**3GPP TSG-SA WG2 Meeting #145ES2-2104385**

**Elbonia, 17 - 28 May, 2021**

**Source: Huawei, HiSilicon**

**Title: Local DNS Server Configuration to UE**

**Document for: Agreement**

**Agenda Item: 8.3**

**Work Item / Release: eEDGE\_5GC /Rel-17**

***Abstract of the contribution:*** *This contribution clarify how to select DNS server close to UE’s point of connection.*

# Discussion

For distributed anchor scenario, a local DNS address is configured as DNS server sent to the UE. And the UE sends DNS query to that indicated local DNS server.

This contribution proposes to document this into the new TS, including that the local DNS server is selected based on the UE location and the DNS configuration information provisioned by AF (in case only one EAS in that DNAI).

# Proposal

It is proposed to capture the following changes vs. TS 23.548.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 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.

In Edge Computing deployment, an application service may be served by multiple Edge Application Servers typically deployed in different sites. These multiple Edge Application Servers that host service may use a single IP address (anycast address) or different IP addresses. To start an Edge Application Service, the UE needs to know the IP address(es) of the Application Server(s) serving the Service. The UE may do a discovery to get the IP address(es) of a suitable Edge Application Server (e.g. the closest one), so that the traffic can be locally routed to the Edge Application Server and service latency, traffic routing path and user service experience can be optimized.

EAS Discovery is the procedure by which a UE discovers the IP address(es) of a suitable Edge Application Server(s) using Domain Name System (DNS). EAS Re-discovery is the EAS Discovery procedure that takes place when the previously discovered Edge Application Server cannot be used or may have become non-optimal (e.g. at edge relocation).

NOTE 1: This specification describes the discovery procedure based on 5GS NFs as to ensure the UE is served by the application service closest to the UE's point of attachment. However, this does not exclude other upper layer solution that can be adopted by operator or service provider, like the EAS Discovery procedure defined in TS 23.558 [5], or other alternatives shown in Annex A and Annex B. How those other solutions work, or whether they are able to guarantee the closest application service for the UE, is out of the scope of this specification.

In order to provide a translation of the FQDN of an EAS into the address of an EAS as topologically close as possible to the UE, the Domain Name System may use following information:

- The source IP address of the incoming DNS Query; and/or,

- a EDNS Client Subnet (ECS) option (as defined in RFC 7871 [6]).

NOTE 2: UE IP address can be subject to privacy restrictions, which means that it is not to be sent to Authoritative DNS / DNS Resolvers outside the network operator within ECS option or as Source IP address of the DNS Query. UE source IP address can be protected by using NAT mechanism.

EAS (re-)discovery procedures described in this specification should use the top level domains (TLDs) in the public namespace by default.

If a private namespace is used, an Edge Computing Service Provider (ECSP) should provision DNS information via AF request with its AF-service-identifier, or DNN and NSSAI. Since private namespaces do not have a common root server or naming, the DNS information for each ECSP should be stored individually to prevent any overwriting of resolution entries.

If the UE applications want to discover/access EAS by using the mechanisms defined in this TS, the DNS queries generated by the UE shall be sent to the EASDF as DNS resolver indicated by the SMF.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

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

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).

For the Distributed Anchor Connectivity Model, in PDU Session establishment procedure, the SMF selects a local DNS Server for the PDU Session. The local DNS Server is configured to UE either via PCO or via DHCP. The SMF is provisioned with EAS deployment information, by local configuration or by AF. Based on the EAS deployment information, the DNAI of the PSA of the PDU Session, and local configuration, the SMF determines the local DNS server address for the PDU Session.

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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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 local configuration or based on EAS deployment information in AF request as specified in clause 6.2.3.2.2. 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 based on the DNAI corresponding to the inserted local PSA, EAS deployment information, and local configuration, and configures it to the UE as new DNS server. In addition, the SMF also configures traffic routing rule on the UL CL (including e.g. Local DNS server address) or the BP (e.g. the new IP prefix @ Local PSA) 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 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.

NOTE: Option D assumes that ULCL steering is based on L4 information (i.e. DNS port number) and that 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 (e.g. upon UE mobility). In this case, the SMF includes the IP address of Local DNS Server in PDU Session Establishment Accept message as in step 11 of clause 4.3.2.2.1 of TS 23.502[3] or in a network initiated PDU Session Modification procedure. The UE configures the Local DNS Server as DNS server for that PDU Session.

The UL CL/BP and Local PSA are inserted or changed as described in TS 23.502 [3]. In the case of IPv6 multi-homing, the SMF may also send an IPv6 multi-homed routing rule along with the IPv6 prefix to the UE to influence the selection of the source Prefix for the subsequent DNS queries as described in TS 23.501 [2] clause 5.8.2.2.2.

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

- For Option C, the SMF configures traffic routing rule on the UL CL (including e.g. Local DNS server address) or the BP (e.g. the new IP prefix @ Local PSA) 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. If the UL CL/BP and Local PSA are inserted after PDU Session Establishment, the SMF sends PDU Session Modification Command (Local DNS Server Address) to UE.

If, based on operator's policy or UE’s mobility, the Local DNS Server IP Address in the local Data Network needs to be notified or updated 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 the DNS server for the PDU Session. The UE sends the following DNS Queries to the indicated Local DNS Server.

NOTE 1: The UE does not need to know that the new DNS server is “local”.

4. UE sends a DNS Query message. In the case of IPv6 multi-homing the UE selects the source IP prefix based on the IPv6 multi-homed routing rule provided by SMF.

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. The Local DNS Server resolves the FQDN of the DNS query by itself or communicates with other DNS server to recursively resolve the EAS IP address.

- For Option D: The Local PSA sends the DNS traffic to the Local DNS Server that resolves the FQDN target of the DNS query by itself or that communicates with a C-DNS server to recursively resolve the EAS IP address.

NOTE 2: The Local PSA can send the DNS traffic to the Local DNS Server via tunnelling or via IP address replacement. If IP address replacement is used, the SMF instructs the Local PSA to modify the packet's destination IP address (corresponding to EASDF) to that of the target DNS.

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.

NOTE 3: If IP address replacement has been enforced at step 5, the Local PSA replaces the source IP address to EASDF IP according to SMF instruction.

If SMF decides to remove the UL CL/BP and Local PSA as defined in TS 23.502[3] clause 4.3.5.5, e.g. due to UE mobility, the SMF sends a PDU Session Modification Command to configure the new address of the DNS server on UE (e.g. to set it to the address of EASDF).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*