Workgroup: Network Working Group
Internet-Draft:
draft-du-intarea-service-routing-in-mec-01
Published: 10 July 2022
Intended Status: Informational
Expires: 11 January 2023
Authors: Z. Du
China Mobile

Service Routing in Multi-access Edge Computing

Abstract

This document introduces a service routing mechanism in the scenario of Multi-access Edge Computing.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 11 January 2023.

Copyright Notice

Table of Contents

1. Introduction

The operators are deploying Multi-access Edge Computing (MEC) to provide services with lower latency to their users. Comparing to accessing service in the clouds, the MECs can provide service much nearer to the users.

However, in the current architecture of Internet, we need to send a DNS query to get the IP address of the service firstly, and then access the service [RFC1035]. It is not the optimal solution in the MEC scenarios which are sensitive to the latency of service accessing. In this document, we introduce a mechanism that can access the service directly without the DNS procedure.

In the 5G architecture, a UE (User Equipment) need to connect to a UPF (User Plane Function) working as a gateway by using a tunnel, and then access service via the destination IP address.

In the scenarios of MEC, the service may be accessed within the MEC, meanwhile the MEC also provides a UPF Function for the UEs. Therefore, in fact, the service access takes place in a limited domain [RFC8799]. In this limited domain, we can use a specific IP address to directly access the service.

2. Proposed Mechanism Description

In the proposed mechanism, a UE should have a session with the UPF in the MEC. Also, the UE should be aware that it can access the service more quickly within the MEC if the service is available in the MEC. The proposed mechanism is described briefly as below.

Firstly, the UE send a normal DNS query if it wants to access a service, such as "www.local-weather.com". Meanwhile, it can make a destination IP address itself by hashing the domain name, and try to establish a TCP connection directly.

Secondly, the UE may establish the connection successfully by using the specific IP address, and get access to the service bypassing the DNS procedure. If it fails, the UE can wait for the normal destination IP address received from the DNS procedure.

In this mechanism, the specific IP address can contain some information about the service, so we call it service routing in this document. The specific IP address is called the Service Routing IP address.

3. Service Routing IP Address

There are several options for the Service Routing IP address.

In the first option, we can assume that the UE can receive an MEC prefix for the service routing in the procedure of establishing the session between the UE and the UPF in the MEC. For example, the length of an MEC prefix is 64 bits, and the length of the hashed domain name is also 64 bits. In the MEC, the server of the service should use the same hash algorithm to generate the Service Routing IP address, and the 128 bits IPv6 address should be routed correctly within the MEC. Hence, the MEC works like a virtual network node containing services, with the MEC prefix as a Location, and the hashed domain name as a Function.

In the second option, we can use a ULA IP address (Unique Local Address) for the Service Routing IP address [RFC8799]. The procedure is similar to the first option, but the Service Routing IP address becomes the format of <MEC_ULA_Preifx: Hashed_Domain_Name>. The MEC_ULA_Prefix contains a specific subnet-ID.

In the last option, we can use all the 128 bits as the Hashed_Domain_Name. In this situation, the UE does not need to receive a specific prefix in advanced, and all the services in different MECs have the same IP address for the same service to support this quick access.

4. Requirements of Service Routing Network Nodes

In the MEC, the network should support forwarding the Service Routing IP. In the client and server, they should support the binding of the Service Routing IP and the traditional DA IP. The value of the Service Routing IP exists mainly in the period of establishing the connection. After the connection is established, we can use the normal DA IP instead.

5. HASH Conflict between Services

At the beginning of the adoption of the mechanism, we do not think there would be too many essential services requiring this ultimate user experience, so that we assume that there would be no Hash conflict between the services. If the mechanism is adopted widely, and conflict exists between hashed domain names in the MEC, we can enable the mechanism only on the most essential service. Another option is to change the HASH algorithm that is running on the clients and the severs to make a better Hash result.

6. Service Routing for Fixed Clients

MEC can also support accessing via fixed clients. In this situation, the BNG (Broadband Network Gateway) as the gateway of the client can work similarly to the UPF. A tunnel between the BNG and the MEC may be needed, and the MEC prefix can be obtained in the procedure of authentication. In the authentication of a fixed client, a more static session can be established because the client will not move.

7. IANA Considerations

TBD.

8. Security Considerations

TBD.

9. Acknowledgements

TBD.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC8799] Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", RFC 8799, DOI 10.17487/RFC8799, July 2020, <https://www.rfc-editor.org/info/rfc8799>.

10.2. Informative References

[RFC1035]
Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

Author's Address

Zongpeng Du
China Mobile
No.32 XuanWuMen West Street
Beijing
100053
China

Email: duzongpeng@foxmail.com