

## **Draft new Recommendation ITU-T Y.3145 (ex.Y.FMC-AAEC)**

### **Application addressing in multi-access edge computing in IMT-2020 networks and beyond**

#### **Summary**

Application addressing is the process to discover the IP address of the server which the application running on when UE intends to access the application. On the basis of Y.3137, which specifies use cases and requirement of application addressing in multi-access edge computing, this Recommendation presents the framework and technical solutions of application addressing in multi-access edge computing in IMT-2020 networks and beyond.

#### **Keywords**

Application addressing, framework, IMT-2020, multi-access edge computing

## Table of contents

1. Scope.....	3
2. References.....	3
3. Definitions.....	3
3.1. Terms defined elsewhere .....	3
3.2. Terms defined in this Recommendation .....	4
4. Abbreviations and acronyms.....	4
5. Conventions .....	4
6. Overview .....	5
7. Framework of application addressing in multi-access edge computing .....	5
7.1. Framework of application addressing at first service request .....	6
7.2. Framework of application addressing for user at mobility .....	6
7.3. Framework of application addressing when EAS's performance degraded.....	7
7.4. Framework of application addressing in FMC network .....	7
7.5. Framework of application addressing across multiple edge computing platform operators .....	8
8. Procedures of application addressing in multi-access edge computing.....	8
8.1. Procedure of application addressing at first service request.....	8
8.2. Procedure of application addressing for user at mobility .....	10
8.3. Procedure of application addressing when EAS 's performance degraded.....	11
8.4. Procedure of application addressing supporting FMC .....	12
8.5 Procedure of application addressing with hierarchical DNS deployment .....	13
8.6 Procedure of application addressing with hierarchical DNS deployment and cache in the local DNS .....	15
9. Security Considerations .....	15
Bibliography.....	17

## **Draft new Recommendation ITU-T Y.3145 (ex.Y.FMC-AAEC)**

### **Application addressing in multi-access edge computing in IMT-2020 networks and beyond**

#### **1. Scope**

This Recommendation presents the framework and technical solutions of application addressing in multi-access edge computing (MEC) in IMT-2020 networks and beyond. The following aspects of application addressing in MEC are addressed in this Recommendation:

- Overview;
- Framework;
- Procedures.

#### **2. References**

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T Y.3130] Recommendation ITU-T Y.3130 (2018), *Requirements of IMT-2020 fixed mobile convergence*.
- [ITU-T Y.3131] Recommendation ITU-T Y.3131 (2019), *Functional architecture for supporting fixed mobile convergence in IMT-2020 networks*.
- [ITU-T Y.3137] Recommendation ITU-T Y.3137 (2022), *Technical requirements of application addressing in edge computing for future networks including IMT-2020 networks*.

#### **3. Definitions**

##### **3.1. Terms defined elsewhere**

- 3.1.1 Application addressing** [ITU-T Y.3137]: The process to discover the IP address of the server which the application running on when UE intends to access the application.
- 3.1.2 Edge computing** [b-ITU-T Y.3073]: This refers to a strategy to deploy processing capability at network edge where end terminals are connected, and to perform the processing of data which is derived from and fed to the end terminals.
- 3.1.3 Fixed mobile convergence** [b-ITU-T Y.3100]: In the context of IMT-2020, the capabilities that provide services and applications to end users regardless of the fixed or mobile access technologies being used and independently of the users' location.
- 3.1.4 IMT-2020** [b-ITU-T Y.3100]: Systems, system components, and related technologies that provide far more enhanced capabilities than those described in [b-ITU-R M.1645].

NOTE – [b-ITU-R M.1645] defines the framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000 for the radio access network

**3.1.5 Multi-access edge computing (MEC)** [b-ITU-T Y.3117]: System which provides an IT service environment and cloud-computing capabilities at the edge of an access network that contains one or more types of access technology, and in close proximity to its users.

### **3.2. Terms defined in this Recommendation**

This Recommendation defines the following terms:

None.

## **4. Abbreviations and acronyms**

This Recommendation uses the following abbreviations and acronyms:

BRAS	Broadband Remote Access Server
DNS	Domain Name System
EAS	Edge Application Server
ECP	Edge Computing Platform
EDC	Edge Dispatch Centre
FMC	Fixed Mobile Convergence
FW	Firewall
IP	Internet Protocol
LDNS	Local Domain Name System
MEC	Multi-access Edge Computing
NAT	Network Address Translation
QoE	Quality of Experience
QoS	Quality of Service
SMF	Session Management Function
UE	User Equipment
UPF	User Plane Function

## **5. Conventions**

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

## 6. Overview

With MEC, the operators are able to host their own or third party applications and contents closer to the user. The user can access the application/content via locally deployed User Plane Function (UPF) to fulfil the low latency requirement of diverse services, with the heavy traffic offloading from backbone network to the edge. However, currently in the industry, there is still a lack of common understanding of how to support application addressing in MEC in IMT-2020 networks and beyond. It is important to standardize the application addressing in MEC, which is the process to discover Internet Protocol (IP) address of optimal edge application server (EAS) based on the user's real-time location and the load conditions of EAS, thus to fulfil the service requirements.

According to [ITU-T Y.3130], through fixed mobile convergence (FMC) provided by IMT-2020, the end user can enjoy the seamless service experience and ubiquitous service availability, and service providers can provide seamless service realization for fixed and mobile access networks. Application addressing in MEC is necessary in the context of FMC, which aims to provide seamless edge applications experience and ubiquitous edge application availability.

As specified in [ITU-T Y.3137], there are new technical requirements of application addressing in MEC in IMT-2020 networks and beyond, so the framework and procedure of application addressing in MEC need to be studied.

## 7. Framework of application addressing in multi-access edge computing

The framework of application addressing in MEC in IMT-2020 networks including high-level description of functionalities is provided in this clause.

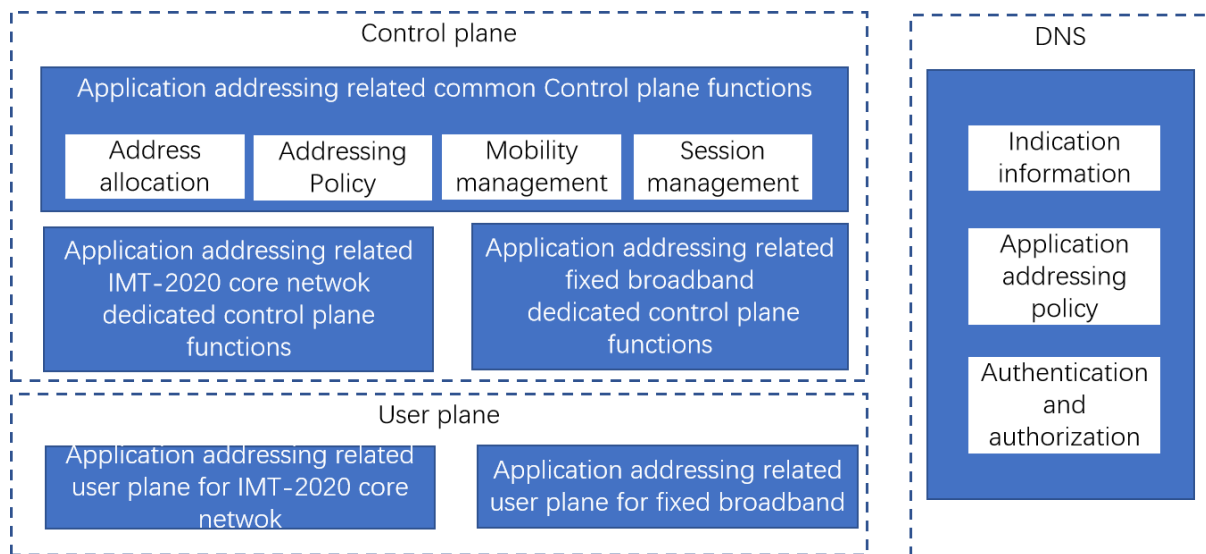


Figure 7-1 – Framework of application addressing in MEC

Figure 7-1 presents the framework of application addressing in MEC from a functional point of view. The framework of application addressing in MEC is composed of three main components as follows, and each main component consists of several functions.

- Control plane, which takes most of the control logic, including the address allocation, addressing policy, mobility management and session management.
- User plane, which provides packets switching under instruction of control plane.
- Domain Name System (DNS), which performs application addressing, based on the cooperation with control plane and user plane, including the indication information, application addressing policy and authentication and authorization.

### 7.1. Framework of application addressing at first service request

This chapter mainly describes a framework of application addressing at first service request. The framework is shown in Figure 7-2.

The geographical location of edge site is distributed, and how to obtain the optimal edge service site for user will be a core issue in MEC.

NOTE - Addressing mode of the most edge computing applications are not global addressing and the position of edge site is pre-configured on the User Equipment (UE) to realize the accurate addressing from the UE to the edge site. However, this manual configuration of static routes is not suitable for the global MEC service mode, especially at the first service request.

According to this framework, combining the existing IMT-2020 traffic steering technology, the application addressing at first service request process could be optimized, and the accurate edge application addressing is realized.

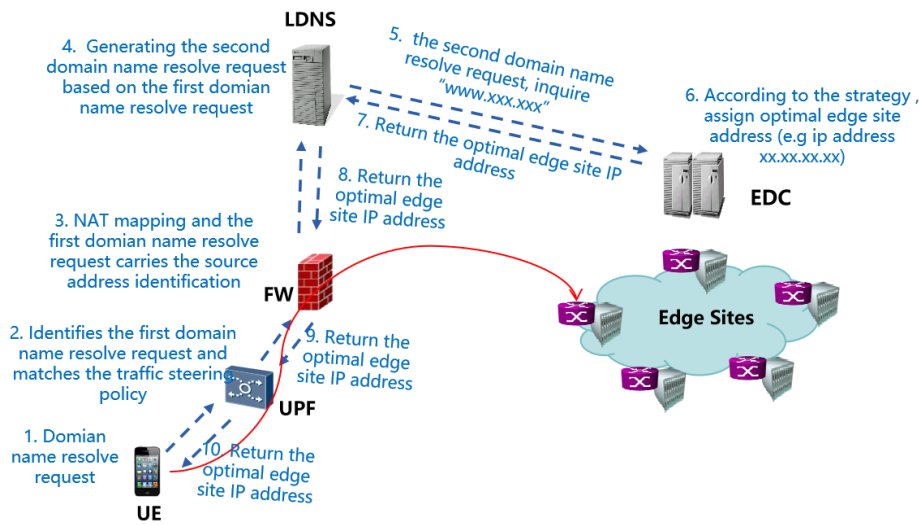


Figure 7-2 – Framework of edge application addressing at first service request

As shown in the Figure 7-2, after receiving the first domain name resolve request, local domain name system (LDNS) generates and sends the second domain name resolve request to edge dispatch center (EDC). EDC could obtain the source address identification carried in the second domain name resolve request. Then the EDC could determine the edge site address corresponding to the source address identification, which carried in the second domain name resolve request.

Through this framework, it is possible to promote the data process location from the central node of the network to the edge site. It is possible to accelerate the data transmission speed between the end user and the edge site, reducing the network delay and improving the user experience.

### 7.2. Framework of application addressing for user at mobility

According to [ITU-T Y.3137], for UE at mobility, the previous UPF and previous EAS may be not optimized now, so UE at new location initiates a new DNS request to find suitable EAS and UPF, the framework is shown in Figure 7-3.

The application addressing relocation is triggered when the conditions are met, and then edge relocation is performed by EDC. Then the traffic steering configuration is finished by IMT-2020 core network. When services have service continuity needs, the context transfer is performed with the cooperation of EDC and EAS.

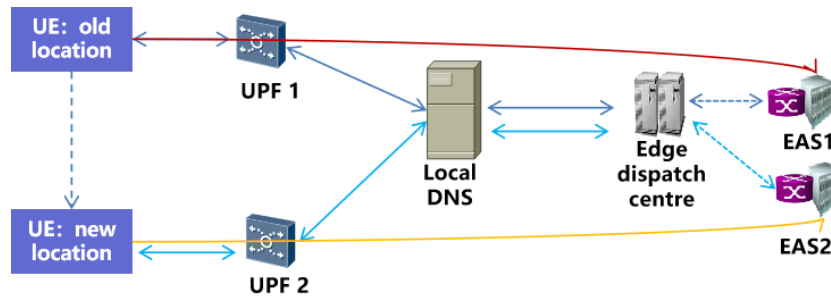


Figure 7-3 - Framework of application addressing for user at mobility

Through this framework, it is possible to re-select the optimal EAS for UE at mobility, further reducing the extra network delay and guaranteeing the service continuity.

### 7.3. Framework of application addressing when EAS's performance degraded

When the initially assigned EAS becomes non-optimized since its own condition degraded, new EAS is required to guarantee the service quality as shown in Figure 7-4. EDC chooses new EAS for UE according to, but not limited to, the location and status of EAS and UE's location, and then the IMT-2020 core network configures the traffic steering rule to the new EAS.

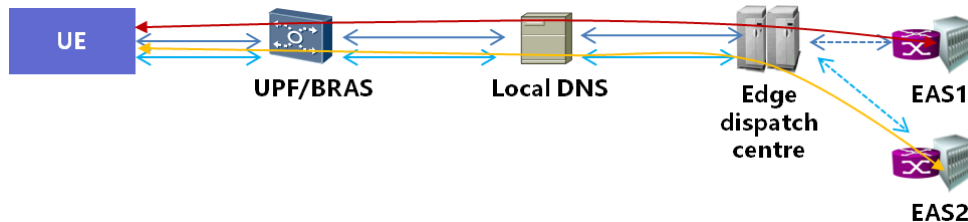


Figure 7-4 - Framework of application addressing when EAS's performance degraded

Through this framework, it is possible to re-select the optimal EAS for UE, and guarantee the service quality of service (QoS) and service continuity when edge application server's performance getting worse.

### 7.4. Framework of application addressing in FMC network

When UE changes the access network, the UE's IP address may change, and a new DNS request may be triggered. There are two frameworks in application addressing in FMC. One is that the service requests to be served on same EAS, another is that service requests may be assigned to different EAS as shown in Figure 7-5 and Figure 7-6.

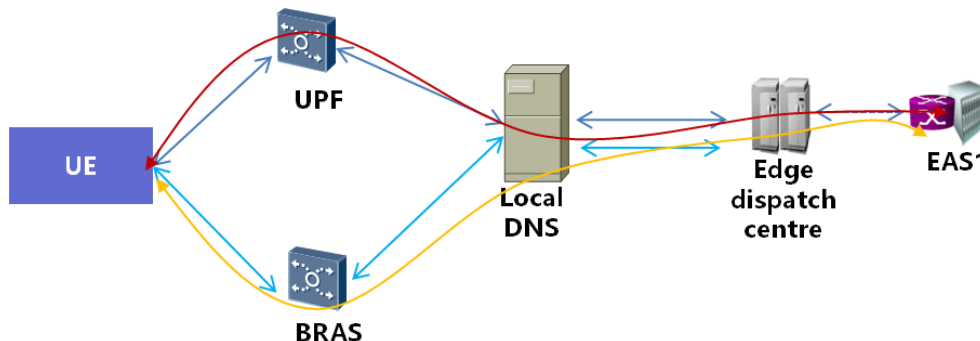


Figure 7-5 – Framework of application addressing in FMC network with the same EAS

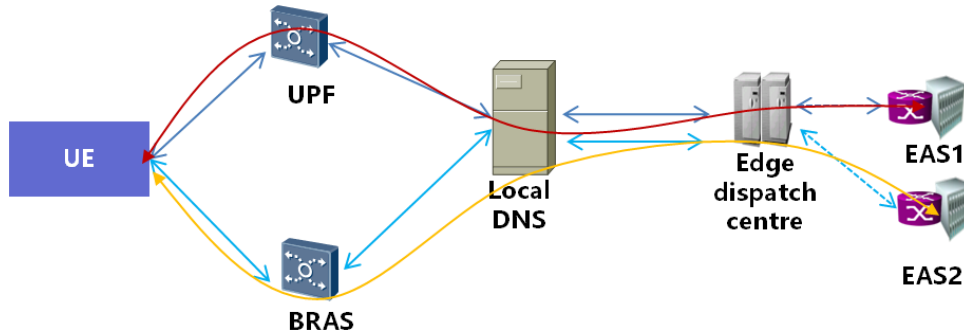


Figure 7-6 – Framework of application addressing in FMC network when the EAS changes  
Through this framework, it is possible to re-select the optimal EAS when UE changes the access network, and guarantee the service consistency and service continuity .

### 7.5. Framework of application addressing across multiple edge computing platform operators

In edge computing, there will be various EAS deploying same services belonging to different edge computing platform (ECP) operators, among different ECPs, so in application addressing in MEC, it is required for different ECP operators to have a coordination mechanism to assign an optimal EAS for UE as shown in Figure 7-7.

EDC selects the optimal ECP provider based on the status of EAS. And then ECP performs scheduling based on internal strategy to assign optimal EAS for users.

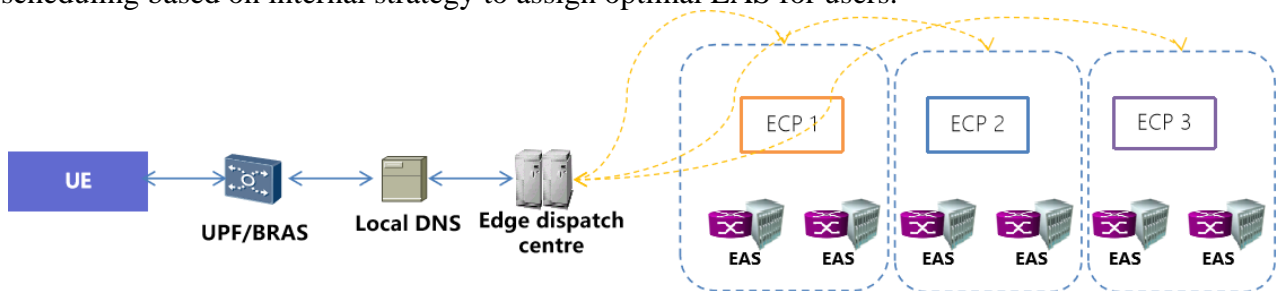


Figure 7-7 - Framework of application addressing across multiple ECP operators

Through this framework, it is possible to select the optimal EAS across multiple ECP operators, and enhance the coordination among ECPs.

## 8. Procedures of application addressing in multi-access edge computing

### 8.1. Procedure of application addressing at first service request

In the framework specified in clause 7.1, UE needs to discover the IP address of the suitable edge site, which deployed EAS, via Local DNS and EDC. Generally EDC could be deployed or operated by network operators or the third party providers. So the traffic can be locally steering to a suitable edge site in order to optimize end user experience.

1. UE sends the first domain name resolve request to the UPF;
2. UPF identifies the first domain name resolve request and matches the traffic steering policy based on the identification result;

NOTE 1 - For UPF, the domain name information in DNS resolve request message could be identified;

3. The UPF sends the first domain name resolve request which meets the traffic steering policy to the Firewall (FW);



4. The FW receives the first domain name resolve request which meets the UPF traffic steering policy and does the Network Address Translation (NAT) mapping for generating the first domain name resolve request carrying a source address identification (eg. public network IP address of FW);

5. The FW sends the first domain name resolve request carrying the source address identification to LDNS;

6. The LDNS extends the first domain name resolve request with the source address identification and generates the second domain name resolve request;

NOTE 2 - For LDNS, the DNS protocol is required to support carrying the identification of source address (eg. public network IP address of FW) ;

7. The LDNS sends the second domain name resolve request to EDC;

8. The EDC determines the edge site address corresponding to the source address identification, which carried in the second domain name resolve request; (eg.EAS deployed on edge site);

NOTE 3 - For EDC, it is required to assign optimal edge site based on key factors including but not limited to UE's location information, edge site's location, EAS load status, network link information and service requirements such as network latency etc.

NOTE 4 - For EDC, it is required to acquire the information of the mapping relationship between multiple sets of the source address identification (eg.public IP address of FW) and UE location information from IMT-2020.

NOTE 5 - The EDC could support to resolve the domain name.

9. The EDC sends DNS response to the LDNS;

10. The LDNS response to the UE carrying the edge site address information.

NOTE 6 - For the whole addressing process,it is required to support to send the information of assigned edge site and related UPF to Session Management Function (SMF), to assist the configuration of traffic steering rule.

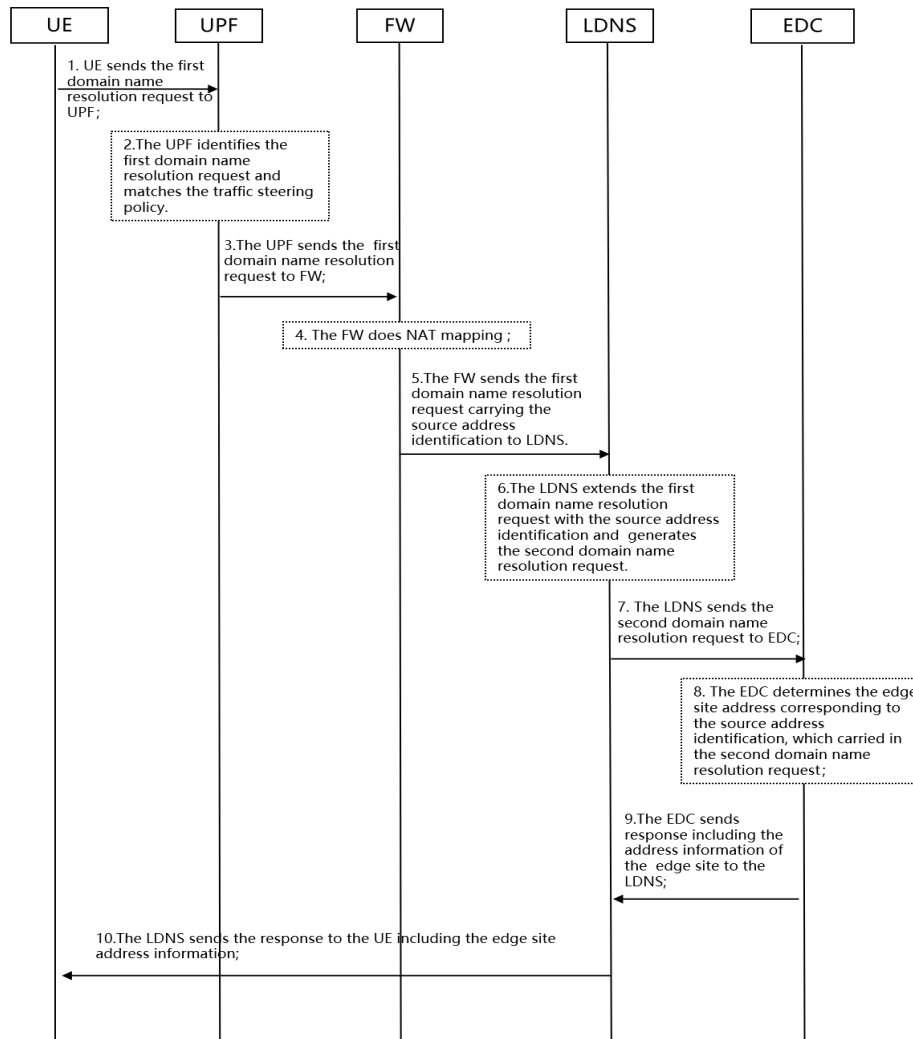


Figure 8-1 – Procedure of application addressing at first service request

## 8.2. Procedure of application addressing for user at mobility

In the framework specified in clause 7.2, when UE is at mobility, the relocation of the UPF may be triggered to make sure the service continuity. In addition to that, the relocation of EAS may be required, because the quality of experience (QoE) may be degraded since the distance between EAS and UE becomes longer when UE still accesses to same EAS, so the seamless relocation of EAS may be required in application addressing as shown in Figure 8-2.

There is service continuity problem for service with continuity needs, so it is required to define pre conditions to trigger the application relocation. The precondition may be the UPF handover message when user at mobility.

1. EAS1 subscribes the UPF change event to IMT-2020 networks.
2. SMF notifies EAS1 that the UPF accessed by UE is switched.
3. UE makes sure the precondition is met when receiving the UPF handover message.

NOTE 1 - The UPF handover message is sent by previous EAS (e.g, EAS1) after receiving the notification message from SMF, which indicates that the accessing UPF of UE changes. For example, UE changes the access from UPF1 to UPF2.

4. UE sends the DNS resolution request to EDC, with the information of user identification information, application identification information, and service continuity needs.

5. EDC receives DNS resolution request and re-selects the new EAS (e.g EAS2) based on the service continuity needs information and user identification information.
6. EDC sends the DNS resolution response message to UE, carrying the address information of the new EAS.
7. EDC sends the synchronization instructions respectively to previous EAS(e.g, EAS1) and new EAS (e.g EAS2), and the instruction information includes user identification information, application identification information and service continuity needs, which instruct the previous EAS(e.g, EAS1) synchronizes the service data corresponding to the user identification information to the new EAS(e.g EAS2).

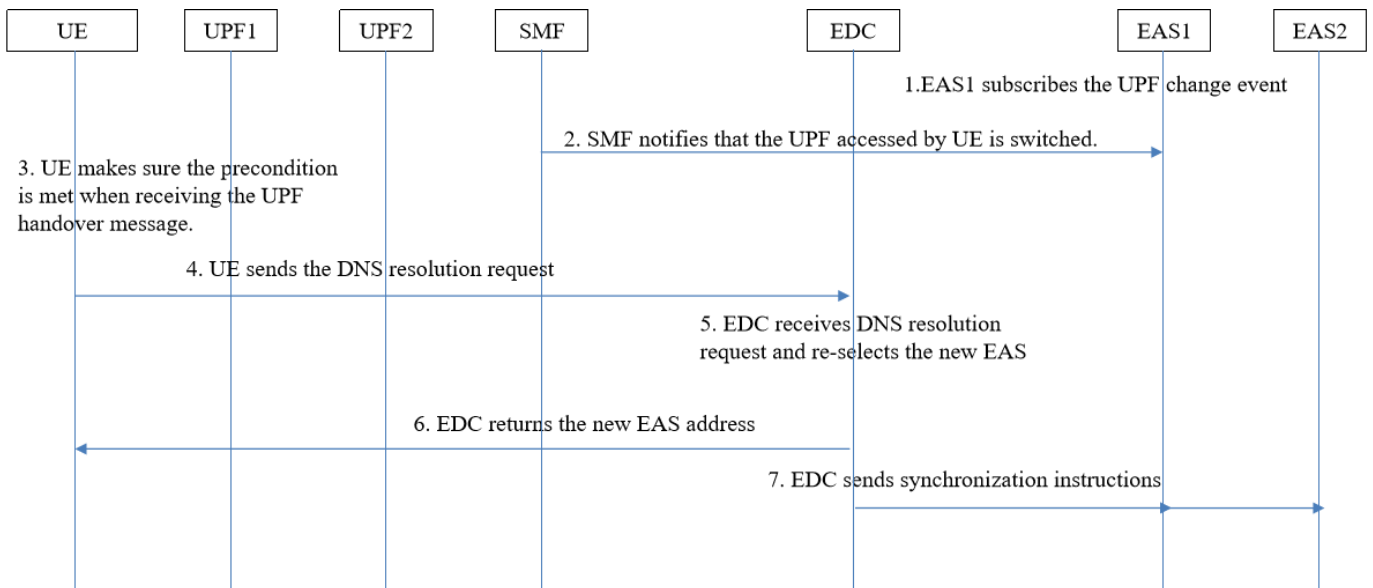


Figure 8-2 – Procedure of application addressing for user at mobility

NOTE 2- For EDC, it needs to store the information of domain name resolution records; the domain name resolution record includes at least a mapping relationship between the multi sets of user identification information and address information of the EASs.

NOTE 3- Before EDC sends the synchronization instructions respectively to previous EAS(e.g, EAS1) and new EAS (e.g EAS2), EDC queries the domain name resolution record based on the user identification information, and determines the address information of the previous EAS and the address information of the new EAS.

### 8.3. Procedure of application addressing when EAS 's performance degraded

In the framework specified in clause 7.3, UE and the application server could know the real-time status of the service quality, including, not limited to the delay, rate, so the relocation could be triggered by UE or the application server. When the initially assigned EAS becomes non-optimized causing the connection status are getting worse,, a new EAS is required to guarantee the QoS as shown in Figure 8-3.

Also, there is also service continuity problem for service with continuity needs, so it is required to define preconditions to trigger the application relocation. The precondition may be the performance of server getting worse.

1. When the connection status parameter reaches a preset threshold, UE determines that the precondition is currently met.

NOTE 1- UE obtains the connection status parameter between the UE and the previous EAS(e.g, EAS1).

2. UE sends the DNS resolution request to EDC, with the information of user identification information, application identification information, and service continuity needs.

3. EDC receives DNS resolution request from UE and re-selects the new EAS (e.g EAS2) based on the service continuity needs and user identification information. .

4. EDC sends the DNS resolution response message to UE, carrying address information of the new EAS.

5. EDC sends the synchronization instructions.

NOTE 2- The detailed synchronization is same as clause 8.2.

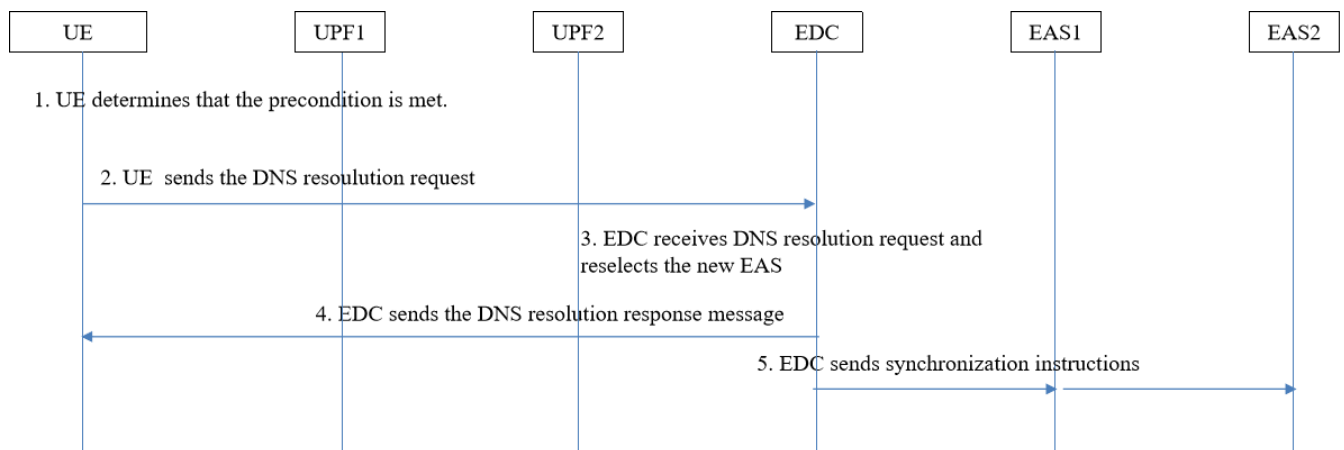


Figure 8-3 – Procedure of application addressing when EAS's performance degraded

#### 8.4. Procedure of application addressing supporting FMC

According to [ITU-T Y.3130] and [ITU-T Y.3131], through FMC provided by an IMT-2020, the end user may enjoy a seamless service experience and ubiquitous service availability, and service providers can provide seamless service for fixed and mobile access networks.

In the framework specified in clause 7.4, FMC supported edge application addressing is necessary, to make sure the service continuity of application addressing in MEC with guaranteed QoS including the handover between different access networks and migration from a single access network to multiple access networks as shown in Figure 8-4.

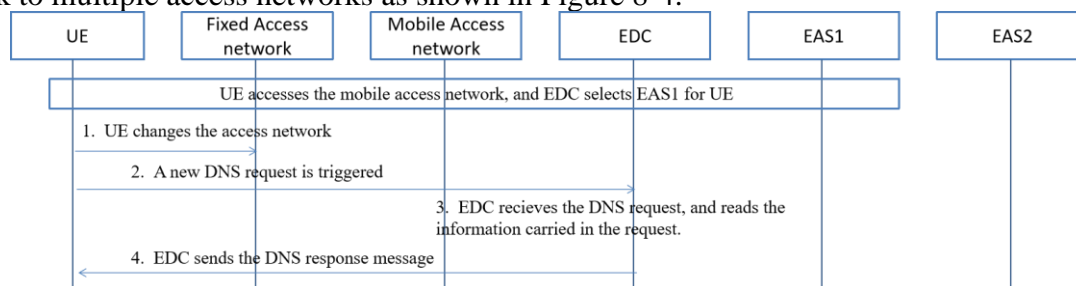


Figure 8-4 – Procedure of application addressing supporting FMC

Precondition: UE accesses the mobile access network and EDC selects EAS1 for UE.

1. UE changed the access from mobile access network to fixed network.

2. UE initiates a new DNS request.

3. EDC receives the DNS request and reads the information carried in the request.
4. EDC sends the DNS response message to UE to access to the EAS2.

When UE changes the access network, the UE's IP address may change, and a new DNS request may be triggered. There are two framework in application addressing in FMC. One is that the service requests to be served on same EAS, another is that service requests may be assigned to different EAS.

### 8.5 Procedure of application addressing with hierarchical DNS deployment

In the framework specified in clause 7.5, there may be hierarchical DNS deployment, with local DNS resolves the DNS request, and central DNS resolves the recursive query of local DNS. Multiple Local DNS are responsible for different areas. So the coordination within the hierarchical DNS need to be considered. In edge computing, there will be various EAS deploying at least one same edge computing services and may be associated with different local DNS. The procedures are as below:

There are different methods to obtain the service status information, one is that local DNS receives the service status information send by at least one target service and generates the service status information, and the information sending period is associated with the frequency of service status information changes and/or the number of service requests, another is the local DNS sends the information to at least one target service associated with the local DNS for requesting the status information, and receives the service status information send by at least one target service and generates the service status information .

Figure 8-5 depicts the procedure of application addressing with hierarchical DNS deployment when local DNS determines target EAS

Precondition: Local DNS reports the service status information to central DNS, and the reporting period is associated with the frequency of service status information changes and/or the number of service requests.

Case 1:local DNS receives the service status information send by EAS

1. Local DNS receives the information, which used to request the DNS service query, and also contains the requirements and the service identification;

NOTE 2 - The requirements include at least the resource requirements and the performance requirements. And the resource requirements include at least the networking requirements and computing requirements.

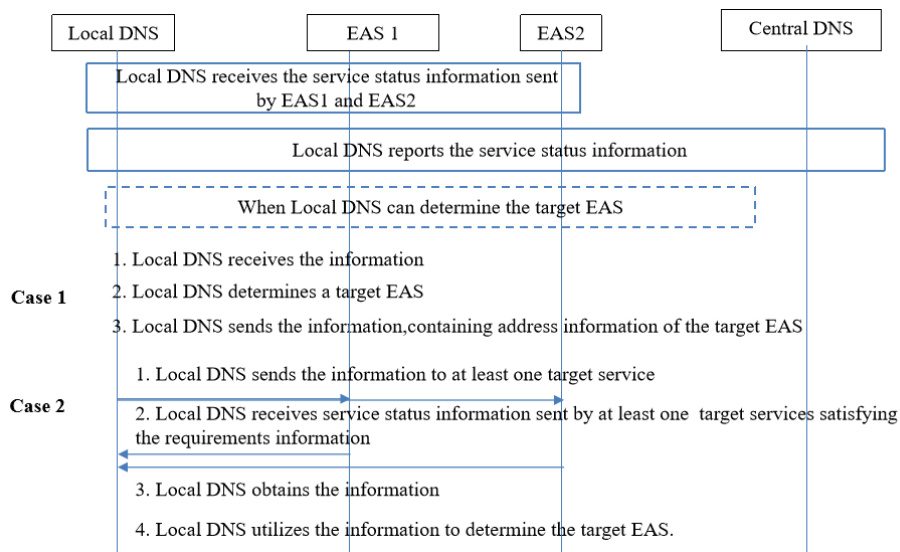


Figure 8-5 – Procedure of application addressing with hierarchical DNS deployment when local DNS determines target EAS

2. Local DNS determines a target EAS corresponding to the target service utilizing the requirements, the service status information and the service location information of target services.
3. Local DNS sends the information, containing address information of the target EAS.

Case 2: local DNS sends the information to request the target services to return the related information

1. Local DNS sends the information to at least one target service, to request at least one target service that satisfies the requirements;
2. Local DNS receives service status information sent by at least one target services which satisfies the requirements;
3. Local DNS obtains the information which contains at least one target service satisfying the requirements and corresponding service status information;
4. Local DNS utilizes the above mentioned information to determine the target EAS.

NOTE 3- Bases on the service status information, local DNS determines the target EAS from the at least one target services satisfying the requirements. For example, if there are five EAS satisfying the requirements, the local DNS determines the target EAS bases on the service status information and service location information, and obtaining the target EAS.

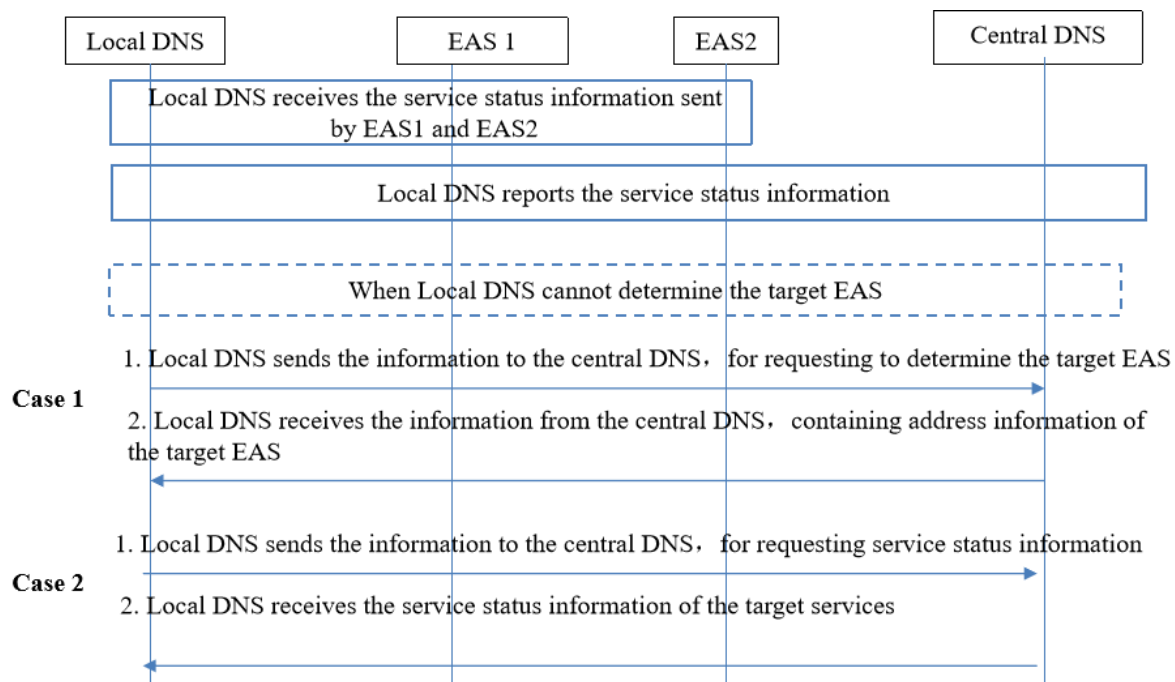


Figure 8-6 – Procedure of application addressing with hierarchical DNS deployment when local DNS cannot determine target EAS

Figure 8-6 depicts the procedure of application addressing with hierarchical DNS deployment when local DNS cannot determine target EAS.

When Local DNS cannot determine the target EAS associated with the local DNS, one case is:

Case 1:

1. Local DNS sends the information to the central DNS, for requesting to determine the target EAS, containing at least the requirements and the service identifier;
2. Local DNS receives the information from the central DNS, containing address information of the target EAS.

Case 2:

1. Local DNS sends the information to central DNS, for requesting service status information of the target services;
2. Local DNS receives the service status information of the target services sent by central DNS and obtaining the service status information.

## 8.6 Procedure of application addressing with hierarchical DNS deployment and cache in the local DNS

In the framework specified in clause 7.5, in the process of determining the target EAS, local DNS may be looked up from a cache; if the target EAS is not found in the cache, then the target EAS can be determined using a local lookup or a central DNS lookup as shown in Figure 8-7. In this way, the efficiency of the service domain name query can be improved and the amount of resolution of the DNS system can be reduced.

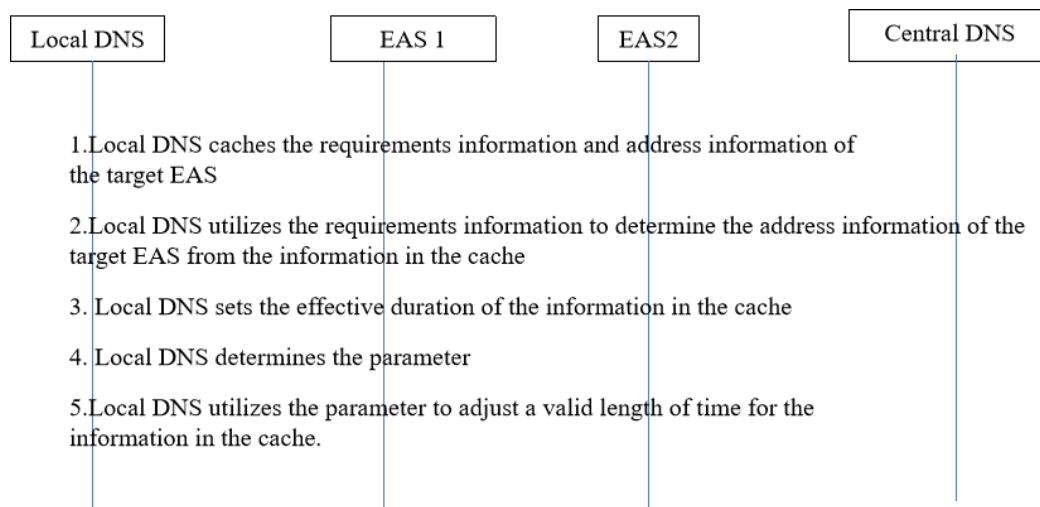


Figure 8-7 – Procedure of application addressing with hierarchical DNS deployment and DNS cache

1. Local DNS caches the requirements and address information of the target EAS.
2. Local DNS utilizes the requirements to determine the address information of the target EAS from the information in the cache.

NOTE 1 - Local DNS receives the information ,which used to request the DNS service query, and also contains the demand information and the service identification.

NOTE 2- The information in the cache contains the mapping relationship of at least one of the service' requirements and the address information of the EAS .

3. Local DNS sets the effective duration of the information in the cache, based on the frequency of change of service status information and/or the number of service requests.
4. Local DNS determines the parameter, which characterizes a probability of determining address information of the target EAS based on the information in the cache.
5. Local DNS utilizes the parameter to adjust a valid length of time for the information in the cache.

## 9. Security Considerations

The network information is needed to assist the application addressing process, and the authentication and authorization of EDC to obtain the network information is required. In addition,

the security and privacy related requirements specified in [ITU-T Y.3137] are applicable to this Recommendation.



### **Bibliography**

- [b-ITU-T Y.3073] Recommendation ITU-T Y.3073 (2024), *Framework for service function chaining in information-centric networking*.
- [b-ITU-T Y.3100] Recommendation ITU-T Y.3100 (2017), *Terms and definitions for IMT-2020 network*.
- [b-ITU-T Y.3117] Recommendation ITU-T Y.3117 (2023), *Quality of service assurance-related requirements and framework for smart education supported by IMT-2020 and beyond*.
- [b-ITU-R M.1645] Recommendation ITU-R M.1645 (2003), *Framework and overall objectives of the future development of IMT-2000 and systems beyond IMT-2000*.
-