ETSI White Paper No. 39

Enhanced DNS Support towards Distributed MEC Environment

1st edition – September 2020

ISBN No. 979-10-92620-34-4

Authors:

Masaki Suzuki, Takuya Miyasaka, Debashish Purkayastha, Yonggang Fang, Qiang Huang, Jinguo Zhu, Balendu Burla, Xiaopeng Tong, Dan Druta, Jane Shen, Hanyu Ding, Guo Song, Marco Angaroni, Viscardo Costa

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

About the authors

Masaki Suzuki
KDDI,

Takuya Miyasaka
KDDI,

Debashish Purkayastha
InterDigital,

Yonggang Fang
ZTE,

Qiang Huang
ZTE,

Jinguo Zhu
ZTE,

Balendu Burla
Intel,

Xiaopeng Tong
Intel,

Dan Druta
AT&T,

Jane Shen
Futurewei,

Hanyu Ding
China Mobile,

Guo Song
China Mobile,

Marco Angaroni
Italtel,

Viscardo Costa
Italtel,

Contents

Executive Summary

This White Paper focuses on the enhanced Domain Name System (DNS) support towards the distributed Multi-access Edge Computing (MEC) environment. In the current ETSI Industrial Specification Group (ISG) MEC, MEC puts a major assumption for simple client-server deployment, and the distributed environment is not fully specified. In terms of providing the connectivity between devices and applications, the current specifications basically support it by using DNS but still need some extensions in the deployment phase, e.g., protocols, parameters and efficient use of Application Programming Interfaces (APIs). For instance, the deployed system has to consider the mobility that causes frequent route updates, the enormous volume of connection, and inevitable disruption.

In this White Paper, firstly, three possible use cases for the distributed environment are introduced. A MEC system consists in general of multiple MEC hosts distributed at the edge and connected by the underlying networks. In order to provide the best Quality of Service (QoS) and Quality of Experience (QoE) to a user, the user device is normally connected to the closest MEC host where an application instance is configured and orchestrated for running to better serve the user by the MEC orchestrator, including the case where that is triggered by user through the User App LCM proxy. However, such location based MEC host selection may not always be the best choice, from a QoS/QoE perspective.

Secondly, three requirements for the distributed environment are derived as follows. Based on the use cases, the MEC system should support the case where the best service may be decided by other than location, e.g., service latency, resource availability as well as the device identifier. Also, the MEC system should shorten the disruption time while changing the serving MEC host.

Then, potential deployment options for the extension of current DNS support are indicated. Those are classified into two categories depending on associating network, 3GPP specific one and generally applicable ones. Regarding the 3GPP specific one, since the study item in 3GPP SA2 is currently ongoing, there are three supported types of connectivity, two ways to discover edge services, and a few options are introduced. More informed DNS query solution for local DNS services in 5GC is also introduced. Regarding the other ones, enhanced DNS solution, Hypertext Transfer Protocol (HTTP) redirection solution, UE application, device application interface solution, virtual Internet Protocol (IP) solution, and edge DNS server solution are introduced.

Finally, this White Paper concludes with a table that summarizes if the potential solutions satisfy each requirement. The quantitative evaluation is not conducted in this White Paper and which solution is the best for deployment may depend on a different use case. Hopefully, MEC providers will decide according to their own situation together with mobile network operators, application providers, and other relating service providers.

1 Introduction

Multi-access edge computing (MEC) technology is emergingly recognized with 5G technologies. It is originally derived from the cloud technologies and shifting the computing resources towards the device (edge) side. In general, low latency, less volume of network traffic, and data localization are the major benefits gained from MEC. In this context, MEC is expected to be adopted as one of the key elements for the Vehicle to everything (V2X) applications (see 5G Automotive Association, Toward fully connected vehicles: Edge computing for advanced communications [1]) as well as the gaming, Augmented/Virtual Reality (AR/VR) applications (see GSMA, "Cloud AR/VR Streaming: Accelerate mass adoption and improve quality of experience of AR/VR using 5G and edge cloud [2]). For the flexible adoption, MEC is capable of deployment with not only cellular network, e.g., Long-Term Evolution (LTE) and 5G, but also Wi-Fi, or other fixed access networks.

While MEC is highly activated in open source software field, it is standardized in an ETSI Industry Specification Group (ISG) MEC. ETSI ISG MEC has already published several Application Programming Interface (API) specifications to realize and facilitate the adoption to the MEC ecosystem. Currently, MEC-based edge computing deployments in the field are on their way.

Various forms of MEC deployments can be recognized in the industry. The current major assumption for deployment is the simple client-server model. The key deployment drivers are low latency, reduced data traffic, data localization and better operation and management.

An evolutional deployment approach with more widely distributed edge resources may not yet be fully supported by the current MEC framework and is one of the promising topics for ETSI ISG MEC in phase 3. In terms of the connectivity, the current specification supports the connectivity between devices and application instances by using Domain Name System (DNS) even under the distributed environment. However, some extensions are still needed for the deployment, covering aspects such as protocols, application design, parameters and efficient use of the APIs. For instance, the deployments have to take into account the mobility of devices, the connectivity arrangements for the application instances from multiple devices, and the acceptable disruption time for the applications due to mobility events.

This White Paper documents the preparation for the upcoming evolution, focusing on the connectivity that is one of the most important aspects. Firstly, possible use cases for the distributed MEC environment are introduced in the following clause. After that new requirements for a distributed MEC environment are clarified. Then, the main part of this White Paper introduces solutions to realize enhanced connectivity support. These solutions are finally summarized (and categorized into 3GPP-friendly and general).

2 Possible use cases for distributed MEC environment

The MEC architecture enables cloud computing capabilities and distributed IT service environment on the edge of networks. A MEC host includes a virtualization infrastructure and the computing platform for running applications or services (which are indeed deployed at the edge of the networks to reduce the

end-to-end latency). A MEC system may consist of multiple MEC hosts distributed at the edge and connected by the underlying networks.

In order to provide the best QoS and QoE to a user, the user device is normally connected to the closest MEC host where an application instance is configured and orchestrated for running to better serve to the user by the MEC orchestrator, including the case where that is triggered by user through the User App LCM proxy. However, such location based MEC host selection may not always be the best choice, from a QoS/QoE perspective.

[Use Case 1] The best serving MEC host does not only depend on its location at the networks and distance to the user device, but also depends on the traffic load of the underlying network and the computing resource usage on the MEC host. A MEC host initially serving a user device may possibly become not the best one, e.g. once a lot of user devices in the serving area request the service from the closest MEC host, for example in a big event. As a result, the serving MEC host may become overloaded and needs to distribute some services to other application instances running on neighbour MEC hosts. Therefore, either network operators and/or the MEC service providers would like to optimize and distribute the services among the nearby MEC hosts to balance the load of traffic and computing. In some cases, user devices may query the information about the same service provided by nearby MEC hosts and select a host with less overload to continue being served.

[Use Case 2] When a user device is a mobile phone or a portable equipment, the best serving MEC host to the user device may not always be the best one as the user device may move from one cell to another which is under another MEC host service area. Therefore, this mobility event may trigger the user device or the MEC application mobility service to find a new MEC host to best serve to the user. In addition, this may invoke the MEC application mobility to transfer the existing service to the new application instance seamlessly.

[Use Case 3] In a V2X use case described in ETSI GS MEC 030 [3], an Intelligent Transportation System (ITS) Operator may provide a country-wide V2X service over different operators' networks, i.e. deploying different MEC systems, to offer the V2X service to vehicles belonging to different OEMs. In another case, V2X services may be provided by different network operators in the same country and/or in different countries. Therefore, when a vehicle runs on the highway, it may cross the serving areas of different MEC hosts, or even cross MEC systems of different PLMNs. Consequently, a V2X client-server continuity needs to be maintained in such operational conditions.

3 Requirements for service discovery

The following requirements may need to be considered.

- [Requirement 1] In the case where the operator wants to dynamically choose the optimized MEC host (due to, e.g., operation policies), Internet Protocol (IP) addresses for those hosts are supposed to link not only with fully qualified domain name (FQDN), but also with other metrics, e.g., device identifier, location, latency, resource availability, resource utilization, or performance indexes.
- [Requirement 2] As depicted in Figure 1, in the case where the different devices need to connect to different MEC hosts, the same FQDN is supposed to link with different IP addresses. The DNS server

may return different IP address depending on the device in question.

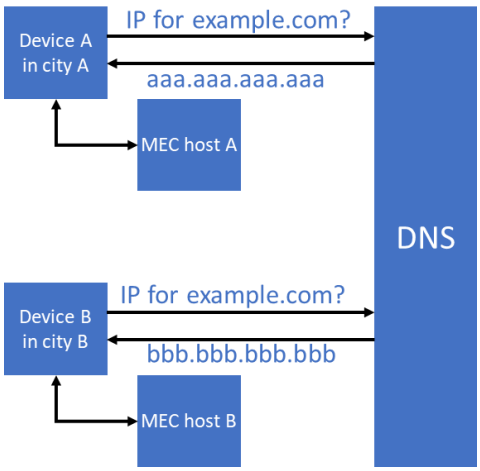

Figure 1: Abstract behaviour for requirement 2

- [Requirement 3] In the case of mobility of devices, the metrics for the MEC host selection may drastically change. Therefore, the serving MEC host should be updated according to the location of the device. In addition, in the case of latency critical application, the update should be completed in real-time manner.

4 DNS support in MEC system

Figure 2 depicts the basic call flow when a device resolves the appropriate IP address in the case where the appropriate IP address dynamically changes.

Figure 2: High-level call flow to establish/update connection with MEC hosts

The detailed steps are as follows:

1. As described in A.2, DNS support in ETSI GS MEC 003 [4], MEO always keeps DNS rules up to date
2. Device asks DNS (Resolver) to resolve IP address from FQDN
3. DNS (recursive resolver) resolves the requested FQDN recursively and sends a DNS query to DNS (authoritative server)
4. DNS (authoritative server) returns IP address to DNS (recursive resolver)
5. DNS (recursive resolver) returns IP address to Device
6. Device establishes a connection to MEC host A
7. According to the situation, MEO would update DNS rules
8. After the update, when Device asks an IP address via DNS (recursive resolver), DNS (authoritative server) would return the corresponding IP address [*Note: Alternatively, as soon as MEO updates DNS rules, the device may be triggered to update IP address and implement mechanisms to redirect existing flows. The device may not have to wait for cache expiry.*]
9. Device establishes the connection to MEC host B

However, current DNS support cannot fulfil the requirement 1, 2, and 3 in clause 3 and cannot be applicable for the distributed MEC environment.

5 Solutions and evaluations

When we consider both cases of deployment, one in a 3GPP network and the other in a generic network, the solution can also be categorized into two types correspondingly.

5.1 3GPP specific solution

5.1.1 Enhancement of support for edge computing in 5G core network

In the case where the MEC system is deployed with/in 5G Core Network (5GC), the service discovery functionality can be provided by 5GC. Regarding the service discovery, since no normative work has been completed in 3GPP SA2, considering the alignment and applicability, which it is for further study. At the moment, the study in 3GPP TR23.748 [5] is ongoing.

According to 3GPP TR23.748 [5], 5GC supports at least the following three types of connectivity, all of them applicable to MEC.

- Distributed Anchor Point
- Session Breakout
- Multiple PDU sessions

Edge service discovery – the process of locating optimal edge services -- requires device geolocation and edge service availability. Geolocation information is generated and maintained inside 5GC while service availability requires application deployment information. 5GC and applications are owned by different entities, with no information exchange currently defined per current 3GPP specifications. Due to this situation, 3GPP SA2 is working on a draft to enhance service discovery capability from the 5GC side.

There are two ways to discover edge services:

- 5GC obtains edge service availability from applications and resolves DNS requests
- Applications obtain device geolocation information and resolve DNS requests

A few options are proposed in 3GPP TR23.748 [5], as follows:

- Use an additional DNS resolver. SMF passes it to UE as the first hop DNS resolver. It can be a local DNS resolver or a new DNS AF within 5GC. This new DNS resolver carries edge service information from applications. Combined with the 5GC UE location info, the DNS resolver can direct UE to the optimal edge service.
- Expose UE location information to an application authoritative resolver via local UPF information. It can be a local NAT subnet or configured locally.
- Leverage DNS resolvers within EAS. EAS can be located either via URSP (UE Route Selection Policy) or AF influencing (using traffic descriptors). An optimal SMF would be selected to anchor a UPF with targeted EAS deployed. The target EAS uses the DNS resolver to resolve UE request.

ETSI MEC APIs and reference architecture can be adopted to support EAS and DNS resolvers. DNS resolvers can be updated by UE locations or application edge service availability.

5.1.2 More Informed DNS Query solution for local DNS services in 5GC

5.1.2.1 Description

Communication Service Provider's (CoSP) local DNS servers always locate very far from the edge site and are thus not able to provide more informed DNS services for the devices to access Cloud Service Provider (CSP) applications within the edge site area. As the below example diagram (Figure 3) shows, the device's DNS query for CSP applications will be forwarded by CoSP's local DNS to the authoritative DNS. Due to a lack of extra information for the decision, the authoritative DNS will respond with a MEC application in the Area B that is far away from the devices. Accordingly, it will influence the latency.

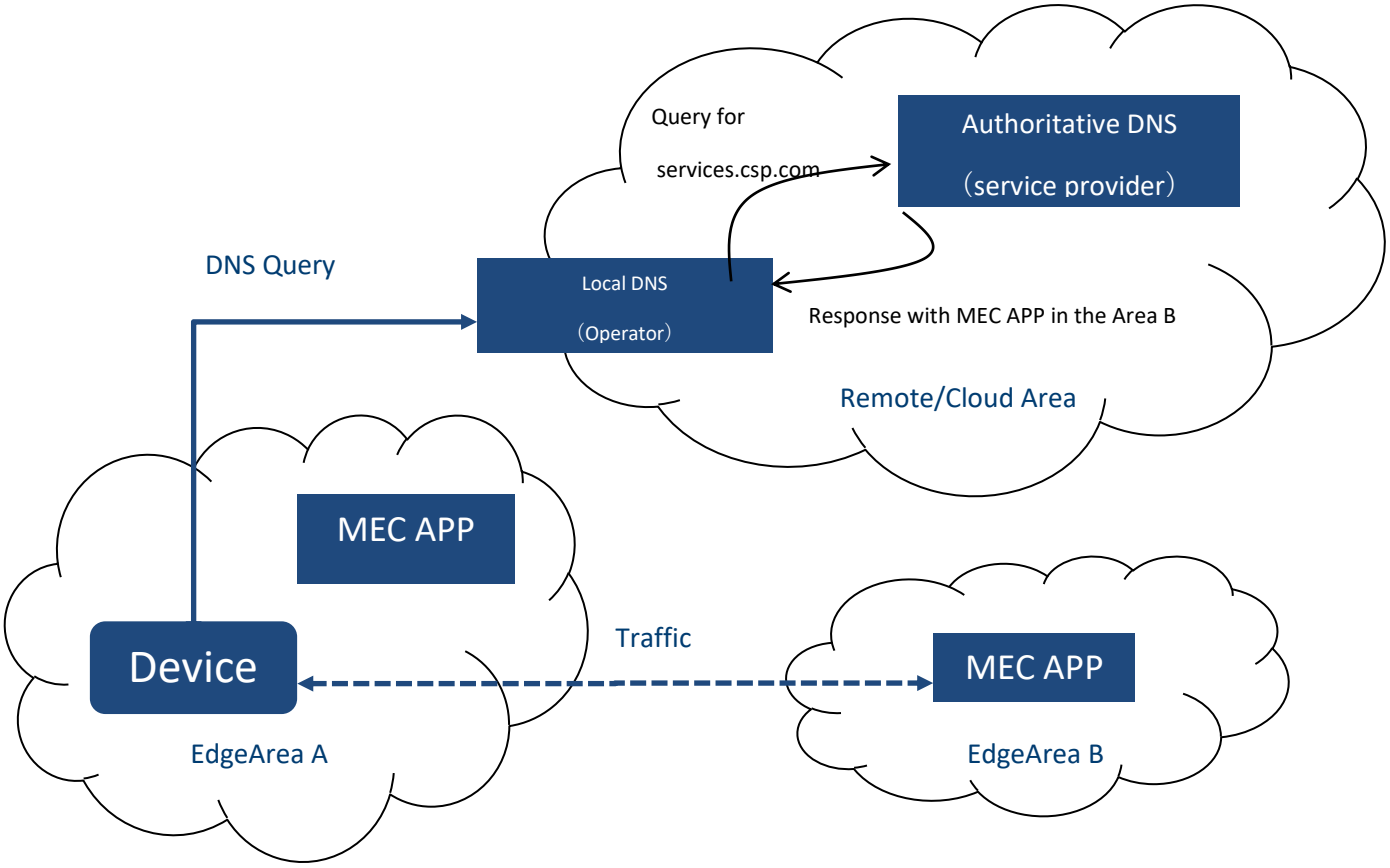

Figure 3: An example diagram for more informed DNS query

Besides, the local DNS is owned by the operator and may not able to provide full flexibility for the CSP to add, modify and delete DNS entry. From the real deployment point of view, CSPs prefer to own the MEC hosts (sit at the edge data center owned by CSP) including edge DNS as well rather than using local DNS services provided by operators. With 5G network exposure capability over NEF northbound interface, the traffic routing will become more informed as shown in the below message flow diagram:

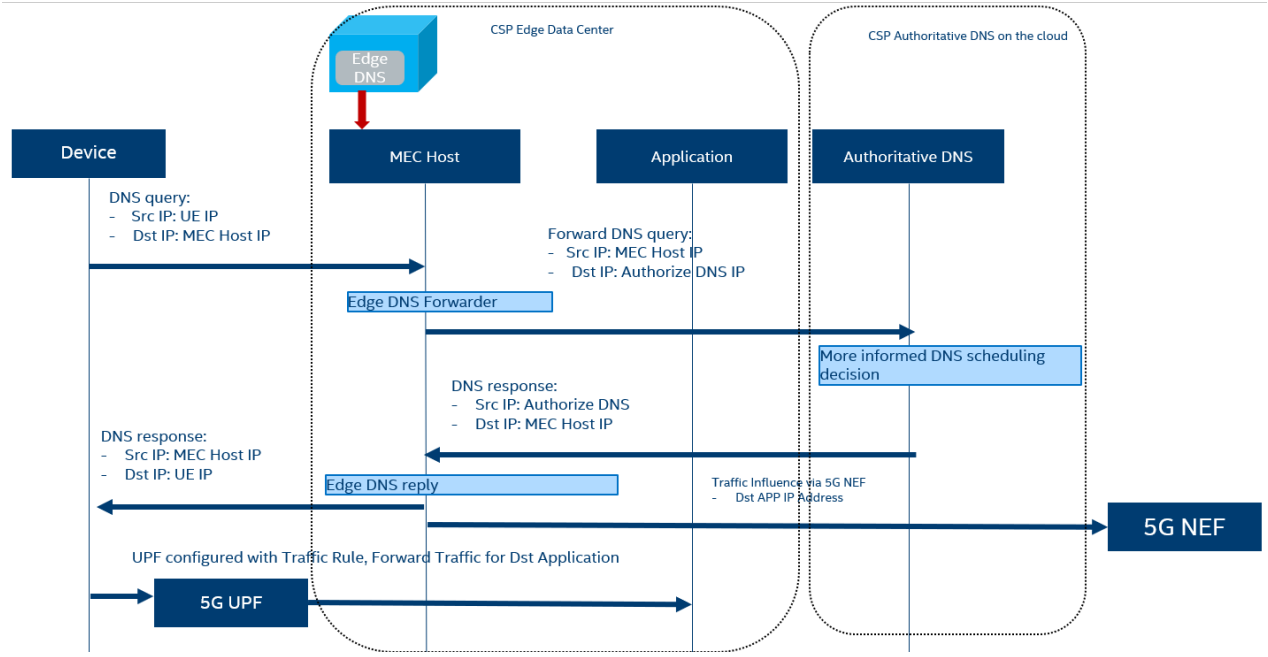

Figure 4: Message flow diagram of more informed traffic routing

NOTE: MEC Host should be capable to interact with 5G NEF.

5.1.2.2 Evaluation

Requirement 1 is satisfied as described in subclause 5.2.6.1.

To fulfil Requirement 2, for multiple devices' DNS query with same FQDN, authoritative DNS will collaborate with the edge DNS to make an intelligent scheduling decision for the service discovery. And the Edge DNS and authoritative DNS can leverage enhanced DNS technology such as EDNS Client Subnet (ECS, IETF RFC 7871 [6]) …etc.

To fulfil Requirement 3, the application on the device side can be well designed to detect the service connection condition such as latency, packets loss rate…etc. and then decide whether to initiate new service discovery for the same FQDN. On the other hand, the service provider can also leverage 5G NEF interface to subscribe notification event about location change, and accordingly instruct application on the device side to initiate the new service discovery.

5.2 Generally applicable solutions

The following solutions are not only applicable for the 3GPP network, but also applicable for generic network.

5.2.1 Enhanced DNS solution

5.2.1.1 Description

In the case of a distributed MEC environment, e.g., illustrated in Figure 2, multiple devices may connect to different MEC hosts simultaneously. Also, in the case of mobility, e.g., vehicles, each device may need to change the serving MEC host according to the location, resource availability or other metrics.

The request from the device contains not only FQDN, but also other metrics to specify the appropriate MEC host, e.g., device identifier, location, performance metrics, or resource metrics. The required parameters depend on the operator's policy. The enhanced DNS system is expected to support such kinds of additional parameters. Regarding geographical location of devices, EDNS client subnet (ECS) specified in IETF RFC 7871 [6] supports to estimate the device's location as depicted in Figure 5. However, other metrics are not compatible with the state-of-the-art DNS protocols. The operation might be an extension of the ECS operations and the extra information can be included in an extended FQDN, e.g., device_id.example.com, or a newly defined option of EDNS0 (IETF RFC 6891 [7]) for this distributed MEC environment purpose.

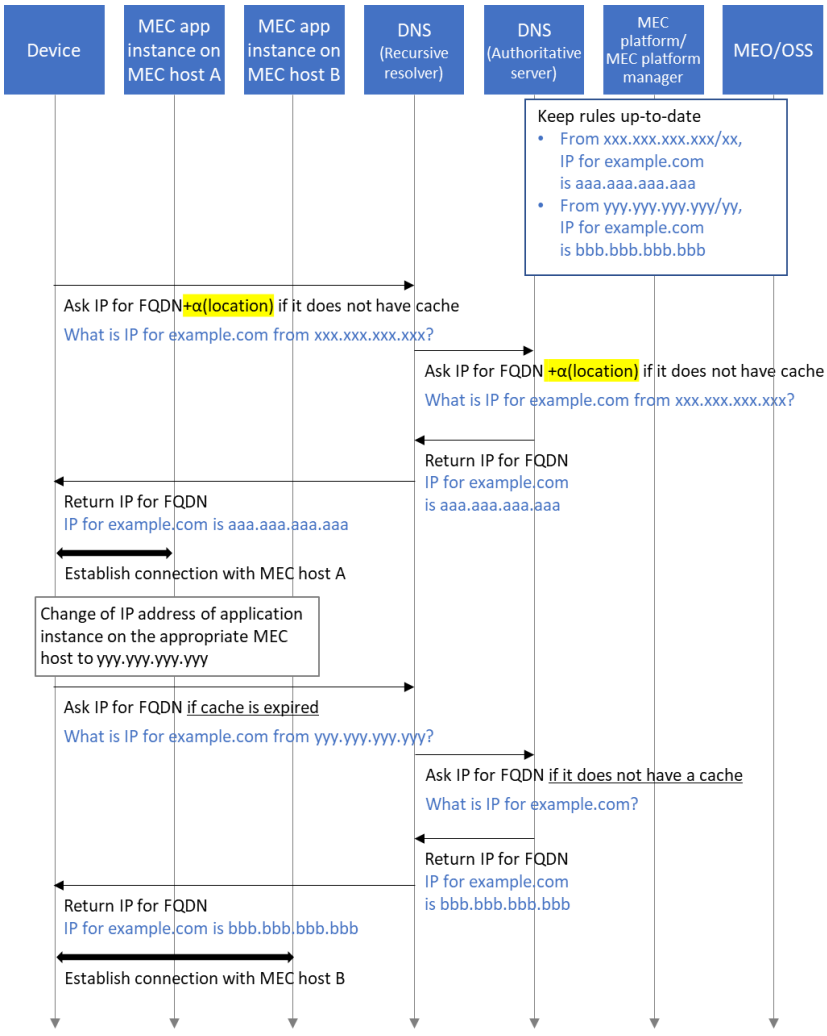

Figure 5: High-level message flow to establish connection with MEC hosts using ECS

5.2.1.2 Evaluation

To fulfil Requirement 1, the parameters to specify the optimized MEC host should be included in the header of EDNS0.

To fulfil Requirement 2, same as for the requirement 1, the parameters to specify the device should be included in the header of EDNS0.

To fulfil Requirement 3, since the IP resolution process is triggered by the device, time to live (TTL) should be sufficiently short. Note that the appropriate TTL configurations are for further study. For instance, if TTL is long, the device cannot connect to the updated MEC host as soon as serving host becomes inappropriate. If it is short, the devices too frequently ask DNS to resolve IP addresses, which may cause too much consumption of DNS server resources by the devices. As an alternative to fine tuning TTL, triggering devices to update cache or redirect existing flows, as soon as DNS configuration changes, is a viable option.

In terms of the MEC systems, the solutions are perfectly aligned with the current MEC specifications. The extension is required only for DNS resolution procedures as described in 5.2.1.1 Description. If some parameters, e.g., geographical location, communication latency, computing resource availability, and other performance and availability related parameters, are required to be exposed to the device, ETSI GS MEC 016 [8] Device application interface can be further extended to support the required exposure.

Note: According to ETSI GS MEC 003 [4], the connectivity to the DNS server is provided only from the MEC platform. The interface directly from MEO/OSS is for further study.

5.2.2 HTTP redirection solution

5.2.2.1 Description

In the case where MEC system cannot provide DNS service that has sufficient capabilities of dynamic relocation, the MEC platform should support applications to redirect application layer queries, e.g., Hypertext Transfer Protocol (HTTP), to dynamically update the connection to the appropriate MEC host. The redirection function should cover all the possible MEC hosts that may be distributed in the wide area, and the function should be located in the front end of cloud system. In this White Paper, the function node is named Application Gateway (GW). In this context, the current DNS support is sufficiently capable of realizing this solution. As an assumption, Application GW and MEC system exchange the information that is required to decide the appropriate MEC host. Figure 6 illustrates the high-level message flow to establish a connection to the application instance located on MEC host A. Then, Figure 7 illustrates the high-level message flow to update the connection to the application instance located on MEC host B.

Note 1: After the notification in the figures, it might be better to periodically notify the status to Application Gateway in order to avoid unnecessary redirection.

Note 2: The interface between MEO/OSS and Application GW is not specified in ETSI GS MEC 003 [4], it needs to be further specified. The connectivity to the DNS server is provided only from the MEC platform. The interface directly from MEO/OSS is for further study.

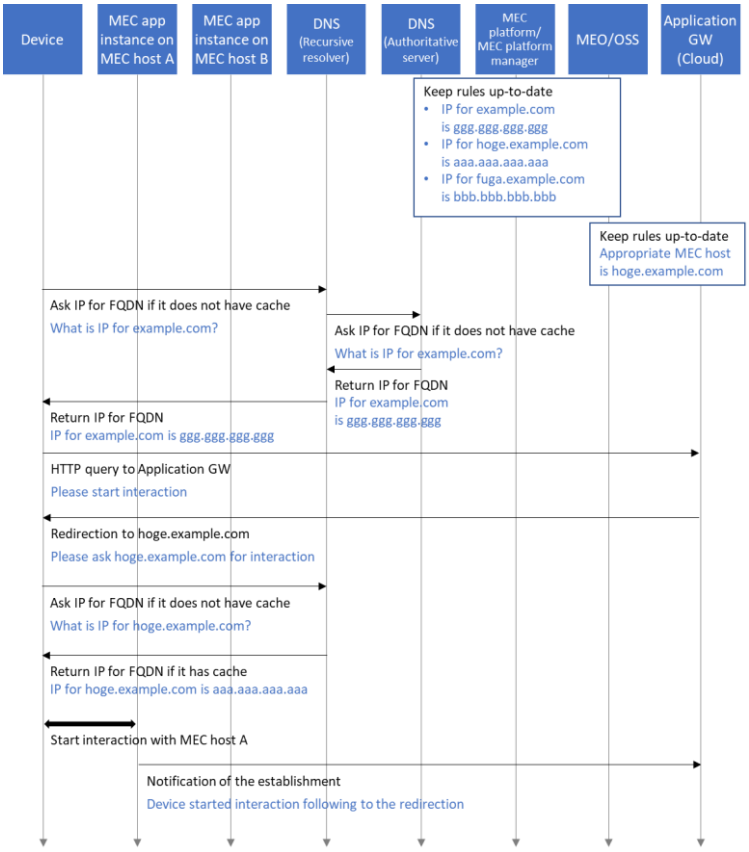

Figure 6: High-level message flow to start communication with MEC host A

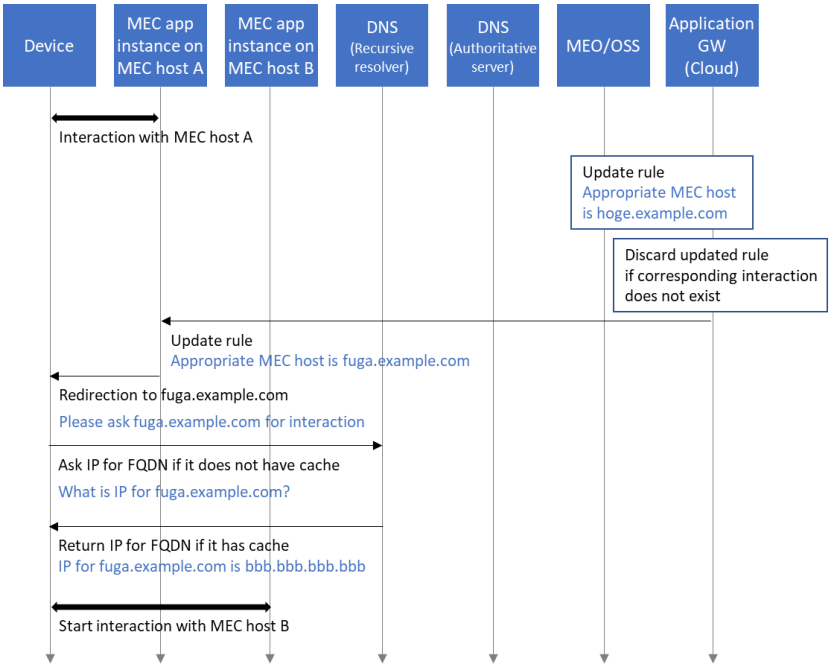

Figure 7: High-level message flow to update the connection to MEC host B

5.2.2.2 Evaluation

To fulfil Requirement 1, http queries or other queries of compatible application layer protocol should be extended to include extra parameters to decide the appropriate MEC host. The application GW resolves the appropriate MEC host based on the extra parameters. Then, the application instance redirects the http query to the target MEC host. Note that the application GW needs to be capable of dealing with it and MEC platform will support it, e.g., providing manifest for the resolve process. Application instance on a MEC host may need to collect the necessary information and transfer it to the application GW.

To fulfil Requirement 2, if more than 2 devices are connecting to the same application instance on the MEC host, the application instance can control the redirection individually. This solution can easily fulfil Requirement 2.

To fulfil Requirement 3, if the application is designed like the application GW immediately redirects the http query to the appropriate MEC host as soon as another MEC host becomes the most appropriate. Note that even if the serving MEC host becomes not the best MEC host, the device and the serving MEC host will be kept connected in order to properly start and complete the redirection procedures.

5.2.3 Device application interface solution

5.2.3.1 Description

As long as a device is able to communicate with the MEC system, i.e. it discovers the corresponding User Application Lifecycle Management Proxy and gets successfully identified and authorized, the device is enabled to use the device application interface API (DevApp API) that is specified in ETSI GS MEC 016 [8]. MEO notifies the URL of the target MEC application instance, or alternatively its IP address, via the API. The device may ask DNS, if it was served a URL, to know the corresponding IP address. It then establishes the connection to the target MEC Application Instance. An example message flow is depicted in Figure 8. The principles are basically the same as the HTTP redirection solution. Differently from the HTTP redirection solution, MEO/OSS directly notify the device of the URL/IP address.

As a premise, if using URL, application instances on different MEC hosts should be assigned with a different URL and those are appropriately defined in advance or dynamically.

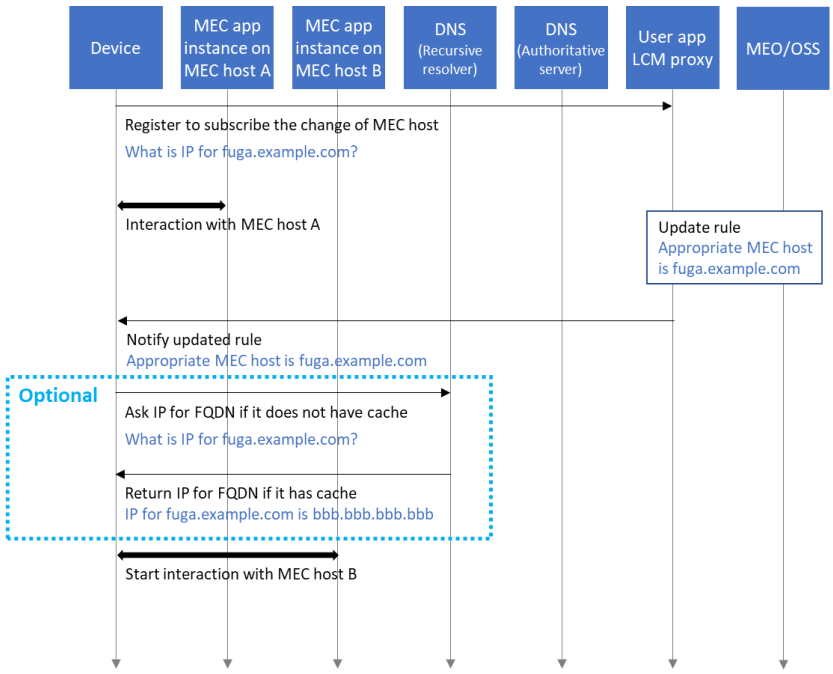

Figure 8: High-level message flow to update the connection to MEC host B

5.2.3.2 Evaluation

To fulfil Requirement 1, the MEO should monitor the performance metrics of the MEC Host at a location serving the user. If the MEO determines the need for a new application instance for the device, the MEO would notify the corresponding new address to the device. If the address is expressed in URI format, the device might need to ask DNS to resolve it to IP address. Alternatively, if the IP address is provided, the device traffic can be forwarded to the new IP address directly. Each device is able to communicate with MEC system independently from other devices. This solution naturally fulfils Requirement 2. The same as the HTTP redirection solution, if the MEO notifies the new application instance address as soon as the most appropriate MEC host changes, the update is completed in a real time manner. As a premise, the device will always be able to communicate with the MEC system.

5.2.4 Virtual IP solution

5.2.4.1 Description

Once an application instance links with a virtual IP address, the MEC application instance keeps its IP address until it is deleted even if the connecting entity moves from one MEC host to another as depicted in Figure 9. Each host links with the specific IP address individually and serving MEC host is dynamically selected according to the network location of the device without any additional procedures appeared in the other solutions. Note that the nearest in this context means that the topological (not necessarily geographical). The high-level message flow is depicted in Figure 10. However, it might be difficult for the network operator and application provider to control the serving MEC host as they intend, and the application might suffer from the unexpected disruption. In addition, an application requires to reserve a unique IP address across the entire MEC system network and assign it to all the MEC hosts, in order to

avoid IP address conflict between virtual IP address and IP address in MEC host's IP address pool. Note that how to deal with the stateful application is for further study.

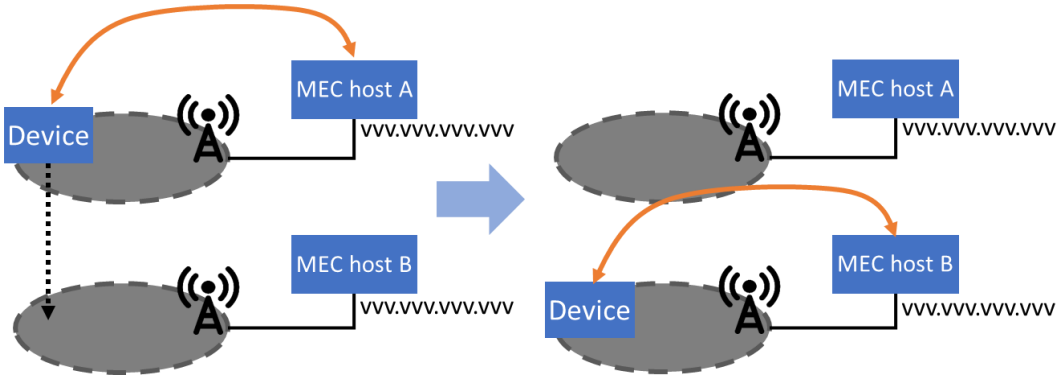

Figure 9: Expected behavior in the case of Virtual IP (also known as IP anycast)

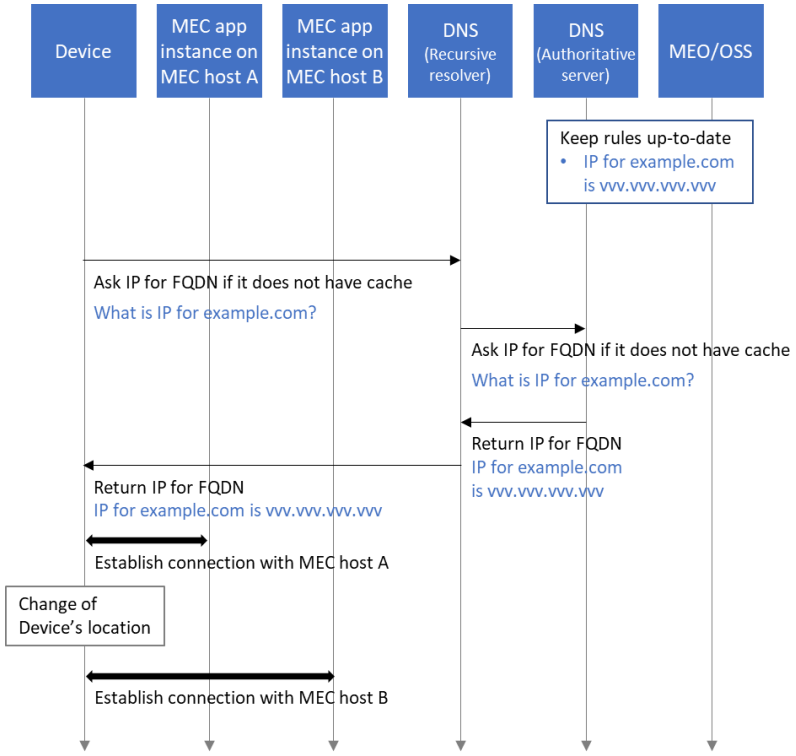

Figure 10: High-level message flow to establish/update connection to MEC hosts

5.2.4.2 Evaluation

Regarding Requirement 1, this solution can be equivalent with dealing with location information. Regarding R-2, each device individually connects to the nearest host. No extension is required in terms of MEC specification.

5.2.5 Edge DNS server solution

5.2.5.1 Description

Each MEC host is associated with a DNS Server (Edge DNS Server), to satisfy latency-minimization requirements. Such DNS Servers constitute the lowest layer of a DNS hierarchy thus they are able to act as recursive resolvers toward upper level DNS Server(s). In addition, they can be programmed to store locally FQDN-IP associations that overwrite responses, for the same FQDN, coming from the upper level DNS Servers. A possible mechanism to implement this behavior is RPZ (Response Policy Zone) - see DNS Response Policy Zone [9]. Queries for FQDNs that do not match any RPZ entry are instead forwarded to upper DNS Server and the relevant response is handled in the usual manner.

The device acquires the Edge DNS Server address in a deployment-dependent way (e.g. Dynamic Host Configuration Protocol (DHCP)) while attaching to a specific MEC Host. While the device moves and comes under coverage of another MEC Host, the Edge DNS Server address on the device can be updated, again in a deployment-dependent way (e.g. DHCP renewal containing a different DNS server address).

MEO configures each MEC Host with a specific FQDN-IP association. Such association is bound, as an ETSI-MEC DNS rule, to a particular MEC Application. The FQDN of the rules is the same, but the IP address is different based on the MEC Host. In this way, the device resolves the same FQDN to a different IP address, based on its position, and ends up communicating with the MEC Application instantiated on the MEC host the device is attached to.

See the figure 11 below which shows an example message flow.

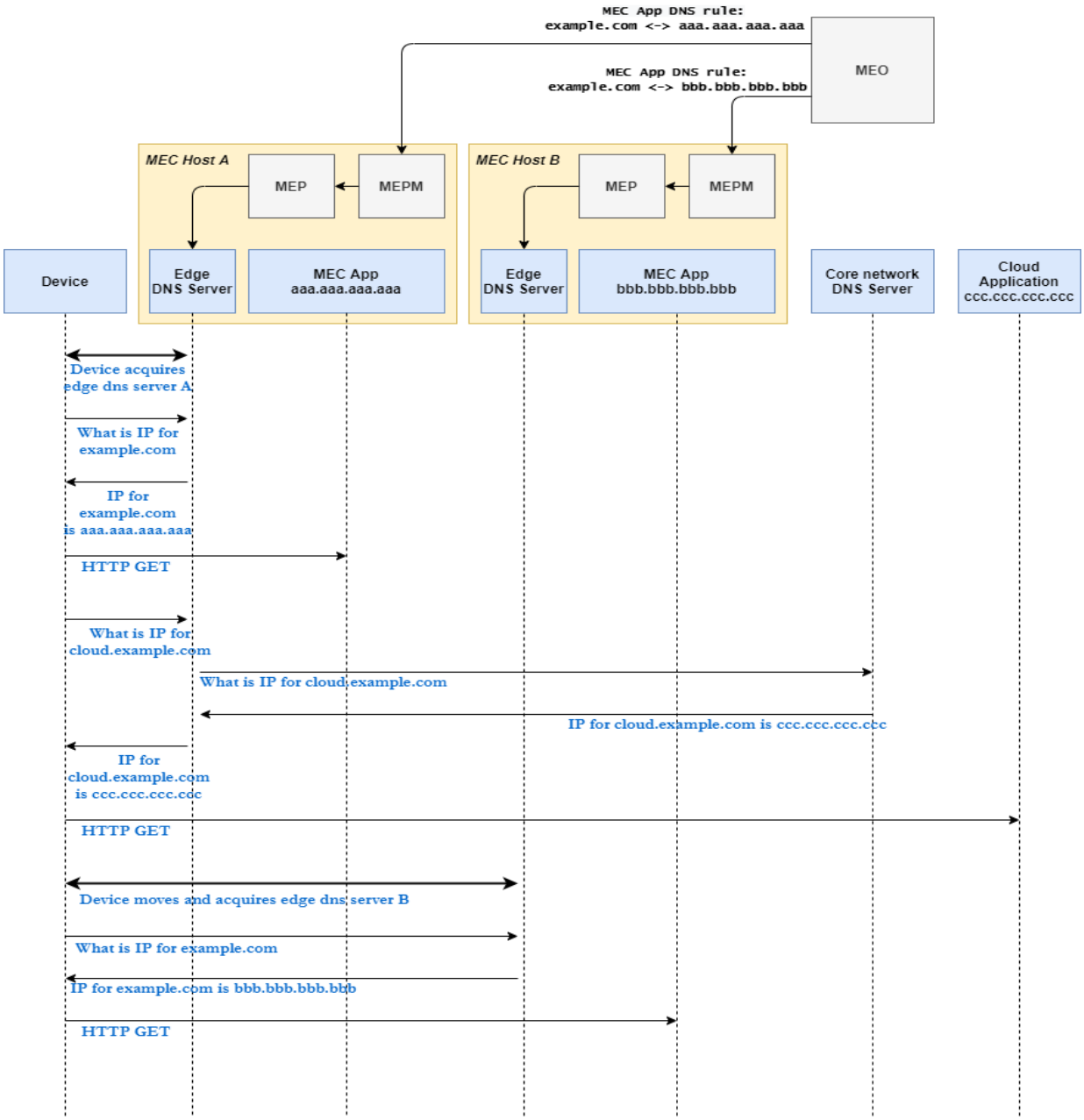

Figure 11: High-level message flow to establish/update connection to MEC hosts

5.2.5.2 Evaluation

To fully satisfy requirement 1, the MEO should be able to configure additional properties, reflecting the metrics mentioned in Requirements paragraph (device identifier, location, etc.), on the DNS rule. This requires an extension to the current ETSI-MEC standard interfaces, e.g. mm3. The Edge DNS Servers should also support some kind of geolocation mechanism (or other previously proposed DNS protocol extensions) that work in conjunction with the above mentioned RPZ feature.

Requirement 2 is satisfied by design.

Requirement 3 is satisfied by the design, but how long the updates can take depends on the way the device gets to know of the new Edge DNS Server. In case of basic DHCP, the timing depends on the DHCP lease time. The TTL of the FQDN-IP association on the device influences the update time too.

6 Conclusion

In this White Paper, we introduced the list of deployment options suitable to support the distributed MEC environment, in terms of providing the connectivity between devices and application instances. The following table summarizes all identified solutions and clarifies if each potential solution satisfies each requirement. The quantitative evaluation is not conducted in this White Paper and we do not decide which solution is the best for deployment. Hopefully, the MEC provider will decide according to their own situation together with mobile network operators, application providers, and other relating service providers.

Options	Requirement 1	Requirement 2	Requirement 3
3GPP applicable solution			
Enhancement of support for edge computing in 5G core network	We cannot evaluate if the solution satisfies the requirement since the study item is on-going.		
More Informed DNS Query solution for local DNS services in 5GC	Satisfied if MEC host is capable of interaction with 5G NEF.	Satisfied but the authoritative DNS needs collaboration with edge DNS.	Satisfied if application on device is sufficiently aware of the service connection condition, or if service provider leverage 5G NEF interface.
Generally applicable solutions			
Enhanced DNS solution	Satisfied for location, ECS supports resolve procedures. Not satisfied for other metrics, the extension of EDNS0 is required.		Satisfied but the TTL should be appropriately configured.
HTTP redirection solution	Satisfied if the extra parameters and redirection procedures are dealt by the application instances.	Satisfied since the redirection is individually controlled for each device.	Satisfied but the application instance should be notified of the changes of device conditions and trigger the redirection procedures immediately.

Device application interface solution	Satisfied if MEC platform supports dealing with the extra parameters.	Satisfied as the notified URL can be made device-specific.	Satisfied as the MEC system notifies the device of the URL/IP address change through the notification interface of the DevApp API.
Virtual IP solution (IP anycast)	Not satisfied since the selection cannot be controlled from the operator side.	Satisfied since the device automatically connects to the nearest host.	Satisfied if the connection would be updated as soon as the nearest host changes.
Edge DNS Server Solution	Satisfied if MEO is able to set additional properties on the DNS rule	Satisfied since the device, by connecting to the nearest host, queries the edge DNS server and obtains a host-specific IP address	Satisfied but TTL and DHCP lease time should be appropriately configured

Definition of abbreviations

For the purpose of this White Paper, the abbreviations given apply.

3GPP	3rd Generation Partnership Project
5GC	5G Core Network
API	Application Programming Interface
AR	Augmented Reality
CoSP	Communication Service Provider
CSP	Cloud Service Provider
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ECS	EDNS client subnet
EDNS	Extension Mechanisms for DNS
FQDN	Fully Qualified Domain Name
GW	Gateway
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
ISG	Industrial Specification Group
ITS	Intelligent Transportation System
LCM	Life Cycle Management
LTE	Long-Term Evolution
MEC	Multi-access Edge Computing
MEO	MEC Orchestrator
OEM	Original Equipment Manufacturer
OSS	Operations Support System
QoS	Quality of Service
QoE	Quality of Experience
RPZ	Response Policy Zone
TTL	Time To Live
UE	User Equipment
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
V2X	Vehicle to Everything
VR	Virtual Reality

References

[1] 5G Automotive Association, Toward fully connected vehicles: Edge computing for advanced automotive communications, https://www.etsi.org/images/files/ETSIWhitePapers/ETSI_White_Paper_Network_Transformation_2019_N32.pdf.

[2] GSMA, Cloud AR/VR Streaming:Accelerate mass adoption and improve quality of experience of AR/VR using 5G and edge cloud, https://www.gsma.com/futurenetworks/wp-content/uploads/2019/03/Cloud-ARVR-booklet-for-MWC19.pdf.

[3] ETSI GS MEC 030 V2.1.1, Multi-access Edge Computing (MEC);V2X Information Service API, https://www.etsi.org/deliver/etsi_gs/MEC/001_099/030/02.01.01_60/gs_MEC030v020101p.pdf.

[4] ETSI GS MEC 003 V2.1.1, Multi-access Edge Computing (MEC); Framework and Reference Architecture, https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/02.01.01_60/gs_MEC003v020101p.pdf.

[5] 3GPP TR 23.748, Study on enhancement of support for Edge Computing in 5G Core network (5GC), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3622.

[6] Internet Engineering Task Force, Request for Comments: 7871 Client Subnet in DNS Queries, https://tools.ietf.org/html/rfc7871.

[7] Internet Engineering Task Force, Request for Comments: 6891 Extension Mechanisms for DNS (EDNS(0)), https://tools.ietf.org/html/rfc6891.

[8] ETSI GS MEC 016 V2.2.1, Multi-access Edge Computing (MEC); Device application interface, https://www.etsi.org/deliver/etsi_gs/MEC/001_099/016/02.02.01_60/gs_MEC016v020201p.pdf.

[9] “DNS Response Policy Zone,” Available: https://dnsrpz.info/

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org