the EASDF may simply forward the DNS Query towards a preconfigured DNS server/resolver for DNS resolution.

- When the EASDF receives a DNS Response message, the EASDF may notify the EAS information (i.e. EAS IP address(es) and optionally the EAS FQDN) to the SMF if the DNS message reporting condition provided by the SMF is met. The SMF may trigger UL CL/BP and L-PSA insertion as specified in clause 6.3.3 in TS 23.501 [2] based on the Notification.

 The ECS option or the Local DNS server address provided by the SMF to the EASDF are part of the rules to handle DNS queries from the UE. They are related to candidate DNAI(s) for that FQDN for the UE location. The SMF may provide rules to handle DNS queries from the UE to the EASDF either when the SMF establishes the association with the EASDF for the UE, and may update the rules at any time when the association exists. For the selection of the candidate DNAI(s) for an FQDN for the UE, the SMF may consider the UE location, network topology and information of EAS deployment received as part of PCC rules. After the UE mobility, if the provided ECS option or the Local DNS server need be updated, the SMF notifies them to the EASDF.

Editor's Note: The sentence above means that the EASDF gets the FQDN(s) from SMF. How the SMF getting the FQDN(s) with DNS related information e.g. the ECS option or the Local DNS server address needs to be clarified in AF influence on traffic routing procedure specified in 3GPP TS 23.502 [3].

Once the UL CL/BP and L-PSA have been inserted, the SMF may decide that the DNS messages for the FQDN are to be handled by local DNS resolver/server from now on. This option is further described in clause 6.2.3.2.3.



Figure 6.2.3.2.2-1: EAS discovery procedure with EASDF

1. UE sends PDU Session Establishment Request to the SMF as shown in step 1 of clause 4.3.2.2.1 of TS 23.502 [3].

2. The SMF selects EASDF as described clause 6.3.x (TBD) of TS 23.501 [1]. This selection may use NRF discovery or may be based on SMF local configuration. The EASDF may have registered onto the NRF.

Editor’s Note: It is FFS whether the EASDF can register itself to the NRF.

3. The SMF invokes Neasdf\_DNSContext\_Create Request (UE IP address, callback URI , rules to handle DNS messages from the UE) to the selected EASDF. The rules to handle DNS messages from the UE (i.e. DNS message handling rule) may include DNS message forwarding rule and/or DNS message reporting rule. The DNS message forwarding rule includes DNS server address to be forwarded and/or the ECS option to be added.

 This step is performed before step 11 of PDU Session Establishment procedure in clause 4.3.2.2.1 of TS 23.502 [3].

 The EASDF creates a DNS context for the PDU Session, and stores the UE IP address, the callback URI and rules to handle DNS messages from the UE into the context.

 The DNS message reporting rule includes the reporting condition for the EASDF to report the DNS information including EAS related information to SMF when it receives DNS Queries or DNS Responses.

- For EASDF to process DNS Query for ECS options or local DNS server address handling, the SMF may provide the reporting rule to instruct the EASDF to send the EAS FQDN(s) to the SMF if the EAS FQDN in the DNS Query message matches with the FQDN(s) filters in the DNS message reporting rule.

- For EASDF to process DNS Response for specific IP address or FQDN ranges, the SMF provides the reporting rule to instruct the EASDF to report EAS IP address/FQDN to the SMF if the EAS IP address in the DNS Responses message matches one of the IP address range(s) of the reporting rule, or the FQDN in the DNS Response matches one of the FQDNs in the DNS message reporting rule.

 The EASDF is provisioned with the forwarding rule(s), i.e. ECS option(s) or local DNS Server(s) for the FQDN(s) and DNAI(s), before the DNS Query message is received at the EASDF or as a consequence of the DNS Query reporting.

4. The EASDF invokes the service operation Neasdf\_DNSContext\_Create Response (IP address of the EASDF) and with information allowing later the SMF to update or delete the context.

 The IP address of the EASDF is the address which is to be used by the UE to reach the EASDF as a DNS Server for the PDU Session.

5. The SMF includes the IP address of the EASDF as DNS server in PDU Session Establishment Accept message as in step 11 of clause 4.3.2.2.1 of TS 23.502 [3]. The UE configures the EASDF as DNS server for that PDU Session.

Editor's Note: How to guarantee that the UE uses the EASDF's IP address for the subsequent DSN Query in step 8 is FFS.

6. The SMF may invoke Neasdf\_DNSContext\_Update Request (PDU Session Context ID, rules to handle DNS queries from the UE) to EASDF. The update may be triggered by UE mobility, e.g. when UE moves to a new location, or by a reporting by EASDF of a DNS Query with certain FQDN, or, the update may be triggered by insertion/removal of Local PSA, e.g. to update rules to handle DNS messages from the UE or by new PCC rule information.

Editor’s Note: It is FFS whether and how the AF-triggered DNS server information change trigger DNS context update procedure.

7. The EASDF responds with Neasdf\_DNSContext\_Update Response.

8. The UE sends DNS Query message to the EASDF.

9. If the DNS Query message matches the DNS message reporting condition for the UE, the EASDF sends the DNS message report to SMF by invoking Neasdf\_DNSContext\_Notify Request.

10. The SMF responds with Neasdf\_DNSContext\_Notify Response.

 For Option A, the SMF may include corresponding ECS option in the response message. For Option B, the SMF may include corresponding local DNS Server IP address in the response message. The EASDF may as well be instructed to simply forward the DNS Query to a pre-configured DNS server/resolver.

Editor’s Note: It is FFS whether it is aligned with the usage of notification in SBI. This behaviour looks like SMF is requesting a message DNS handling rule (i.e. where to forward the DNS message or whether to include ECS option, what to include ECS option.). Normally, the Notification message is just sending ack or nack. The NF service model should be re-visited.

11. The EASDF handles the DNS Query message received from the UE as the following:

- For Option A, the EASDF adds the ECS option into the DNS Query message as specified in RFC 7871[6] and sends it to C-DNS server;

- For Option B, the EASDF sends the DNS Query message to the Local DNS server.

 If neither a reporting nor a forwarding rule provided by the SMF matches the requested FQDN in the DNS Query, the EASDF may simply forward the DNS Query to a pre-configured DNS server/resolver.

12. EASDF receives DNS Responses from the DNS system and determines that a DNS Response can be sent to the UE.

13. The EASDF may send an DNS message reporting information to SMF by invoking Neasdf\_DNSContext\_Notify request including EAS information if the EAS IP address or the FQDN in the DNS Response message matches the reporting condition provided by the SMF.

 The EASDF does not send the DNS Response message to the UE but waits for SMF instructions (in step 14 or step 16).

14. The SMF invokes Neasdf\_DNSContext\_Notify Response service operation.

Editor’s Note: it is FFS whether DNS message handling rule can be transferred in Notify Response message. Otherwise, SMF needs to invoke additional NF service similar to the step 6.

Editor’s Note: Following aspect is FFS: The SMF may send the DNS message handling rule to the EASDF to instruct EASDF whether to buffer the DNS Response.

15. The SMF may perform UL CL/BP and Local PSA selection and insert UL CL/BP and Local PSA.

 Based on received EAS information received from the EASDF and other UPF selection criteria, as specified in clause 6.3.3 in TS 23.501 [2], the SMF may perform UL CL/BP and Local PSA selection and insertion as described in TS 23.502 [3].

16. The SMF invokes Neasdf\_DNSContext\_Update Request (forward DNS response indication).

 The forward DNS response indication is used to indicate the EASDF to forward the cached DNS Response received in Step 12 to UE.

17. The EASDF responds with Neasdf\_DNSContext\_Update Response.

18. The EASDF sends the DNS Response to UE.

##### 6.2.3.2.3 EAS Discovery Procedure with Local DNS Server/Resolver

For the case that the DNS message is to be handled by local DNS resolver/server, the DNS Query is routed to the local DNS resolver/server corresponding to the DNAI where the L-PSA connects. The SMF is provisioned with the local DNS server address based on configuration or per AF request. Based on the operator’s configuration, one of the following options may apply when UL CL/BP and Local PSA have been inserted (during or after PDU Session Establishment):

- Option C: The SMF chooses a local DNS server, and configures it to the UE as new DNS server. SMF may obtain the IP address of the local DNS server via local configuration. The local DNS server is determined based on the DNAI supported by the L-PSA. In addition, the SMF also configures the UL CL with the traffic routing rule (including e.g. Local DNS server address) to route traffic destined to the local DN including the DNS Query messages to the L-PSA. The local DNS server resolves the DNS Query either locally or recursively by communicating with other DNS servers.

- Option D: If the SMF has configured that DNS Queries for an FQDN query can be locally routed on the UL CL, then the subsequent DNS queries for the FQDN will be locally routed to a local DNS proxy. The local DNS proxy receives and handles the DNS Query that is addressing EASDF by replacing the source/target IP addresses of the DNS Query and Response messages as described in step 5 in clause 6.2.3.2.3.

NOTE: Option D assumes that either ULCL steering is based on L4 information (i.e. DNS port number) or ULCL has visibility of the DNS traffic (i.e. FQDN in the DNS Query message). The UPF may be instructed by the SMF to apply different forwarding of non-ciphered UL DNS traffic based on the target domain of the DNS Query. Option D requests modification of destination IP address of DNS messages. Whether this is allowed or not is subject to local regulations. Option D does not apply to DoH or DoT messages.



Figure 6.2.3.2.3-1: EAS discovery with local DNS server/resolver

1. The SMF inserts UL CL/BP and Local PSA.

 UL CL/BP/Local PSA insertion can be triggered by DNS messages as described in clause 6.2.3.2.2. Or, the SMF may pre-establish the UL CL/BP and Local PSA before the UE sends out any DNS Query message. The UL CL/BP and Local PSA are inserted as described in TS 23.502 [3].

 When the UL CL/BP and Local PSA are inserted, the SMF configure the UL CL/BP for DNS Query handling:

- For Option C, the SMF configures the UL CL/BP with the traffic routing rule (including e.g. Local DNS server address) to forward UE packets destined to the local DN to the Local PSA. The packets destined to local DN includes DNS Query messages destined to local DNS Server.

Steps 2 and 3 are performed for option C:

2. The SMF sends PDU Session Modification Command (Local DNS Server Address) to UE.

 If, based on operator’s policy, the Local DNS Server IP Address in the local Data Network needs to be notified to UE, the SMF sends PDU Session Modification Command (Local DNS Server Address) to UE.

3. The UE responds with PDU Session Modification Complete.

 The UE configures the Local DNS Server as DNS server for the PDU Session. The UE sends the following DNS Queries to the indicated Local DNS Server.

4. UE sends a DNS Query message.

5. The DNS Query message is forwarded to the local DNS Server and handled as described in following:

- For Option C, the target address of the DNS Query is the IP address of the Local DNS Server. The DNS Query is forwarded to the Local DNS Server by UL CL/BP and Local PSA.

- For Option D:

a. The local DNS proxy modifies the packet's destination IP address (corresponding to EASDF) to that of the L-DNS and stores the original IP address (EASDF-IP) and the packet's source IP address (corresponding to UE's IP address) to its own (i.e. the local DNS resolver's) IP address and stores the original source IP address (UE-IP) for later processing.

b. The local DNS proxy then forwards the modified DNS Query to the L-DNS and processes as follows:

- If the L-DNS can resolve the IP address for the requested FQDN of EAS, it responds to the local DNS proxy with the desired IP address of the local EAS.

- If the L-DNS cannot resolve the IP address for the requested FQDN of EAS but it is connected to a C-DNS, it communicates with the C-DNS to recursively resolve the EAS IP address.

6. The Local PSA receives DNS Response message from local DNS server, it forwards it to the UL CL/BP, and the UL CL/BP forwards the DNS Response message to UE.

#### 6.2.3.3 EAS Re-discovery Procedure at Edge Relocation

Editor’s Note: This clause also describes rediscovery (UE based), and aspects and assumptions based on applicable clause 9.2.2 in the TR.

For PDU Session with Session Breakout connectivity, the UE may need to re-discover the EAS after the insertion/change/removal of an L-PSA.

This procedure is used by the SMF to trigger the EAS rediscovery procedure when a new connection to EAS need to be established. It applies to both Session Breakout using ULCL and Session Breakout using BP.

Editor’s Note: It is FFS whether the same procedure is needed for change of SSC mode 3 PSA with IPv6 multi-homing scenario. For this scenario, the UE’s IPv6 prefix can be released with the existing procedure, therefore, the UE is aware when to release DNS cache if needed.

Figure 6.2.3.3-1: EAS re-discovery procedure at Edge relocation

During a previous EAS Discovery procedure on this PDU Session the UE may have cached EAS information (i.e. EAS IP address corresponding to an EAS FQDN) locally, e.g. during the previous connection with the EAS (for more information see Annex C UE considerations for EAS (re)discovery).

1. Due to the UE mobility the SMF triggers L-PSA insertion, change or removal for the PDU Session, the UP management event notifying to the AF may trigger the EAS relocation.

1a. The AF triggers EAS relocation e.g. due to EAS load balance or maintenance, etc, and informs the SMF the related information.

2. The SMF executes the network requested PDU Session Modification procedure from the step 3b-11b as defined in clause 4.3.3.2 TS 23.502 [3]. The SMF makes the decision to indicate the EAS rediscovery to the UE based on information provided by AF or based on SMF's local configuration.

Editor’s Note: It is FFS for the detail information provided by the AF.

 The SMF sends PDU Session Modification Command (EAS rediscovery indication, [impact field]) to UE. The impact field is used to identify which EAS(s) need to be rediscovered. If the impact field is not included, it means all EAS(s) associated with this PDU Session need to be rediscovered.

Editor’s Note: Which information that is used by SMF to compose the optional impact field and how that is provisioned to SMF is FFS.

 For the following connection with the EAS(s) for which the EAS rediscovery need be executed per the received EAS rediscovery indication and impact field, the UE does not use the old EAS information stored locally. Instead it triggers EAS discovery procedure to get new EAS information as defined in clause 6.2.3.2.

NOTE 1: The active connection(s) between the UE and the EAS(s) are not impacted.

Editor’s Note: Whether interaction between the 5GS and application layer DNS cache for EAS rediscovery is required or not is FFS.

### 6.2.4 Support of AF Guidance to PCF Determination of Proper URSP Rules

This clause describes how an Edge Computing related AF may send guidance to PCF determination of proper URSP rules to send to the UE.

NOTE 1: This clause can apply in all deployment models.

An AF related with Edge computing may need to guide PCF determination of proper URSP rules. The guidance sent by the AF may apply to any UE or to a set of UE(s) e.g. identified by a Group Id. The AF may belong to the operator or to a third party.

NOTE 2: Some examples of the delivery of such AF guidance are shown in Annex D.

An AF may deliver such guidance to the PCF via application guidance for URSP determination mechanisms defined in TS 23.502 [3] clause 4.15.6.x. This mechanism is defined only to deliver the guidance to a PCF of the HPLMN of the UE.

The usage of such guidance for URSP generation is defined in TS 23.503 [4] clause 6.6.2.2.

The PCF may use the different guidance received from different AFs and local operator policy to determine the URSP to send to a UE.

## Editor's Note: Whether including Route Selection Validation Criteria in the URSP is sufficient for the UE and/or Network to restrict access to specific (DNN, S-NSSAI) to certain locations is FFS.6.3 Edge Relocation

### 6.3.1 General

### 6.3.2 Edge Relocation Triggered by AF

Editor’s Note: this clause refers to TS 23.502 for procedures addressing the multiple AF scenario (e.g. central and distributed AFs for EC) like AF relocation at Edge relocation proposed in clause 9.2.6, and AF provide DNAI and target N6 info to the SMF as concluded in 9.2.3 in TR.

### 6.3.3 Edge Relocation Using EAS IP Replacement

Editor’s Note: This clause describes seamless change of Edge AS using address replacement in the UPF to keep the UE unaware of the EAS change as in clause 9.2.5.

EAS IP replacement enables the local PSA UPF to replace the source EAS IP address and port number with the target/new target EAS IP address and port number for the Destination IP address and Destination Port number field of the uplink traffic and replace the target/new target EAS IP address and port number with the source EAS IP address and port number for the Source IP address and Source Port number field of the downlink traffic based on the enhanced AF Influence information for EAS IP replacement (i.e. Support of EAS IP Replacement Capability, source EAS IP address and port number, target EAS IP address and port number). The source AS IP address and port number are the destination IP address and port number of the uplink traffic, generated by UE, for a service subject to Edge Computing. The source EAS IP address is the one discovered by UE for a service subject to Edge Computing.

EAS IP replacement requires support of TCP/TLS/QUIC context transfer between EAS.

NOTE 1: The feasibility of this requirement, i.e. TCP/TLS/QUIC context transfer between EAS, is unclear and whether third party platforms would support this TCP/TLS/QUIC context transfer between EAS is unknown/not clear.

#### 6.3.3.1 EAS IP Replacement Procedures

##### 6.3.3.1.1 Enabling EAS IP Replacement Procedure



Figure 6.3.3.1.1-1: Enabling EAS IP Replacement Procedure

NOTE 1: This procedure covers the scenarios that the UE moves from non-EC to EC or the AF decides to enable the EAS IP replacement in the middle of a session.

1. UE requests to establish a PDU Session.

2. UE is preconfigured with the Source EAS IP address or discovers the IP address of the application server for the service subject to Edge Computing, and the Source EAS IP address is returned to the UE via EAS Discovery procedure.

3. UE communicates with the Source EAS.

4. AF detects that the EAS is capable of runtime context minoring and an optimal EAS is found, then AF decides to influence the traffic routing in 5GC. The EAS IP replacement information (i.e. Support of EAS IP Replacement Capability, source EAS IP address and port number, target EAS IP address and port number) is sent to the SMF within the AF Influence information and the SMF reconfigures the UL CL UPF and Local PSA with EAS IP replacement information. Or when UE moves to an area where the Local PSA has been configured to enforce EAS IP address replacement.

 UL CL is configured by SMF to forward the destination IP address in the UL packet equals to the Source EAS IP address to Local PSA.

 Local PSA is configured by SMF to enforce the "Outer Header Creation" and " Outer Header Removal" as described in step 6. FARs "Outer Header Creation" and " Outer Header Removal" are reused for such an instruction from SMF to UPF.

 Detailed enhancement to the AF Influence procedure is described in clause 6.3.3.2.

5. Early Notification procedure with enhancement described in clause 6.3.3.2 is triggered, SMF notifies AF about the target DNAI. Based on the target DNAI, the AF selects a proper target EAS, then the AF triggers to mirror the runtime context between Source EAS and Target EAS. Once the Target EAS is ready, AF responds to SMF about the Target EAS IP information (i.e. Target EAS IP address and port number). SMF reconfigures Local PSA for EAS IP address replacement between Source EAS and Target EAS.

6. Local PSA starts to perform "Outer Header Creation" and " Outer Header Removal" FARs as instructed by SMF, which results in EAS IP address replacement:

- For UL traffic, the destination IP address and port number are replaced with the Target EAS IP address and port number at Local PSA;

- For DL traffic, the source IP address and port number are replaced back with the Source EAS IP address and port number at Local PSA.

NOTE 2: In this solution, the PSA UPF need not to understand the logic of EAS IP replacement.

7. Late Notification procedure with enhancement described in clause 6.3.3.2 is triggered, SMF notifies AF about the start of the EAS IP replacement.

 Then all subsequent uplink traffic of this EC service for this UE is forwarded to the target EAS.

NOTE 3: AF decides when and how to stop the Source EAS from serving the UE based on its local configuration.

##### 6.3.3.1.2 EAS IP Replacement Update upon DNAI and EAS IP Change



Figure 6.3.3.1.2-1: EAS IP Replacement Update upon DNAI and EAS IP change

1. For UL traffic, the destination IP address is replaced with the old Target EAS IP address at Local PSA; for DL traffic, the source IP address is replaced back with the Source EAS IP address at Local PSA.

2. When Early Notification happens, the SMF notifies AF about the target DNAI. Based on the target DNAI, the AF selects a proper new target EAS, then the AF initiates runtime session context migration from the old Target EAS to the new Target EAS. When the resource in the new Target EAS is ready, the AF responds with the new Target EAS IP address and port number to SMF. SMF decides whether to relocate UL CL and Local PSA and configures the EAS IP address replacement using "Outer Header Creation" and " Outer Header Removal" in Local PSA2 if PSA relocation happens.

3. Local PSA2 starts to perform "Outer Header Creation" and " Outer Header Removal" FARs as instructed by SMF, which results in EAS IP address replacement:

- For UL traffic, the destination IP address and port number are replaced with the new Target EAS IP address and port number at Local PSA;

- For DL traffic, the source IP address and port number are replaced back with the Source EAS IP address and port number at Local PSA.

4. Late Notification procedure with enhancement described in clause 6.3.3.2 is triggered, SMF notifies AF about the start of the EAS IP address replacement towards the new Target EAS.

NOTE 1: AF decides when and how to stop the old Target EAS from serving the UE based on its local configuration.

##### 6.3.3.1.3 Disabling EAS IP Replacement Procedure



Figure 6.3.3.1.3-1: Disabling EAS IP Replacement Procedure

1. Local PSA performs "Outer Header Creation" and " Outer Header Removal" FARs as instructed by SMF, which results in EAS IP address replacement:

- For UL traffic, the destination IP address and port number are replaced with the old Target EAS IP address and port number;

- For DL traffic, the source IP address and port number are replaced back with the Source EAS IP address and port number.

2. Due to UE Mobility to a Non-EC environment, Early Notification is triggered, target DNAI is set to empty value, AF knows the UE moves out of EC environment and mirrors the runtime session context from old Target EAS to Source EAS. Once ready, the AF indicates SMF to disable the local routing at UL CL and the EAS IP replacement at Local PSA for this PDU Session.

3. UL and DL traffic goes through Remote PSA, no EAS IP address replacement happens at Remote PSA.

NOTE 1: AF decides when and how to stop the old Target EAS from serving the UE based on its local configuration.

#### 6.3.3.2 Enhancement to AF Influence

The AF may additionally include the capability indication for Support of EAS IP Replacement, Source and Target EAS IP address(es) and Port number(s) in the Nnef\_TrafficInfluence\_Create/Update request. Based on the Source EAS IP address(es), the SMF knows which service flow(s) is(are) subject to EAS IP Replacement.

SMF sends the "Outer Header Creation" and " Outer Header Removal" FARs to Local PSA UPF as described in step 6 of clause 6.3.3.2, and Local PSA UPF starts the EAS IP address replacement as described in clause 6.3.3.1. Then the SMF needs to notify AF about the start of EAS IP replacement using Late Notification procedure.

For load balancing purpose, the AF may move some UE(s) from the old Target EAS) to the New Target EAS in the same local DN identified by the DNAI. For the abnormal condition of EAS, the AF may move all the UEs being served by the source EAS to a target EAS in the same local DN. For this purpose, the AF needs to include the capability indication for Support of EAS IP Replacement, List of impacted UE IP address and port number, the old Target EAS IP address and port number for the impacted DNAI, the new Target EAS IP address and port number for the impacted DNAI in the Nnef\_TrafficInfluence\_Create/Update request.

The additional parameters for enabling the EAS IP Replacement are defined in clause 5.6.7.1 of TS 23.501 [2], clause 4.3.6.3 and 4.3.6.4 of TS 23.502 [3].

### 6.3.4 Simultaneous Connectivity for Source and Target EASs

Editor’s note: This clause describes seamless change of Edge AS using simultaneous connectivity for source and target EAS to reduce latency and packet loss. Whether this clause is needed is TBD based on actual contribution inputs.

### 6.3.5 Packet Buffering for Low Packet Loss

Editor’s Note: This clause describes seamless change of Edge AS using buffering of packets as in clause 9.2.1 to reduce packet loss.This procedure aims at synchronizing between EAS relocation and UL traffic from the UE, ensuring that UL traffic from the UE is sent to the new EAS only when EAS context transfer has been carried out.

This procedure may be applied at change of local PSA. It consists of buffering uplink packets in the target PSA in order to prevent there is packet loss if the application client sends UL packets to a new EAS before the new EAS is prepared to handle them. During the buffering, the old EAS may continue to serve the UE over the former PSA.

Buffering starts upon request by AF and continues till AF indicates otherwise. The EAS relocation procedure (e.g. the migration of the service context) happens at the application layer. That is outside the scope of 3GPP.

As an alternative to this procedure, upper layer solutions can provide the needed synchronization between EAS relocation and UL traffic from the UE.

NOTE: Upper layer solutions may still be needed when there are other EAS relocation scenarios (e.g. EAS (re)selection upon DNS cache entry expiry) not related to PSA change.

Buffering of uplink packets is not meant to apply to all traffic being offloaded at the new PSA but to the traffic identified by the application the rule associated with the buffering request.

Editor’s Note: Whether Buffering of uplink packets applies to an application traffic depends on the application requirement. It is FFS how to consider the application priorities and apply buffering with the right granularity.



Figure 6.3.5-1: Packet buffering for low packet loss

1. The SMF decides to change the local PSA of a PDU Session with UL CL.

2. The SMF may send an early notification to the AF after target PSA (i.e. PSA2) is selected and waits for a notification response from the AF. The AF may reply in positive to the notification by indicating that buffering of uplink traffic to the target DNAI is needed as long as traffic to the target DNAI is not authorized by the AF . This is e.g. as defined in Steps 1 and 2 of TS 23.502 [3] Figure 4.3.6.3-1.

3. The SMF configures the PSA2 as specified in step 2 in clause 4.3.5.6 and step 2 in clause 4.3.5.7 of TS 23.502 [3], which may request the PSA2 to buffer uplink traffic. The PSA1 (i.e. source PSA) keeps receiving downlink traffic from EAS1 and send it to the UE until it is released in step 7.

4. The SMF sends an N4 Session Modification Request to the UL CL to update the UL CL rules regarding to the traffic flows that the SMF tries to steer to PSA2..This is e.g. as defined in TS 23.502 [3] Figure 4.3.5.7-1 step 3

5. The SMF sends a Late Notification to the AF. This corresponds e.g. to step 4a-c of TS 23.502 [3] Figure 4.3.6.3-1 and is also described in step 6 or 7 of TS 23.502 [3] Figure 4.3.5.7-1.

6a A new EAS is selected by the application (e.g. at DNS cache entry expiry, the DNS Query is resolved and the response includes a new EAS that is near the new PSA (PSA2)). Any traffic sent to the new EAS is buffered at PSA2.

6b. The application layer completes the EAS relocation (This corresponds to step 4d of TS 23.502 [3] Figure 4.3.6.3-1). The UE context is completely relocated from the old EAS to new EAS. The old EAS stops to serve the UE

NOTE 2: 6a and 6b are related which implies there is some sort of coordination at application layer that is outside of 3GPP scope.

7. When EAS relocation is completed, the AF sends a notification response to the SMF. This corresponds to step 4e-g of TS 23.502 [3] Figure 4.3.6.3-1(and is e.g. also described in step 6 or 7 of TS 23.502 [3] Figure 4.3.5.7-1) and may indicate that buffering of uplink traffic to the target DNAI is no more needed as traffic to the target DNAI /EAS is now authorized by the AF.

8. (if AF has indicated that buffering of uplink traffic to the target DNAI is no more needed as traffic to the target DNAI /EAS is now authorized by the AF) The SMF updates the PSA2 by indicating the PSA2 to send the buffered uplink packets (step 8b) and to stop buffering.

 The SMF releases PSA1.

### 6.3.6 Edge Relocation Considering User Plane Latency Requirement

Edge relocation may be performed considering user plane latency requirements provided by the AF.

In a network deployment where the estimated user plane latency between the UE and the potential PSA-UPF is known to the SMF, the 5GC provides the enhancement of AF influence to consider the user plane latency requirements requested by the AF so that the SMF decides to relocate the PSA-UPF based on AF requested requirements.

The AF may provide user plane latency requirements to the network via AF traffic influence request as described in TS 23.502 [3], clause 5.2.6.7. The user plane latency requirements may include the following information:

- Maximum allowed user plane latency: The value of this information is the target user plane latency. The SMF may use this value to decide whether edge relocation is needed to ensure that the user plane latency does not exceed the value. The SMF may decide whether to relocate the PSA UPF to satisfy the user plane latency.

- User plane latency preference: This parameter denotes AF preference for the user plane latency. The SMF may decide to (re-)select the PSA UPF considering this parameter.

Editor’s Note: It is FFS whether this parameter indicates “an indicator denoting the shortest user plane latency preference” or “a value for minimum user plane latency”.

The user plane latency requirements requested by AF is informed to the SMF via AF influenced Traffic Steering Enforcement Control (see TS 23.503 [4] clause 6.3.1) in PCC rules. After receiving the user plane latency requirements from AF via PCF, the SMF may take appropriate actions to meet the requirements e.g. by reconfiguring the user plane of the PDU Session as described in the step 6 of Figure 4.3.6.2-1 in TS 23.502 [3].

## 6.4 Network Exposure to Edge Application Server

### 6.4.1 General

Editor’s Note: This clause describes how to expose information that needs to be delivered timely to applications deployed in edge hosing environments. This clause refers to TS 23.501, TS 23.502 and TS 23.503 for detailed exposure procedures including the enhancements proposed in TR 23.748 clause 9.4. Privacy considerations might be addressed as well.

Editor’s Note: New clauses 6.4.x may be added later for alternative solutions described in NOTES in 9.4 based on input contributions.

Some real time network information, e.g. user path latency, are useful for application layer. In this release, in order to expose network information timely to local AF, the L-PSA UPF may expose network information i.e. QoS monitoring results as defined in TS 23.501 [2], clause 5.33.3, to the local AF.

NOTE 1: Local PSA UPF can expose the QoS monitoring results to local AF via N6. How to deliver the information on N6 is out of SA2 scope.

### NOTE 2: Sending QoS monitoring information that has not been properly integrated over time, i.e. with over-high frequency, can increase risk that the application may over-react to instantaneous radio events/conditions e.g. leading to service instability.6.4.2 Network Exposure to Edge Application Server via Local NEF

Editor’s Note: This clause describes network exposure via local NEF as described in bullets in TR 23.748 clause 9.4.

Local NEF deployed at the edge may be used to support network exposure timely to local AF. The local NEF may support one or more of the functionalities described in TS 23.501 [2] clause 6.2.5.0. and may support a subset of the APIs specified for capability exposure based on local policy. In order to support the network exposure locally, the local NEF shall support event exposure service operation to the local AF. The local NEF selection by AF is described in TS 23.501 [2] clause 6.2.5.0 and 6.3.14.

The local AF subscribes the low latency exposure of QoS Monitoring results to PCF via a local NEF or NEF. The local AF may also subscribe the events via PCF directly. Based on the indication of local event notification and operator's policy, the PCF may include an indication of local event notification (including target local NEF address) within the PCC rule that it provides to the SMF.

The SMF sends the QoS monitoring request to the RAN and N4 rules to the L-PSA UPF. N4 rules may indicate the service data flow needs local notification of QoS Monitoring. When GTP-U Path monitoring is used for QoS monitoring, that is also activated if needed. This is as defined in TS 23.501 [2] clauses 5.33.3. When N4 rules indicate the service data flow needs local notification of QoS Monitoring, upon the detection of the QoS monitoring event, the L-PSA UPF sends the notification to the AF via Local NEF.

During UE mobility, the SMF may trigger the L-PSA UPF relocation/reselection and then send the N4 rules to the new L-PSA UPF to indicate the service data flow needs local notification of QoS Monitoring. The UE mobility may also trigger AF relocation or local NEF reselection, then the local AF should update the subscription for local exposure with QoS monitoring results via local NEF, towards the PCF. This updated /new subscription is then propagated via SMF (via PCC rule updates) and then to the L-PSA UPF via N4 rules.

Figure 6.46.2-1: The association establishment between local UPF and local NEF

0. The UE establishes a PDU Session as defined in clause 4.3.2.2.1 of TS 23.502 [3] A Local PSA is used by this PDU Session.

1. The AF initiates an AF session with required QoS procedure as defined in clause 4.15.6.6 of TS 23.502 [3].

 In the request, the AF may subscribe local notification of QoS monitoring to PCF via Local NEF or NEF. For the QoS monitoring, the AF shall include the corresponding QoS monitoring parameters as defined in clause 5.33.3 of TS 23.501 [2].

 The local AF may find a local NEF based on existing method as in TS 23.501 [2] clause 6.2.5.0 and parameters in clause 6.3.14. The indication for AF request network real-time information is also provided.

Editor’s Note: The local NEF discovery is still FFS.

 The AF may also first initiate an AF Session with PCF and later subscribe to local notification of QoS monitoring to PCF by invoking Npcf\_Authorization\_Subscribe service operation.

Editor’s Note: how to handle the duplicated subscription (via both SMF->PCF->NEF and UPF->NEF) is FFS.

2. The PCF makes the policy decision and initiates the PDU Session modification procedure as defined in clause 4.3.3.2 of TS 23.502 [3], step 1b, 3b, 4-8b. If the local notification of QoS monitoring is subscribed, the PCF includes the indication of local event notification (including target local NEF address) within the PCC rule. The SMF sends local QoS monitoring parameters to the L-PSA UPF via N4 rules.

3. The L-PSA UPF obtains QoS monitoring information as defined in TS 23.501[2] clause 5.33.3.

4. The L-UPF sends the notification related with QoS monitoring information over Nx

Editor’s Note: it is FFS whether the QoS monitoring result report from L-PSA UPF to local NEF is based on SBI or not.

5. Local NEF reports the real-time network information to local AF through Nnef\_EventExposure\_Notify.

6. Due to e.g. UE mobility, the PSA relocation and/or EAS relocation may happen as described in clause 6.3.

7. The new AF may initiate a new AF session to the new Local NEF or NEF/PCF to (re-)subscribe the local notification of QoS monitoring as described in steps 2-4.

8. The old AF revokes the AF session with the old local NEF or NEF/PCF.

## 6.5 Support of 3GPP Application Layer Architecture for Enabling Edge Computing

### 6.5.1 General

Editor’s Note: This clause refers to TS 23.558 for the specifications of the Discovery over the Architecture Enabling Edge Applications.

The 3GPP application layer architecture that is specified in TS 23.558 [5] includes the following functional entities:

- Edge Enabler Client (EEC)

- Edge Configuration Server (ECS)

- Edge Enabler Server (EES)

A UE may host EEC(s) as defined in TS 23.558 [5] and support the ability to receive ECS address(es) from the 5GC and to transfer the ECS address(es) to the EEC(s). In this case, the ECS address provisioning via 5GC is described in clause 6.5.2.

### NOTE: The features described in the other clauses of this specification do not require the UE and the network to support the 3GPP application layer architecture that is specified in TS 23.558 [5].6.5.2 ECS Address Provisioning

Editor’s Note: This clause describes here the procedure agreed in conclusions in 9.1.3.

If the UE hosts an EEC and supports transferring the ECS address received from the 5GC to the EEC, the UE indicates in the PCO at PDU Session establishment or modification that it supports the ability to receive ECS address(es) via NAS and to transfer the ECS Address(es) to the EEC(s).

The ECS Address Configuration Information consists of one or more FQDN(s) and/or IP Address(es) of Edge Configuration Server(s). As described in clause 4.3.2 in TS 23.502 [3], if the UE supports the ability to receive ECS address(es) via NAS and to transfer the ECS Address(es) to the EEC(s), the UE may receive ECS Address Configuration Information from the SMF via PCO during PDU Session Establishment and/or during PDU Session modification procedures. The SMF may derive the ECS Address Configuration Information based on local configuration, the UE's location, and/or UE subscription information. The SMF may decide to send updated ECS Address Configuration Information to the UE based on locally configured policy, updated UE subscription information, or a change of UE location. The PDU Session Modification procedure is used to send updated ECS Address Configuration Information to the UE as described in clause 4.3.3 in TS 23.502 [3].

NOTE: In home routed sessions, the ECS Address Configuration Information comes from the H-SMF.

#### 6.5.2.1 ECS Address Provisioning by a 3rd Party AF

As described in TS 23.558 [5], the Edge Configuration Server can be deployed in the MNO domain or can be deployed in a 3rd party domain by a service provider. If the ECS is deployed in a 3rd party domain by a service provider, a 3rd party AF can use Nnef\_ParameterProvision to provide, update, or delete ECS Information for a UE (See TS 23.502 [3], clause 4.15.6.2).

When the AF uses Nnef\_ParameterProvision to send a new ECS Address Information to the UDM for a UE (e.g. because on Application layer activity, change of UE location, etc.), the UDM may notify the SMF of the updated ECS Address Information and the new ECS Address Information will be sent to the UE in a PDU Session Modification procedure.

Editor’s Note: It is FFS for multiple ECS address configuration information.

Editor’s Note: It is FFS whether the 3rd party AF would know the GPSI; the possibility to configure the ECS address for all UE in one operation should be considered.

Editor’s Note: Potential signalling overload is FFS When the AF uses Nnef\_ParameterProvision to send a new ECS Address Information to the UDM for many UE.

# 7 Network Function Services and Descriptions

Editor’s Note: TBD, this clause is a placeholder for any necessary new Services to be defined in this TS.

Annex A (Informative):
EAS Discovery Using 3rd Party DNS Server

Editor's Note: This is to address the case that operator's DNS setting is overrided by user/application and 3rd party DNS/DoH server is used. sol #14-like solution in TR.

There are different IP discovery mechanisms existing in the application layer. For example, the application client can generate the DNS Query outside of DNS libraries in the OS with DoT, DoH or other over the top mechanisms.

The third party can also deploy a service scheduling server to determine the (E)AS IP address based on the UE’s HTTP(S) request. In this case, the DNS firstly resolves the FQDN in the DNS request of the UE into the IP address of the service scheduling server and then the UE contacts the service scheduling server that can provide the IP address of the EAS that the UE is then to contact.

For the Distributed Anchor Point connectivity model, in order to enable EAS discovery by third party mechanisms, the DNS Server or service scheduling server in the third party could be pre-configured with mapping information between the IP address range which can correspond to the Central PSA UPF or other entities (e.g., a NAT server) on the N6 interface and EAS information. In this case, the DNS Server or service scheduling server in the third party can take the source IP address of the UE request as the location information of UE. The DNS and/or service scheduling server pre-configuration can be based on the agreement between the MNO and service provider.

For the Session Breakout connectivity model, based on agreement with the operator, a possible solution for the service scheduling server is as follows:

- The IP address of the service scheduling server can be set as a condition in the ULCL UPF to offload traffic. The IP address of service scheduling server can be pre-configured or resolved by the EASDF based on procedure defined in clause 6.2.2.2.

- NAT server can be deployed in the local DN or local N6 interface, in order that the source IP address of the UE request sent to the service scheduling server can correspond to the UE location related information.

NOTE: Otherwise, the source IP address of the UE request message sent to the third party DNS server / service scheduling server is bound with the central PSA UPF, so it’s impossible for the third party DNS server / service scheduling server to know which local EAS address could be allocated to the UE.

Based on the mapping relationship between the IP ranges of UE request and the EAS information, the EAS IP address can be allocated to the UE. The above example is briefly shown in Figure A-1.

Service scheduling server

Application Server

Local DN

DNS Server

I-UPF

Central PSA UPF

Local PSA UPF

UE

EAS

1.DNS request

2.DNS response (IP address of Service scheduling server)

3.HTTP request

4.HTTP response (EAS address)

5.HTTP request /response

Central DN

Figure A-1: Service scheduling server mechanism for Session Breakout connectivity model

Annex B (Informative):
Application Layer based EAS (Re-)Direction

Editor's Note: This is to address application layer based EAS rediscovery procedure as concluded in 9.2.3 in TR.

During the application relocation, the AF can reselect a new EAS for the UE. Reselection can be triggered by the AF when it receives a UP path change notification or by an internal trigger of the AF (e.g. load balancing, UE location change, etc.). When the new EAS is reselected, the UE is provided the new EAS address via application layer signalling. For example, the UE can receive the URL or FQDN of the new EAS once the application context relocation is complete and then use DNS to resolve the URL or FQDN. The UE can also obtain the new EAS address via HTTP redirection.

NOTE: The Application layer signalling between the AF (or Old EAS) and UE is application specific and is outside the scope of this specification.

Annex C (Informative):
UE Considerations for EAS (re)Discovery

C.1 General

DNS records obtained from a network resolver contains a time-to-live (TTL) value. This is a hint provided by the network resolver and can be used to determine the length of time that the record is cached. DNS records can be cached in the UE by a system wide stub resolver and by application layer name resolution caches. The application (L7) cache is managed on a per application basis while the OS/system DNS cache is common to applications. Name resolution caches in various applications also have different policies and behaviour. Some applications cache the name records for the length of the application session while others have a time limit.

Editor’s Note: Whether coordination across the 5GC and application domain for name resolver caching behaviour is required or not is FFS.

The following clauses describe the appropriate DNS configuration for the EAS (re)-discovery to work in the UE.

C.2 Impact of IP Addresses for DNS Resolver

The UE can be configured by the 5GC with an IP address for the DNS resolver using ePCO or IPv6 Router Advertisement (RA). 5GC can reconfigure the DNS resolver IP address. In case of anycast IP address of the DNS resolver, the 5GC can use UL-CL/BP to branch out and the DN is responsible to route to the closest instance of the MNO DNS resolver without having to reconfigure the DNS resolver IP address in the UE.

Applications in the UE can request the DNS resolver configured on the UE to resolve an FQDN. However, applications can also be configured with their own DNS resolver address and can use encrypted messaging based e.g., on DNS over HTTPS (DoH) or, DNS over TLS (DoT). Configuration of application DNS resolvers is out of scope of 5GC. DNS messages delivered over DoT, or DoH might be forwarded transparently to the destination address of DNS resolver in the DNS query. The application DNS resolver can be operated by the 5GC operator or by a third party.

A network interface change or NAS SM EAS rediscovery indication can result in the UE OS clearing name/IP address translations in its DNS cache. If network interface change or NAS SM EAS rediscovery indication does not result in the UE OS clearing name/IP address translations in its DNS cache, an application can continue the L4 connection with the old EAS IP address until DNS cache entry times-out and subsequent DNS EAS address resolution request.

C.3 UE Considerations for EAS Re-discovery

An application in the UE that complies with EAS (re-)discovery described in this specification is not recommended to override operator-provided DNS settings.

The OS DNS server configuration does not override the operator provided DNS in a UE compliant to the EAS (re-)discovery procedure. This is necessary for the “closest” EAS server to be selected.

NOTE 1: If an OS, user or applications override the operator-provided DNS settings, the DNS resolvers or servers in the third party can take the source IP address of the DNS request as the location information of UE, which can correspond to the remote PSA UPF or other entities (e.g., a NAT server) on the remote/central N6 interface which can lead to a non-optimal choice of the EAS server address.

NOTE 2: If the DNS server configuration in a OS overrides the operator provided DNS, the DNS queries continue to be sent over the correct PDU Session for the application.

NOTE 3: The UE modem transparently forwards DNS messages for tethered devices that are loosely coupled.

NOTE 4: If the UE (OS or application) uses a DNS resolver that is different than the one provided by the 5GC, then:

- the Session Breakout connectivity mode, option A and B in 6.2.3.2 will not work in case the EASDF is NOT in the DNS resolver chain for recursive DNS resolution.

C.4 UE Procedures for Session Breakout

In the session breakout connectivity model, the selection of a new session breakout path does not result in a new network interface indication at the UE.

NOTE 1: In case of multiple sessions or distributed anchor point connectivity models, when there is a change of network interface, indication of network interface change can be used to flush the UE OS DNS cache.

Session breakout results in a NAS SM message indicating the need to redo DNS lookup sent by the SMF to the UE modem. Thus, in order to support some solutions of this specification, it is necessary for the operating system to receive information of EAS rediscovery from the modem when such signalling has been received and clear the DNS cache in UE OS.

Annex D (Informative):
Examples of AF Guidance to PCF for Determination of URSP Rules

a) The UE is to use a specific (DNN, S-NSSAI) (e.g. working in SSC mode 2 or 3 with the Distributed Anchor deployment) when trying to reach some domains while it should use another (DNN, S-NSSAI) (e.g. working in SSC mode 1) for other domains. In this example, the AF can indicate two FQDN filters, optionally with corresponding filtering rule priorities, if the FQDN filters overlap. For each FQDN filter, the AF can indicate a corresponding DNN, S-NSSAI.

b) Corporate applications only reachable via a specific (DNN, S-NSSAI) negotiated with the operator; corresponding URSP rules (URSP rules referring to domains of these corporate applications) shall only point to this specific (DNN, S-NSSAI). In this example, the AF can indicate one FQDN filter for the corporate applications. Optionally, the AF can indicate also the corresponding DNN, S-NSSAI for the FQDN filter. If DNN, S-NSSAI is not provided by the AF, the NEF can determine it based on the AF identity.

c) Corporate applications reachable via a (DNN, S-NSSAI) but only in some location (DNAI) ; e.g. the corporate applications are only accessible when the UE is in some location corresponding to the corporate premises. In this example, the AF can provide information as in bullet b), and additionally provides DNAI or geographical zone identifier where the corporate applications are accessible. URSP Rules will guide the UE select the (DNN, S-NSSAI) when the UE is in the geographical zone.

d) Internet applications not reachable via a specific (DNN, S-NSSAI) negotiated with the operator but that should be only reachable via a general purpose (DNN, S-NSSAI); e.g. traffic of UE(s) of a third party targeting Internet applications is not to be sent to a specific (DNN, S-NSSAI) negotiated with the operator as this traffic is not expected to cross the Intranet of the corporate. In this example, the default operator rules are used generate a “match all” URSP rule with a low filtering rule priority and a corresponding generic purpose DNN, S-NSSAI.

e) Internet applications reachable via both a specific (DNN, S-NSSAI) negotiated with the operator and via a general purpose (DNN, S-NSSAI) for which the third party may want to set preferences between these 2 kinds of connectivity. These preferences may depend on the UE location. In this example, the AF can indicate FQDN filters as in bullet b), but the FQDN filters are for Internet applications. In addition, the AF can indicate the DNAI or geographical zone identifier where the Internet applications are accessible via the specific DNN, S-NSSAI. In addition, the default operator rules are used generate a “match all” URSP rule with a low filtering rule priority and a generic purpose DNN, S-NSSAI.

f) Combination of bullets c) and e). In this example, the AF can indicate one FQDN filter for corporate applications as in bullet c), and another FQDN filter for Internet applications as in bullet c), In addition, the AF can indicate filtering rule priorities for the FQDN filters, if the FQDN filters overlap.

g) Corporate applications reachable via a (DNN, S-NSSAI) in some location (DNAI) and via another DNN, S-NSSAI in another location; e.g. the corporate applications are only accessible via a location specific corporate DNN, S-NSSAI. In this example, the AF can indicate an FQDN filter as in bullet c), but indicates two or more DNAIs for the FQDN filter, and indicates different DNN, S-NSSAI per DNAI. In addition, if the geographical locations of the DNAIs overlap, the AF can indicate a Route Selection Descriptor Precedence for each DNAI.

The examples b) to e) above can correspond to different AF(s) representing different corporate that have different policies. How the rule precedence between rules for different AFs are set in the URSP rules is up to the operator policy.

Annex E (Informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2021-03 | SA2#143E | S2-2100114 | - | - | - | Proposed skeleton approved at S2#143E | 0.0.0 |
| 2021-03 | SA2#143E |  |  |  |  | Incorporate approved P-CR: S2-2101087, S2-2101095, S2-2101097, S2-2101098, S2-2101090, S2-2101104, S2-2102000, S2-2002002, S2-2102003, S2-2102004, S2-2102005, S2-2102007, S2-2102009, S2-2102069 | 0.1.0 |