

INTERNET-DRAFT  
Intended Status: Proposed Standard  
Expires: September 11, 2017

J.Wei Ed.  
F.Yang  
Huawei Technologies  
March 10, 2017

Anchor-less Mobility Management Solution  
draft-wei-anchorless-mm-00

## Abstract

This memo discusses an anchor-less mobility management solution based on ID/Locator split scheme, especially for VM handoff scenario in MEC network.

## Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/lid-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

## Copyright and License Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

INTERNET DRAFT

<Document Title>

March 10, 2017

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">1.1</a>	Terminology . . . . .	<a href="#">4</a>
<a href="#">2</a>	Mobility Management Gap Analysis . . . . .	<a href="#">4</a>
<a href="#">3</a>	Mobility Solution Based on ID/Locater Split . . . . .	<a href="#">5</a>
<a href="#">4</a>	Relations with Existing DMM Solutions . . . . .	<a href="#">8</a>
<a href="#">5</a>	Security Considerations . . . . .	<a href="#">8</a>
<a href="#">6</a>	IANA Considerations . . . . .	<a href="#">8</a>
<a href="#">7</a>	References . . . . .	<a href="#">8</a>
<a href="#">7.1</a>	Normative References . . . . .	<a href="#">8</a>
<a href="#">7.2</a>	Informative References . . . . .	<a href="#">9</a>
	Contributors: . . . . .	<a href="#">9</a>
	Authors' Addresses . . . . .	<a href="#">9</a>

INTERNET DRAFT

&lt;Document Title&gt;

March 10, 2017

## 1 Introduction

With the development of network technology, there are more and more services sensitive to network latency, for example, interactive VR, tactile Internet, remote control, automatic drive etc. Also low latency has become an important requirement in 5G network design. For service with low latency requirements, the network needs to meet its end-to-end latency requirements.

The MEC (Multi-access Edge Computing) sinks computing and storage capacity to the edge of the network. The MEC server is deployed at the edge of the network and applications could be deployed in the MEC server. This allows the MN to access the required services in close proximity without having to traverse through the core network, thereby reducing the end-to-end RTT, and satisfying latency requirements. One of the basic MEC deployment scenarios is shown in Figure 1:

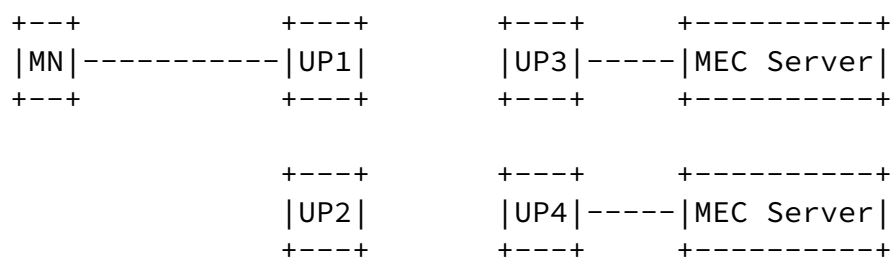


Figure 1: MEC Deployment Architecture

In order to meet the low latency requirements of network services, an alternative approach is to deploy services with low latency requirements in the MEC system. The MEC architecture is an effective means of addressing low latency requirements by deploying the application in an MEC server close to the terminal equipment.

Application instance runs in a MEC server, and the service connection

is established between application runs on MN and application instance runs on MEC server. When the MN moves in the MEC server's coverage area, in order to ensure continuity of the service, the connectivity between MN application and mobile edge application needs to be maintained. As MN moves further away from the location of the mobile edge application, there could be an increased latency between the MN and the mobile edge application. Due to this reason or others (e.g. network congestion), for some mobile edge applications, it might become necessary to relocate the application instance, i.e. relocating the application instance to a new MEC server near to MN's current location, in order to satisfy the latency requirements, when the application instance is relocated the service continuity need to

<Author>

Expires September 11, 2017

[Page 3]

---

INTERNET DRAFT

<Document Title>

March 10, 2017

be maintained. [[GS\\_MEC003](#)]

For instance, when the MN runs interactive VR (Virtual Reality) service, in order to guarantee the high bandwidth and low latency requirement of the VR's service, the MEC server is used to provide service for the MN, that is, the MEC server starts a VM (Virtual Machine) running the VR service for MN, when the MN moves far away from the original MEC server, if the nearest MEC server is available, the VM will be migrated to the new MEC server, and ensuring continuity of VR service. The case where the VM relocation follows MN's mobility is also referred as VM handoff [[Ha2015](#)].

This memo analyzes the mobility scenario of the correspondent node following the MN to avoid the redundancy of the route redundancy, and a mobility management solution based on the ID/Locator split scheme is provided.

## [1.1](#) Terminology

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](#)].

## [2](#) Mobility Management Gap Analysis

In the DMM, the on-demand mobility scheme [ODMM] is proposed, in which the network provides IP session continuity and IP address reachability based on application requirements. If the application requires both session continuity and IP address reachability, the

application chooses to use a fixed IP address; if the application needs IP session continuity but does not need IP address reachability, then the application will use Session-lasting IP Address; if the application neither need IP session continuity nor IP address reachability, then non-persistent IP Address will be used.

On-demand mobility scheme separate applications need IP session continuity from applications don't need IP session continuity , and then the network provides applications with different types of session continuity support based on this separation: for a application that does not require session continuity support, session continuity is not provided, and a new IP address is allowed to be used when the MN moves, in this way the routing redundancy problem could be avoided; for an application that needs session continuity support from the network, the network side sustains the IP address used by the MN during the movement of the MN, so that the IP address used by the application is not changed, however, this approach provides session continuity while also introduces routing redundancy for application traffic. The on-demand approach does not address the

mobility requirements in the VM handoff scenario described earlier.

The fundamental cause for the route redundancy is the dual attributes of the IP address: the network location attribute and the session identification attribute. The two communication sides use IP addresses to identify the session, so in order to maintain session continuity the IP addresses need keep the same, but because IP address also determines network location, when the IP address keeps the same the service traffic flows back to the IP address's IP anchor, which leads to routing redundancy problem.

### [3](#) Mobility Solution Based on ID/Locator Split

ID/Locator separation scheme separate ID attribute from Locator attribute in one IP address, it can be a good choice to solve the routing redundancy problem caused by mobility.

In this memo, the architecture of network-based mobility management solution based on the concept of ID/Locator split is discussed which is also align with DMM working group's existing CP-UP separation architecture. Figure 2 illustrates an overview of the mobility solution architecture.

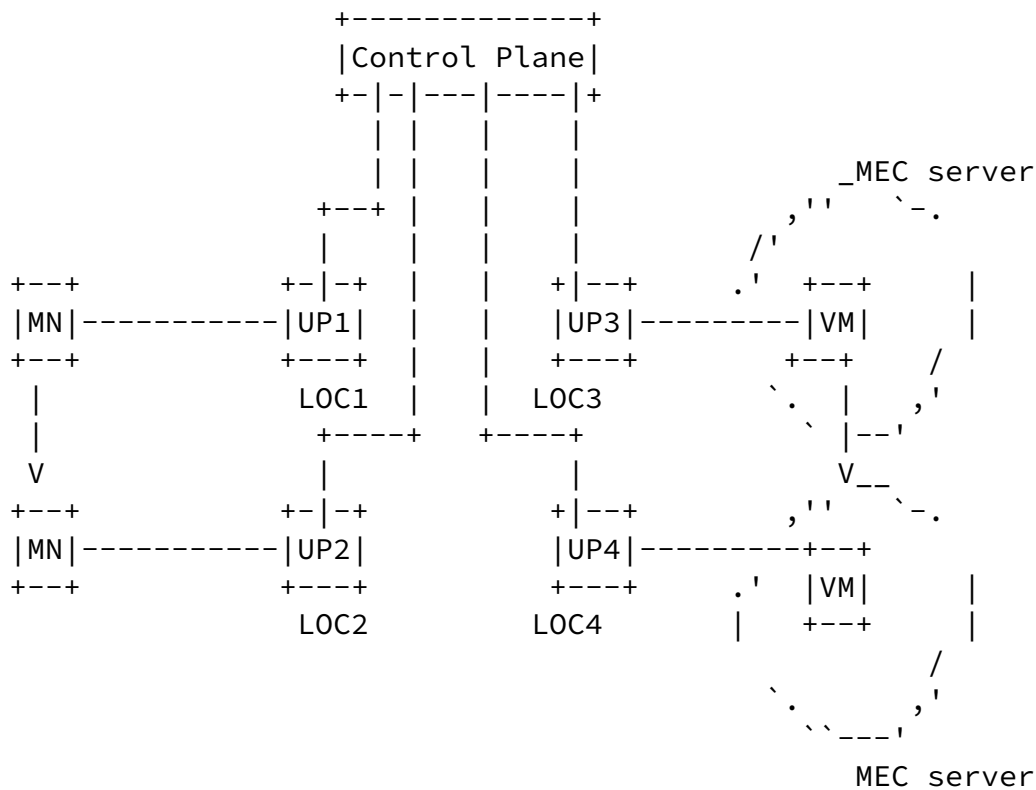


Figure2: Mobile Management Architecture Based on ID/Locator Separation

UP1 to UP4 are data plane functions. They are responsible for the

management of Locator, packet encapsulation and decapsulation, packet forwarding, signaling interaction with Control Plane (for example, ID/Locator relationship update).

The Control Plane is responsible for maintaining the mapping of ID/Locator and configuring the ID/Locator to the corresponding UP to control UP's processing of the packet.

In order not to modify the existing mobile terminal, the two sides of communication in the scheme still use the 5-tuple to identify the session. It is assumed that the IP addresses used by the MN and CN in the communication are IP-mn and IP-cn respectively. During communication, IP-mn and IP-cn only act as IDs, which are used to identify sessions, but are not used as locators. UP1 to UP4 is responsible for allocating Locator for MN and CN.

When the MN is located at UP1, a communication connection is established with MN's correspondent node VM , at which time the VM accesses UP3. The packet between MN and the VM is transmitted through the tunnel established between UP1 and UP3, where the outer header of the tunnel uses the locator assigned by UP1 and UP3.

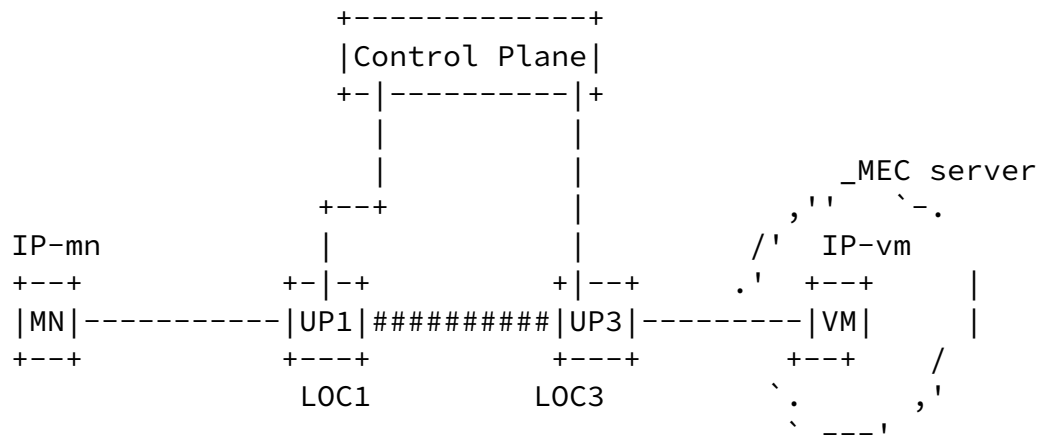
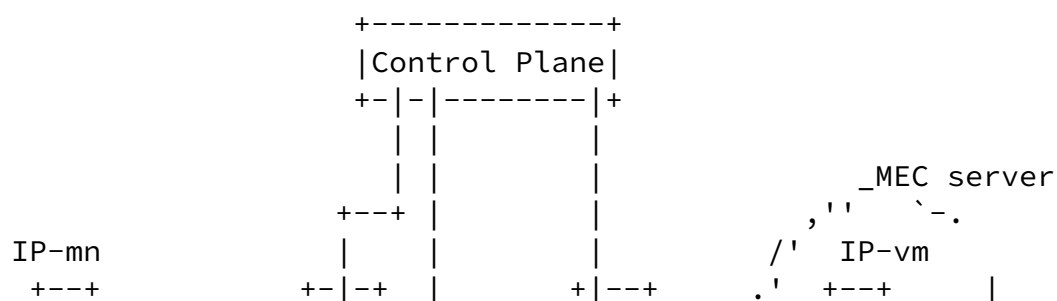


Figure3: Communication Connection before Movement Occurs

When the MN moves to UP2, the communication between the MN and the VM adopts the make-before-break mode. The MN communicates with the VM instance located at the UP3 position until the VM instance completely relocated to the UP4 position. During this period, packets are transmitted through tunnels between UP2 and UP3. The outer header of the tunnel uses the locators assigned by UP2 and UP3.





[Page 7]



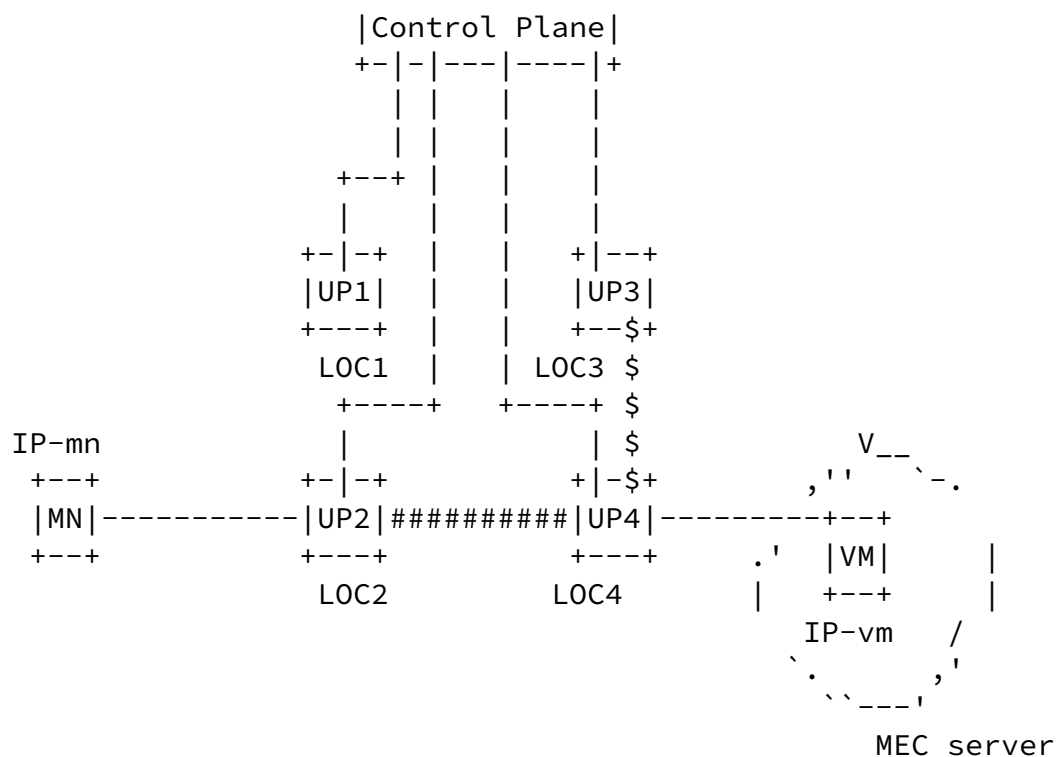


Figure5: Communication Connection after Movement

NOTE: The interaction signaling between Control Plane and User Plane is TBD.

#### [4](#) Relations with Existing DMM Solutions

TBD.

#### [5](#) Security Considerations

TBD.

#### [6](#) IANA Considerations

TBD.

#### [7](#) References

##### [7.1](#) Normative References

[KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate

Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

## [7.2](#) Informative References

- [EVILBIT] Bellovin, S., "The Security Flag in the IPv4 Header", [RFC 3514](#), April 1 2003, <<http://www.rfc-editor.org/info/rfc3514>>.
- [RFC5513] Farrel, A., "IANA Considerations for Three Letter Acronyms", [RFC 5513](#), April 1 2009, <<http://www.rfc-editor.org/info/rfc5513>>.
- [RFC5514] Vyncke, E., "IPv6 over Social Networks", [RFC 5514](#), April 1 2009, <<http://www.rfc-editor.org/info/rfc5514>>.
- [GS\_MEC003] Mobile Edge Computing (MEC); Framework and Reference Architecture, Mar 2016.
- [Ha2015]
- [ODMM]

## Contributors:

I would like to acknowledge the contribution of the following people to the document:

Rui Meng, mengrui@huawei.com

Cheng Chen, chencheng@huawei.com

## Authors' Addresses

Jackie Wei

Huanbaoyuan Q22, Haidian District, Beijing, China

EMail: weixinpeng@huawei.com

Fei Yang

Huanbaoyuan Q22, Haidian District, Beijing, China

<Author>

Expires September 11, 2017

[Page 9]

---

INTERNET DRAFT

<Document Title>

March 10, 2017

yangfei15@huawei.com

<Author>

Expires September 11, 2017

[Page 10]