Mobile-Optimized Future Internet (MOFI):

Architecture and Protocols

(Release 1)

July 2009

Heeyoung Jung* and Seok Joo Koh**

*Electronics Telecommunications Research Institute (ETRI), hyjung@etri.re.kr

**Kyungpook National University (KNU), sjkoh@knu.ac.kr

Summary

This memo presents the architecture of Future Internet for mobility optimization, named the Mobile Optimized Future Internet (MOFI). We first discuss a set of design considerations to be taken, and design the MOFI architecture. We then describe some protocols associated with MOFI: Access Network Protocol (ANP) and Backbone Network Protocol (BNP), User Identifier Resolution Protocol (URP), and Mobility Control Protocol (MCP). The MOFI is purposed to be used as a building block component for overall design of Future Internet architecture.

TABLE OF CONTENTS

1. MOTIVATIONS

With an explosive growth of the number of subscribers of 2G/3G cellular systems and also other wireless data systems such as WiFi and WiMAX, the mobile/wireless networks now become the key driver toward the Future Internet. It was reported that there were over 2 billion cellular phones, compared to 500 million desktop PCs in the year of 2005, and more than 400 million cellular phones were already equipped with capability of Internet access. In addition, a variety of new types of wireless access networks like ad-hoc networks and sensor networks are emerging, and they will be the major access means to Future Internet.

However, it is noted that the current Internet was basically designed for fixed network environment, rather than for mobile/wireless network environment. This has enforced Internet to add some extensional features to satisfy the requirements for wireless/mobile networks, as shown in the example of Mobile IP (MIP) [1, 2]. However, such **patch-on** approach seems to be just a temporal heuristic to the mobility problems, rather than an optimization approach to substantially solve the mobility-related issues.

Based on these observations, some activities already started to design the Future Internet for wireless/mobile environment rather than fixed environment. A typical example is eMobility [3] which is a project of EU FP7. eMobility says that the first generation Internet had been developed mainly for research purpose, and many new protocols have been patched to support commercial requirements in the second generation Internet. Now, eMobility envisions the third generation Internet as the wireless/mobile Internet with the name of Post-IP with advanced capabilities such as wireless QoS, enhanced traffic management, mobility, location awareness, and so on. Also, the considerations on wireless/mobile environment are being taken in the other FP7 projects for architectural design for Future Internet such as 4WARD [4] and Trilogy [5].

GENI [6], a representative testbed project for Future Internet, also notes that wireless/mobile will be the major access means for Future Internet. Some design documents of GENI already covers the issues including ad-hoc and sensor networks. We can also find many FIND projects that are very closely related with wireless/mobile environments [7]. On the other hand, it is noted that the current Internet needs to be substantially changed so as to effectively support the future All-IP networks that consist of a lot of new revolutionary radio technologies such as IMT-advanced or beyond [8].

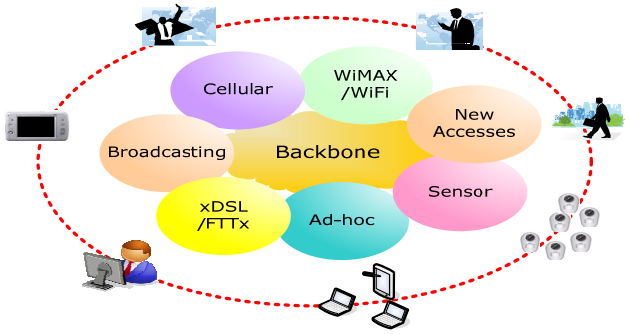
With these observations, we will try to design an architecture of Mobile-Optimized Future Internet (MOFI) to effectively realize seamless mobility in the Future Internet. Based on the MOFI architecture, we present some protocols to provide the mobility functionality in Future Internet.

The main objective of this memo is that the proposed MOFI architecture and its associated protocols could be incorporated as a building block component into the design of overall architecture of Future Internet.

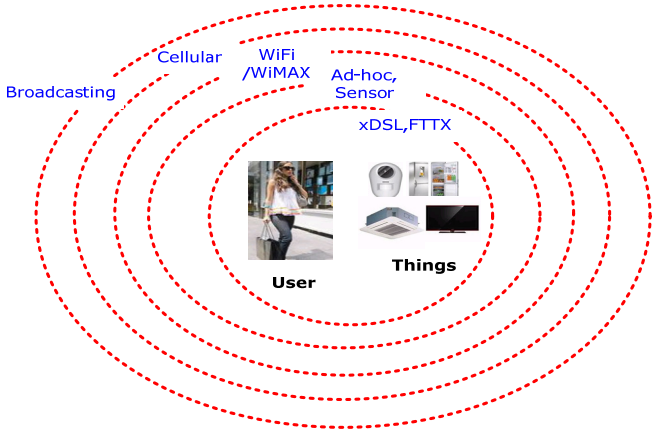
2. DESIGN CONSIDERATIONS

2.1 NETWORK ENVIRONMENT IN FUTURE INTERNET

To design the Future Internet architecture, we first consider network environment envisioned in the Future Internet. Figure 1 illustrates the environment of Future Internet in the perspectives of network and users/things. The figures below show just a logical representation of Future Internet, rather than the physical network architecture.



(a) Network perspective



(b) Users/Things perspective

Figure 1 – Network environment envisioned in Future Internet

In Future Internet, users will benefit from a variety of access ways to the network anytime and anywhere. Communications in Future Internet will be required for 'things' as well as 'human users.' In particular, it is expected that 'mobile' users/things will become dominant, rather 'fixed' ones, in Future Internet. In this context, a crucial requirement for Future Internet is to provide seamless services for the mobile users/things through the mobile optimized Future Internet.

2.2 ESC VISION: EASINESS, SAFETY, AND CHEAPNESS

The architecture of MOFI needs to be designed in the user perspective rather than in the network provider perspective, since Future Internet will be as a social infrastructure, not just for industrial business. In a highly abstract level, Future Internet can be viewed as a 'sphere,' as depicted in Figure 2. The sphere would be a 'virtual media' used for communication between people. People will not care what happens inside the sphere during communication. That is, the sphere is just a black box and completely hidden to people. People will move around freely and communicate with others by way of the communication sphere. In this context, the communication sphere is Future Internet.

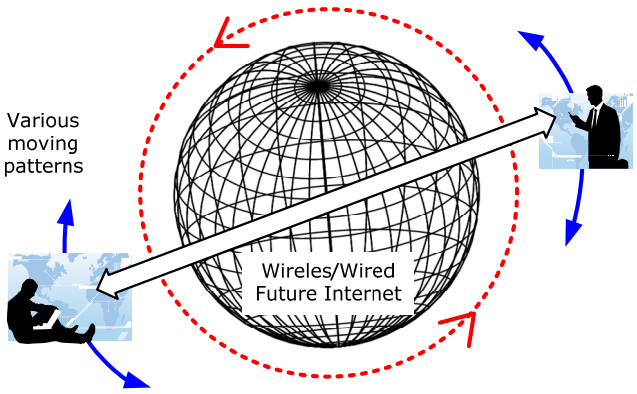


Figure 2 – Communication sphere as Future Internet

From this communication sphere, we can identify the following high level requirement for Future Internet as a vision: "**Future Internet should be able to provide all the people with communications easily, safely and cheaply,**" which gives us the following **ESC vision** for Future Internet.

- Easiness

  Users should be able to access the network **easily (E)** regardless of their intellectual level, age, culture, etc, since Future Internet is a social infrastructure for all the people in the world.

- Safety

  Future Internet should be able to provide people with communications **safely (S)** so as to guarantee people's communication privacy and to prevent the malicious attacks.

- Cheapness

  Future Internet should ensure that people can use the network as **cheaply (C)** as possible, since Internet services will become a part of people's daily life. That is, all the people in the world should be able to use Internet services, regardless of their wealth. In the deployment perspective, the infrastructure of Future Internet should be able to be built in the cost-effective manner.

This ESC vision implies that Future Internet will be able to **escape** from the limitations of the current TCP/IP by simply pushing the **ESC** button and realize seamless mobility, as shown in the figure below.

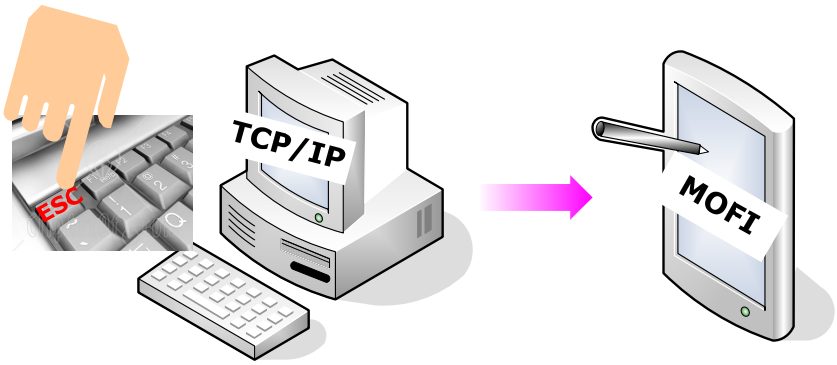


Figure 3 – Escape from the current TCP/IP toward Mobile Optimized Future Internet

2.3 DESIGN GOALS

Our primary goal is to develop the architecture of MOFI. Such architectural design works include a lot of technical issues such as mobility, QoS, security, network management, traffic engineering, AAA, etc. Among these, we will first focus on the **mobility** issue, since the mobile/wireless optimized Future Internet is one of the most essential requirements for Future Internet.

The MOFI is designed with the following design goals.

2.3.1 MOBILE-OPTIMIZED AND STATIC-ALLOWED

The current Internet basically assumes that a host (user equipment) is static. However, it is envisioned that wireless/mobile hosts will become dominant in the Future Internet. Accordingly, we will focus on the design of architecture that is **optimized to mobile users/hosts** and at the same time that **allows static users/hosts.**

2.3.2 ID-BASED COMMUNICATION

In the current cellular networks, a user does not need to know the corresponding user's location information that will be managed in the network (system). The only requirement for communication is to know the identifier (ID) of the corresponding user. This feature facilitates an easy access of users to the network for communication. MOFI will be designed for ID-based communication, in which a user needs to know only the ID of the corresponding user for communication without knowledge of its location. The detailed mapping between ID and locator will be managed by network.

2.3.3 SEPARATION OF IDENTIFIER AND LOCATOR

Identifier (or user identifier) is used to identify a user or host in the network, whereas **locator** is used to represent the current location of the user in the network. Locator can be also used for packet routing/delivery in the network.

In the current Internet, an IP address is used as identifier as well as locator in the network. In terms of mobility, a user identifier needs to be separated from its locator, since the locator may change by user's movement, but the identifier will not change. That is, an identifier should be used only to identify a user in the viewpoint of services provisioning, and a locator should be used so as to locate the user and to deliver packets in the network.

In MOFI, we will primarily consider a name (e.g., bill@microsoft.com) or a number (e.g., telephone number) as user identifier, whereas an IP address will be used as a locator. More specifically, an IP address of the access router that a user is connected to will be used as a locator of the user in the network. Note that the use of the other type of locator is for further study.

2.3.4 ADDRESS-FREE USER HOST

In terms of mobility, another problem of the current Internet is that a user host must configure its own IP address in the network. When a mobile host moves into a new network by handover, it should configure its new IP address (by using DHCP or IPv6 stateless auto-configuration). This address configuration tends to result in quite a long handover delay. One promising way to solve this problem is that a user host does not configure its own address, so as to minimize the performance of mobility or handover. This is in the same line with the design goal, "**ID-based communication.**"

In MOFI, a user identifier will be decoupled from a user locator. A name or number will be employed as a user identifier, whereas IP address of the access router connected to a user will be used as a locator. That is, each host does not need to configure its IP address in the network. In the user side, all the functionalities for communication will be performed only with its identifier, without configuring its IP address.

2.3.5 LOCATION PRIVACY

In the current Internet, a packet header includes the IP address of the sender host. It implies that the sender's location may be revealed to the correspondent user, irrespective of the sender's intention. This results in the location privacy problem.

In MOFI, the location privacy can be provided for the users with the design goals of **separation of identifier from locator** and **address-free user host**. That is, the location of the sender can be hidden to the correspondent user (possibly to the malicious attacker in the network).

2.3.6 SEPARATION OF MOBILITY CONTROL PLANE AND DATA TRANSPORT PLANE

We note that the signalling information conveyed in the control plane is usually mission-critical, and thus it requires the fast and reliable delivery in the network by using out-of-band or dedicated transmission channels. That is, user data and control information need to be processed differently, as shown in the cellular system in which the mobility control functionality is separated completely from the user data transport.

Accordingly, MOFI is designed to separate the mobility control from the user data delivery, which will also facilitate the deployment of many different mobility control schemes into a variety of network systems, independently of the underlying data transport schemes.

2.3.7 NETWORK-BASED MOBILITY CONTROL

From the comparison of MIPv6 [2] and Proxy MIPv6 (PMIPv6) [9], we note that the network-based mobility scheme is preferred to the host-based mobility scheme in the viewpoint of resource utilization, protocol performance and deployment. MOFI is in pursuit of the network-based mobility control. Moreover, the network-based mobility control will be designed in the fashion of '**built-in the Future Internet**,' rather than '**add-on the current Internet.**'

2.3.8 INTRINSIC ROUTE OPTIMIZATION FOR DATA DELIVERY

MIP has the **triangle routing** problem, in which the data path between two hosts will be optimized only after an additional route optimization operation is completed. In MOFI, the routing path between those two hosts should be optimized **intrinsically (from the beginning)**. That is, the direct path should be used between them at the time of beginning of the communication.

2.3.9 SEPARATION OF ACCESS NETWORK AND BACKBONE NETWORK PROTOCOLS

In Future Internet, the access network and the backbone network may have quire different characteristics. In particular, an access network might consist of the wireless links with low bandwidth and unreliable transmissions. On the other hand, the backbone network will be of high bandwidth to support reliable transmissions. Accordingly, the requirements and operations for the respective protocols may be quite different.

In MOFI, Access Network Protocol (ANP) will be designed to consider the wireless network environment, whereas Backbone Network Protocol (BNP) is designed to be as simple as possible. Most of the control functionalities for mobility will be performed by the edge routers (i.e., the first or last access routers to the users) between the access and backbone networks. In particular, we argue that the current IPv4/v6 protocols can be used in the Backbone Network, as an incremental approach (tentative solution) for deployment of Future Internet. This will be helpful for migration from the current Internet to the clean-slate Future Internet.

2.3.10 CROSS-LAYER OPTIMIZATION USING LOWER LAYER INFORMATION

MOFI will be designed based on the cross-layer optimization using the underlying link-layer information, which is useful to improve the mobility performance, especially handover performance, for real-time services.

2.3.11 SUPPORT OF MULTI-HOMING HOSTS WITH MULTIPLE NETWORK INTERFACES

In Future Internet, it is envisioned that a mobile host can access to the network with multiple network interfaces using different wireless access technologies. MOFI will be designed to support such multi-homing hosts (e.g., in the operations of network selection and vertical handover).

2.3.12 SUPPORT OF UNRELIABLE WIRELESS LINKS

In Future Internet, some of the wireless access links may be not reliable, as seen in the example of the ad-hoc or sensor networks. MOFI needs to be designed to guarantee the service availability even in such an unreliable network environment.

2.3.13 SUPPORT OF IDLE MODE HOSTS

In Future Internet, the idle mode host for saving the electrical power will be a substantial feature in the wireless/mobile communications. MOFI needs to support the idle mode hosts effectively.

2.4 RELATIONSHIP BETWEEN VISION AND DESIGN GOALS

The relationship between ESC vision and MOFI design goals is given in the table below.

Table 1 – Design principles and ESC visions in MOFI

No.	Design Principle	Easy	Safe	Cheap
1	Mobile-optimized and Static-allowed	O		O
2	ID-based Communication	O	O	O
3	Separation of Identifier and Locator	O	O	O
4	Address-free User Hosts	O	O	O
5	Location Privacy		O	
6	Separation of Mobility Control and Data Transport		O	O
7	Network-based Mobility Control	O	O	O
8	Intrinsic Route Optimization			O
9	Separation of Access and Backbone Network Protocols	O		O
10	Cross-layer Optimization	O		O
11	Support of Multi-homing Hosts	O		O
12	Support of Unreliable Wireless Links	O		O
13	Idle Mode Support			O

3. ARCHITECTURE

Mobile-Optimized Future Internet (MOFI) is the architecture of Future Internet for mobility optimization. MOFI may be considered as a component building block in the overall Future Internet architecture. In this section, we describe the architecture of MOFI based on the design considerations discussed in the previous section.

3.1 BASIC APPROACHES

The architecture of MOFI is mainly designed under the following approaches.

- Cellular-like mobility management

  MOFI is based on the mobility management concepts used in the current cellular networks such as GSM-MAP and IS-41. The rationale behind this is that the mobility management schemes of the cellular networks have been regarded as quite successful examples in the communication areas. In addition, the cellular networks provide very useful functionalities, such as intelligent network capability, separated planes (control and data), and so on.

- Intelligent edge (or access) router in Future Internet

  Intelligent edge router is essentially required to provide easy access and communication for users in Future Internet. Each access router will perform all the control functions required for mobility optimization, on behalf of the users that are attached to the access router. MOFI is designed on top of these intelligent edge routers.

3.2 IDENTIFIER AND LOCATOR

3.2.1 USER IDENTIFIER (UID)

UID represents "**who are you?**" which is used to **uniquely identify** a user in the network. For communication, UID of a user should be already informed to the corresponding user. UID is referred to as 'Node ID' in the "Patterns in Network Architecture (PNA)" [10]. As a node ID, a UID may refer to a user (human) or a user's equipment (host). In fact, there are many possible mappings between user and host: one-to-many or many-to-one. In this memo, for now, we assume that one user has one host, and we will focus on the UID of a human user.

Under the framework of identifier/locator separation, the following types of UID are being considered in the existing studies:

- Host Identifier (HID) with a public key is used as UID in the Host Identity Protocol (HIP) [11];
- IP address is used as Endpoint Identifier (EID) in the Locator Identifier Separation Protocol (LISP) [12];

In MOFI, a **name** or a **number** can be used as a UID. The specific format of UID would depend on services and applications deployed in Future Internet. So far, some promising formats of UID

include Network Access Identifier (NAI) such as **user@realm** and telephone number such as **12-345-5679.** Some more UID formats may be defined additionally in the future. In the subsequent description of MOFI, we will focus on a NAI format as UID.

3.2.2 LOCATOR (LOC)

Locator (LOC) represents "**where are you?**" which is used to represent the location of a user in the network. An LOC may contain the information on topological or geographical location of the user in the network. LOC is also used for delivery of data packets between users in the network.

Under the framework of identifier/locator separation, IP address is usually used as an LOC. In HIP, an IP address of a host is used as LOC. In LISP, an IP address of the border router of a site (called Ingress/Egress Tunnel Router) is used as an LOC.

In MOFI, we will consider an **IP address of the access router** that a user is attached to, not an IP address of the host, as an LOC. Accordingly, a user host does not need to configure an IP address in the network. This LOC is also a routable IP address for delivery of data packets in the network. Other additional LOC formats may be defined in the future.

3.2.3 SERVICE ID (SID)

SID is used to uniquely identify an upper-layer application or service that is running on the host. In the current Internet, a specific application can be identified by a **socket** address, which is composed of an IP address and a TCP/UDP **port number**.

In Future Internet, there may be many different ways to identify and/or to represent the services and applications, by which the SID format will be determined. For example, a port number may be used as an SID in the similar way with the current Internet, in which an application or service may be uniquely identified with a pair of UID and SID in the network. Alternatively, a distinct service/application name, irrespective of UID, may be used as a SID in Future Internet. For example, Uniform Resource Identifier (URI) may be used as an SID. In this case, the functionality such as 'directory' may be required for mapping between SID and UID [10].

More specific definition and format of SID depend on the service and application architecture of Future Internet, which is still **for further study.**

3.2.4 INTERFACE ID (IID)

IID is used **to identify a host (specifically, its network interface) within a local subnet** of a router. IID is needed for data communications between access router and the host. An example of IID is the IEEE 802 MAC address (or any other link-layer physical addresses of hosts for wired/wireless network interfaces). The specific format of IID depends on the associated link-layer access technology.

More detailed definition and format of IID will depend on the specific access technology, which is outside the scope of MOFI.

3.2.5 SUMMARY AND DISCUSSION

In MOFI, a user (host) has the three levels of identifiers: SID, UID, and IID, which are summarized in the table below.

Table 2 – MOFI identifiers

Identifiers	Examples	Features
Service ID (SID)	port number, URI, or newly defined name formats, etc	Uniquely identify the services or applications running over a host
User ID (UID)	NAI (user@realm), or telephone number, IMSI, etc	Uniquely and globally identify a user in the network
Interface ID (IID)	MAC address, etc	Physical address of network interface of a host; unique in the local subnet

These identifiers can be mapped to the terms defined in the Saltzer's model [13], even though the specific mappings are still for the discussion, as follows:

- Service ID (MOFI) ⇔ Application Name (Saltzer's model)
- User ID (MOFI) ⇔ Node Address (Saltzer's model)
- Interface ID (MOFI) ⇔ Point of Attachment Address (Saltzer's model)

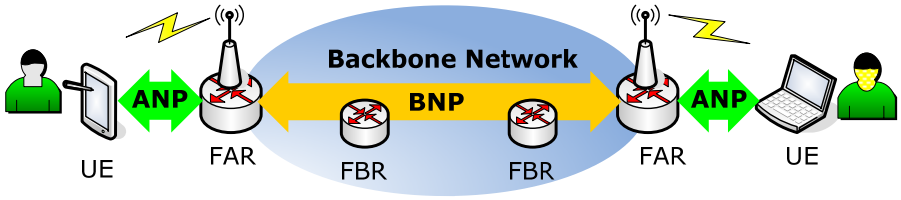
An SID can be mapped to one or more UIDs; that is, an identical service or application may be used by using a different UID. In addition, a UID can be mapped to one or more IIDs; that is, one user terminal may have two or more network interfaces (e.g., in the multi-homing environment). The separation of UID and IID is essential for support of the multi-homing hosts which use multiple IIDs for a single UID.

In MOFI, LOC (locator) is an IP address of the access router, which may contain information on topological or geographical location of the user in the network. LOC will be referred to only by the network (not by user). The separation of UID and LOC is the essential requirement for mobility support, since by user's movement an LOC may change, but UID will not change.

In MOFI, a host does not use any IP address as either UID or LOC; that is, no IP address is configured during handover, which will facilitate the support of seamless handover by omitting the IP address configuration delay.

3.3 NETWORK MODEL

Now, we consider an overall network model for design of MOFI, which consists of a backbone network and a wide variety of wireless access networks, as shown in Figure 4. This figure is based on the communication sphere concept in Figure 2



UE: User Equipment
FAR: FI Access Router
FBR: FI Backbone Router
ANP: Access Network Protocol
BNP: Backbone Network Protocol

Figure 4 – Network model in MOFI

3.3.1 USER EQUIPMENT (UE)

In MOFI, it is assumed that a user has its user equipment (UE) and its own UID that can uniquely identify the user. The UE has one or more Interface Identifiers (IIDs), depending on whether the UE has a single or multiple network interfaces.

UE communicates with the Future Internet Access Router (FAR) that it is attached in the network. In MOFI, data communications between UE and FAR are governed by '**Access Network Protocol (ANP)**', which will be described later.

3.3.2 FUTURE INTERNET BACKBONE ROUTER (FBR)

The backbone network will include a lot of Future Internet Backbone Routers (FBRs) used for delivery of packets between access routers. The relevant data **routing and forwarding will follow the Backbone Network Protocol (BNP),** which may use the current IPv4/IPv6 protocols or the newly defined Future Internet Protocols. **In MOFI, we assume that BNP uses the current IPv4/IPv6 protocol stack**.

3.3.3 FUTURE INTERNET ACCESS ROUTER (FAR)

We consider a variety of wired or wireless access networks between router and UEs. FAR is the first-hop router to the user with wireless network interfaces that users are attached to. UE communicates with its attached FAR by using the ANP for data packet delivery in the network.

The FAR receives the data packets from its local user and forwards them to the correspondent user in the network via BNP.

In deployment of an access network, an FAR may be located with the underlying Point of Attachment (PoA). Alternatively, two or more PoAs may be connected to the FAR, as shown in the figure below.

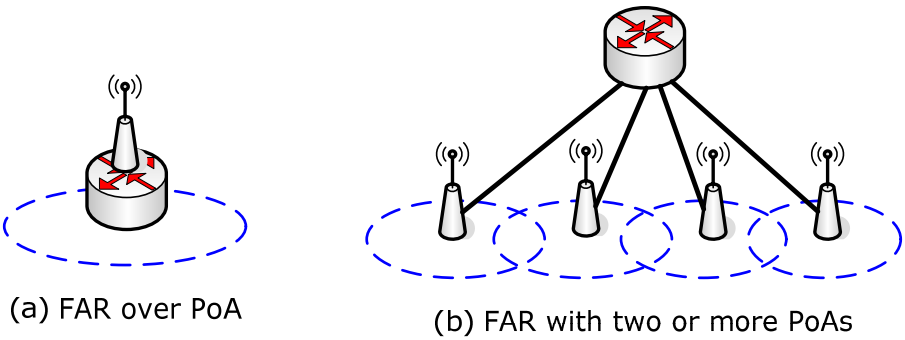


Figure 5 – Deployment of FAR and PoA

In case (a), UE has a direct interface with FAR in the link layer. In case (b), UE communicates with FAR via an associated PoA, in which the movement of UE between two neighbouring PoAs will be managed by the corresponding link-layer mobility management scheme that is outside the scope of this memo.

3.4 DATA TRANSPORT PLANE

3.4.1 PROTOCOL MODEL

It is noted that the design of the protocol and its layering architecture of Future Internet includes a lot of issues to be considered, which still needs significant challenges with further researches and experimentations. At present, we will propose a simplified protocol model as a basis to design the MOFI in the viewpoint of mobility optimization in the network layer, which could possibly be considered as a building block component in the overall design of Future Internet.

In MOFI, we will consider a protocol stack with the three layers (the corresponding identifiers are also shown for each layer), as shown in the figure below.

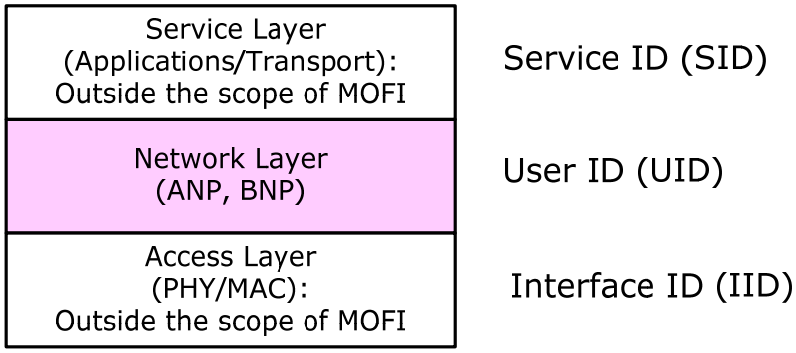


Figure 6 – Protocol stack and MOFI identifiers

- Services Layer

  This layer is responsible for providing services and application for users. The application-layer (HTTP, etc) and transport-layer protocols (TCP, UDP, etc) in the current TCP/IP can be classified as Services layer, which is still a controversial issue that requires further considerations in the engineering perspective. For now, **this layer is outside the scope of MOFI.**

- Network Layer

  This layer is responsible for the user data delivery between two end hosts. The network layer protocol is divided into Access Network Protocol (ANP) and Backbone Network Protocol (BNP). **The ANP is newly defined in MOFI, whereas the current IPv4/IPv6 protocol is tentatively as BNP** (until a better alternative protocol is identified).

- Access Layer

  This includes the MAC/PHY layer, which depends on the underlying wireless link layer. **This layer is outside the scope of MOFI.**

Figure 7 roughly compares the MOFI protocol stack and the current TCP/IP protocol stack.

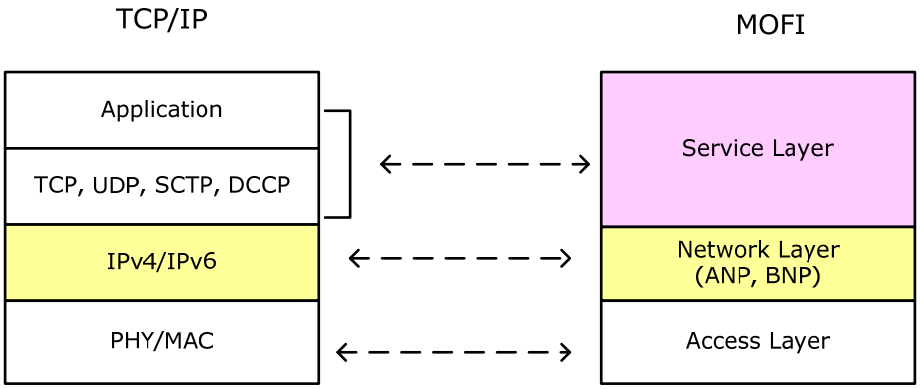


Figure 7 – Comparison of protocol stacks for TCP/IP and MOFI

The network layer protocols are responsible for data transport in the network, as shown in Figure 8. ANP is responsible for data delivery between UE and FAR, and BNP is used to deliver data packets between FARs over backbone network, which will use the current IP protocol in MOFI.

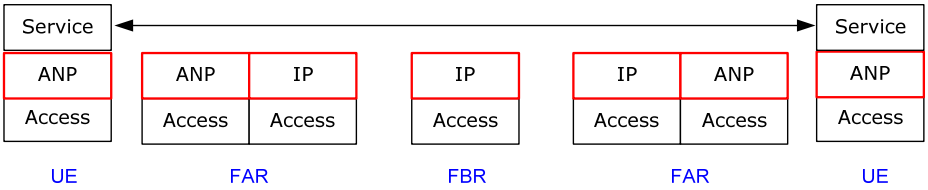


Figure 8 – ANP and BNP (IP) in the data transport plane

3.4.2 DATA TRANSPORT MODEL

In MOFI, the data communications will be done by using UIDs and LOC (IP address of FAR). For discussion, we classify users into Corresponding User (CU) and MU (Mobile User). CU will initiate data communication with MU, as shown in Figure 9.

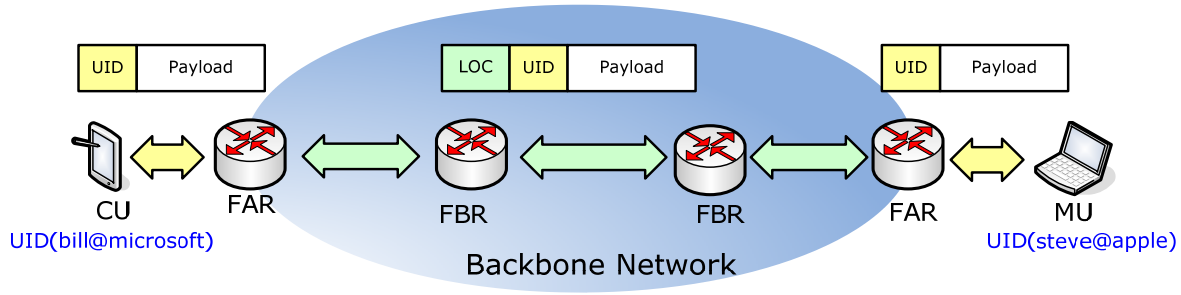


Figure 9 – User data transport in MOFI

Then, the data packet transport operations are summarized as follows:

(1) Data transmission (CU ⇔ FAR)

CU sends the data packets to FAR by using UID of MU. It is noted that CU does not need to know the LOC of MU (IP address of FAR that is attached to MU).

(2) Encapsulation (FAR of CU)

On reception of data packets from CU, FAR of CU first need to identify the LOC of MU. For this purpose, we need to define a mobility control protocol (MCP), which will be described later. FAR of CU will then encapsulate the data packets by adding the LOC of MU (IP address of FAR of MU) into the packet header.

(3) Packet delivery in the backbone network

The encapsulated data packets will be delivered to the FAR of MU by using BNP (the current IP routing/forwarding schemes), possibly via a set of FBRs in the network.

(4) Decapsulation (FAR of MU)

On reception of the encapsulated data packets from FAR of CU, the FAR of MU will get the original data packets by decapsulation, and then forward them to MU.

(5) Data reception (FAR ⇔ MU)

Finally, the MU can receive the user data packets of CU.

3.5 MOBILITY CONTROL PLANE

For mobility control, MOFI uses the Mobility Control Protocol (MCP).

3.5.1 MOBILITY CONTROL MODEL

The following figure shows the functional entities used for mobility control in MOFI, in which the data transport operations are separated from the mobility control operations in the MOFI.

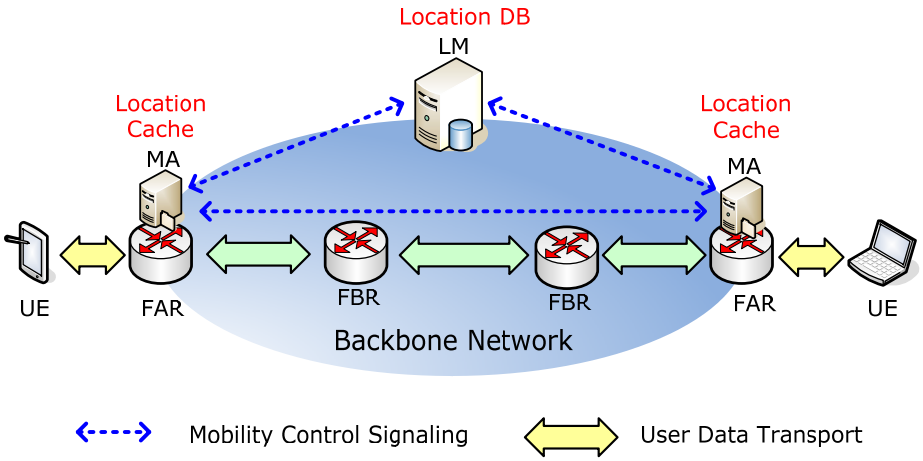


Figure 10 – Mobility Control Model

For data communication, UE has only to know the UID of the corresponding user, without knowing the corresponding LOC. When UE binds to the network, the associated UID and IID are registered with FAR via the **UID Resolution Protocol (URP),** which will be described later.

The mobility control function will be performed by **Mobility Agent (MA)**, which is co-located at FAR, and **Location Manager (LM)**, which is a server in the backbone network. UE is not involved with the mobility control operations. We consider the network-based mobility control in MOFI.

3.5.2 MOBILITY CONTROL OPERATIONS

The MCP is a control protocol used for mobility control in the MOFI architecture. The following figure shows the relationship between the functional entities for mobility control.

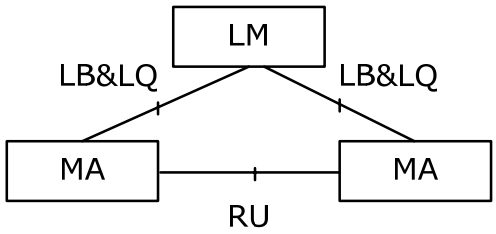


Figure 11 – Mobility Control Operations

Location Binding (LB) is performed between MA and LM. For user data transport, MA will perform Location Query (LQ) with LM so as to identify the locator of MU that CU wants to communicate with. For handover control, the Routing Update (RU) operation between MA of CU and MA of MU is performed for adjustment (optimization) of data delivery path. To support fast and seamless handover, a handover tunnel may be established between the concerned two FARs, which is for further study.

3.5.3 ENCAPSULATION OF MCP PACKETS

The MCP packets will be exchanged between MA and LM or between MAs in the backbone networks. In MOFI, it is assumed that the current IP protocol is used as BNP. Accordingly, the MCP packets will be encapsulated by using TCP, UDP, or SCTP.

It is noted that the SCTP is suitable for mission-critical applications such as signaling (e.g., signaling between SIP servers, or signaling between AAA servers). Therefore, it is recommended that the MCP packets are delivered by using SCTP/IP.

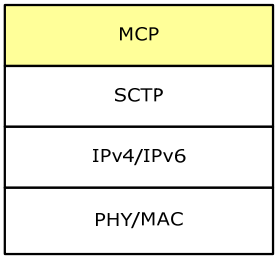


Figure 12 – MCP Protocol Stack

3.5.4 SEPARATION OF MOBILITY CONTROL PLANE AND DATA TRANSPORT PLANE

In MOFI, the mobility control plane is separated from the data transport plane. MA and FAR may be co-located and communicate via a local interface each other.

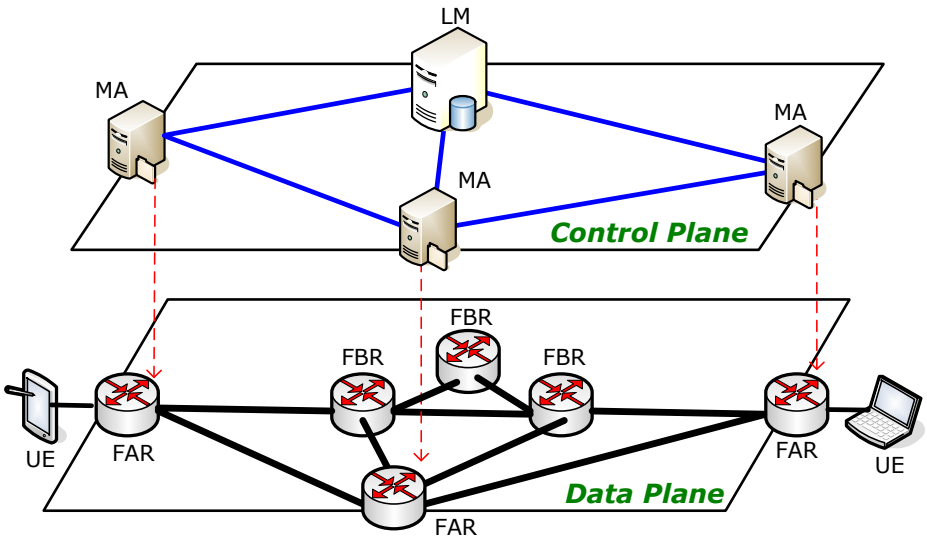


Figure 13 – Separation of mobility control plane and data transport plane

4. PROTOCOLS FOR DATA TRANSPORT

4.1 ANP AND BNP

Both ANP and BNP protocols are used for delivery of data packets in the network.

4.1.1 PROTOCOL MODEL

ANP is the protocol used for data transport between UE and FAR, and BNP defines the protocol for data transport between FAR and other FAR possibly via FBRs in the network. In MOFI, ANP is newly defined, whereas **the current IP (IPv4/IPv6) will be used as the BNP.**

The protocol stacks associated with data transport are shown in the figure below.

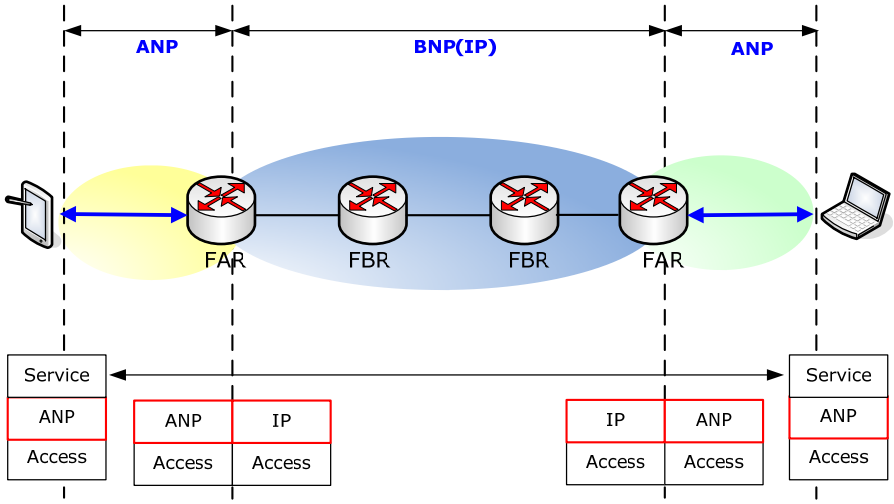


Figure 14 – ANP and BNP for User Data Transport

4.1.2 PACKET STRUCTURE

In MOFI, the two types of user data packets are defined: ANP packet between UE and FAR, and BNP (IP) packet between FARs, as follows:

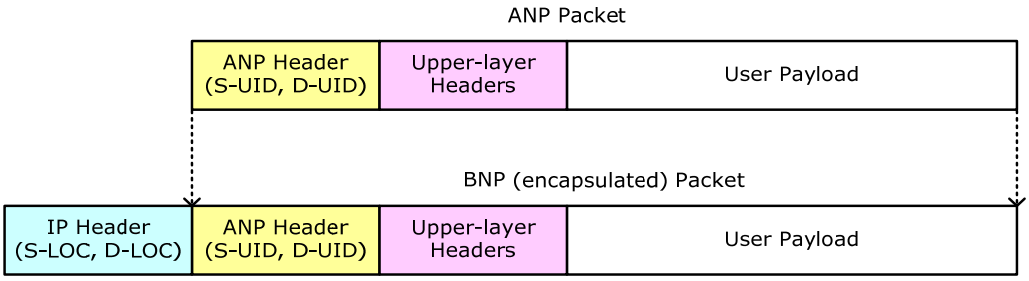


Figure 15 – Structure of Data Packets

In the packet format, the upper-layer header(s) may be defined in the overall architecture of Future Internet, which include the SID and other application/session-specific information. This is outside the scope of MOFI for now.

We refer to the current IPv6 header format for design of the ANP header, which has the following abstract packet format:

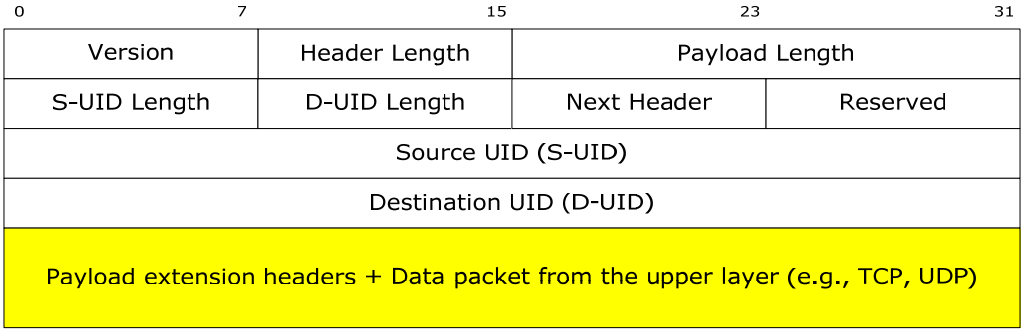


Figure 16 – Abstract Format of ANP Header

Packet Field Description:

- Version (8 bits): indicates this version of ANP. It starts with the version 1;
- Header Length (8 bits): the length of this ANP header in byte;
- Payload Length (16 bits): the length of user payload (in byte) following this ANP header;
- S-UID Length (8 bits): the length of Source UID (in bit);
- D-UID Length (8 bits): the length of Destination UID (in bit);
- Next Header (8 bits): this is the same with the Protocol of IPv4 header and the Next Header of IPv6 header.
- Reserved (8 bits): reserved for future use;
- S-UID (variable): Source UID with the length of S-UID Length
- D-UID (variable): Destination UID with the length of D-UID Length

Note that this ANP header may be followed by some extension headers and/or the user data payload from the upper-layer protocols (e.g., TCP/UDP), which depends on the overall architecture of Future Internet.

ANP may provide the reliable data transmissions between UE and FAR, which is useful in the wireless (intermittent) networks with unreliable links. In this case, the ANP protocol may need to be extended (e.g. by defining another reliable transmission protocol such as TCP in the field of 'Next Header), which is for further study.

As per the assumption of MOFI, the BNP header will be the IP (IPv4/IPv6) header. The BNP (IP) header includes the source and destination IP addresses of the concerned FARs as locators.

4.2 UID Resolution Protocol (URP) with Network Attachment

4.2.1 URP Operations

When a user enters the network, it will establish the network connection with the concerned Point of Attachment (PoA) via an appropriate link-layer connection establishment process (e.g., PPP connection between mobile device and 3G network equipment, or WLAN link connection between mobile device and AP). In this network attachment process, a certain authentication and/or authorization may be performed between a user and service provider, which is specific to the service deployment and outside the scope of the MOFI.

With this network attachment, UE is informed about the physical address (i.e., IID) of FAR for the subsequent UID Resolution Protocol (URP) operations. In MOFI, the URP is newly defined between UE and FAR in the link (access) layer. The main purpose of MOFI-URP is for FAR to obtain information of mapping between UID and IID associated with the UE, which is similar to the IPv4 ARP (Address Resolution Protocol) and IPv6 NDP (Neighbour Discovery Protocol).

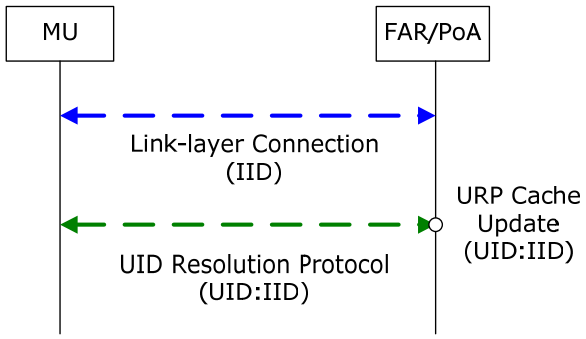


Figure 17 – UID Resolution between UE and FAR/PoA

When a UE enters a new network (FAR), it registers its UID and IID with the attached FAR by exchanging **UID Binding Request (UBR)** and **UID Binding ACK (UBA)** messages. This binding information will be referred to by FAR for forwarding of data packets destined to the concerned UE. In a certain case, FAR may have data packets to transmit to a certain UID, but it does not know the associated IID. In this case, FAR will identify the IID (or UE) in the local subnet by sending a **UID Query Request (UQR)** message (by broadcast) and receiving the responding a **UID Query ACK (UQA)** message from the UE (by unicast).

The differences between TCP/IP-ARP and MOFI-URP are described in the table below.

Table 3 – Comparison between TCP/IP-ARP and MOFI-URP

	TCP/IP (Current Internet)	FI (Future Internet)
UID (logical)	IP address	(e.g.) bill@microsoft
IID (physical)	(e.g.) MAC address	(e.g.,) MAC address, USIM, etc
Protocol	ARP (IPv4), NDP (IPv6)	URP

4.2.2 URP PACKETS

URP packets are encapsulated into the underlying access-layer (link-layer) frame. The URP packet format is shown in the figure below.

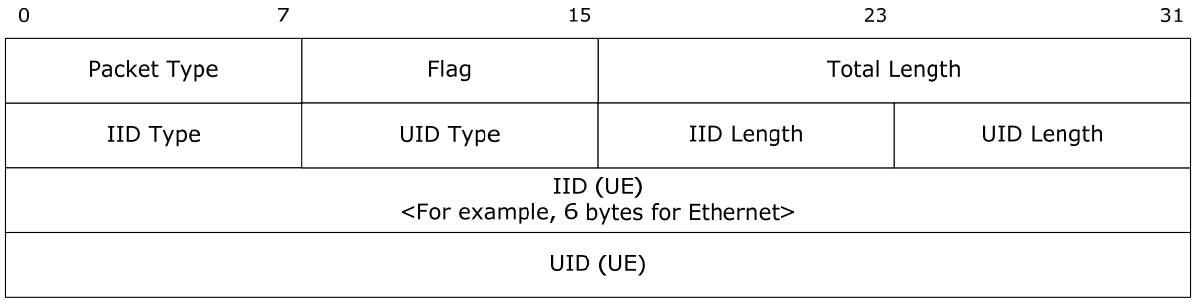


Figure 18 – URP Packet Format

Packet Field Description:

- Packet Type (8 bits): indicates the type of URP packet, which will be described later;
- Flag (8 bits): flag bits to be used for additional information, which is reserved for future use;
- Total Length (16 bits): the length of this packet in byte;
- IID Type (8 bits): the type of Interface Identifier of UE (e.g., IEEE 802 MAC address, 3GPP-specific address, etc), the detailed type code is for further study;
- UID Type (8 bits): the type of UID (e.g., NAI, telephone number, etc), the detailed type code is for further study;
- IID Length (8 bits): the length of IID of UE in byte (e.g., 6 bytes for Ethernet);
- UID Length (8 bits): the length of UID of UE in byte;
- IID (variable): IID of UE (e.g., Ethernet MAC address);
- UID (variable): UID of UE (e.g., NAI, telephone number, etc).

The UID Binding Request (UBR) packet is initiated by UE toward FAR, when UE is attached to the network. FAR shall respond with UID Binding ACK (UBA) packet to UE. The UID Query Request (UQR) packet is initiated by FAR, when FAR has data packets to a certain UE in its subnet. UE shall respond with UID Query ACK (UQA) packet.

At present, the following four types of URP packets are defined:

Table 4 – URP Packets

Packet Type	Encoding value	Description
UID Binding Request (UBR)	1	From UE to FAR (unicast)
UID Binding ACK (UBA)	2	From FAR to UE (unicast)
UID Query Request (UQR)	3	From FAR to UE (broadcast)
UID Query ACK (UQA)	4	From UE to FAR (unicast)

The encoding values of 0 and 5 ~ 255 are for future use.

4.2.3 URP CACHE

In the MOFI-URP operation, FAR maintains and updates its own URP Cache by recording the UIDs and IIDs associated with UEs in the local subnet. The abstract format of the FAR-URP cache table is shown below.

Table 5 – FAR-URP Cache (example)

No.	UID	IID	Status	User Type
1	UID1	IID1	Idle	Static
2	UID2	IID2	Active	Static
3	UID3	IID3	Idle	Mobile
4	UID4	IID4	Active	Mobile
5	…	…	…	…

As shown in the table, the FAR-URP cache maintains UID and IID for each user that is attached to the FAR. This information will be referred to in the packet delivery of the data packets that are destined to the users in the local subnet. In the table, the status field represents whether or not the user is in the active data communication with a certain other corresponding user. That is, 'active' means the UID (user) is bound to the network and also in communication with the other user(s), while 'idle' implies that the user is bound but not in communication. In addition, the FAR-URP cache may have information on the type of UE, static or mobile, which is for further study.

For the perspective of protocol design, some appropriate timers may be used for MOFI-URP operations, which is for further study.

5. MOBILITY CONTROL PROTOCOL (MCP)

5.1 FUNCTIONAL ENTITIES

For mobility control, Location Manager (LM) and Mobility Agent (MA) are newly defined in MOFI.

5.1.1 LOCATION MANAGER (LM) WITH LOCATION DATABASE (DB)

LM manages the location information of all of the users in the network. For this purpose, LM maintains the global location database, which maps between UIDs and LOCs for all of the users.

When a UE moves into FAR, its MA will perform the URP operations and then the Location Binding operation with Location Manager (LM). From this Location Bindings, UID and LOC of UE (IP address of FAR) will be registered with LM. Accordingly, LM will maintain the following Location DB, as shown in the table below.

Table 6 – LM Location Database

No.	UID	LOC	User Type
1	UID1	LOC1	mobile
2	UID2	LOC2	static
3	…	…	…

5.1.2 MOBILITY AGENT (MA) WITH LOCATION CACHE (LC)

It is expected that MA is co-located with FAR, possibly via a local (internal) interface. The MA performs the mobility control with the Location Manager (LM) and the other MAs. For mobility control, each MA performs the location binding and location query operations with LM.

When a UE wants to communicate with another UE, the associated MA/FAR will perform the **Location Query** operation with LM so as to get the locator (LOC) of the corresponding UE. From this Location Query operation, each MA maintains **the Location Cache** (LC) for each of the corresponding (remote) UEs, as shown in the figure below.

Table 7 – MA Location Cache

No.	Remote UID	Remote LOC
1	UID1	LOC1
2	UID2	LOC2
3	…	…

5.2 PROCEDURES

5.2.1 LOCATION BINDING

When an FAR detects a new UE in its network region, its associated MA shall perform the Location Binding (LB) operation by sending a LB Request (LBR) message to the Location Manager (LM). LM responds with the corresponding LB ACK (LBA) message to the LM. This LB operation will be performed each time MU moves into a new FAR area, as shown in the figure below.

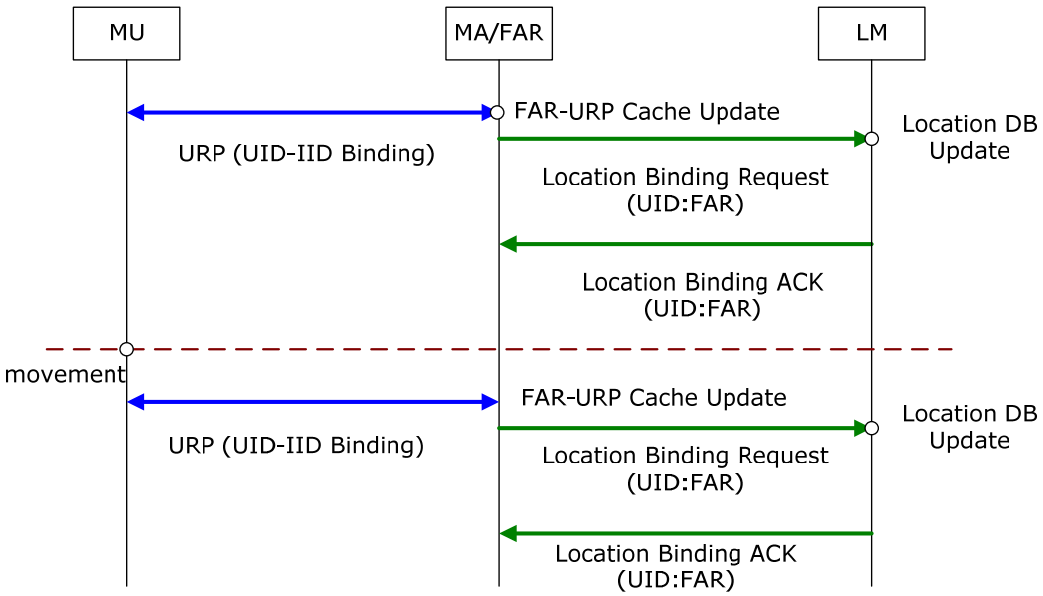


Figure 19 – Location Binding

Based on the LBR message, LM updates its location database (DB) by creating or updating the entry associated with the MU. When MU moves into a new FAR area in the network, it will update the new LOC by contacting with LM.

5.2.2 LOCATION QUERY FOR USER DATA TRANSPORT

We assume that an MU completes its Location Binding operation. Let us consider a CU (UID1) that sends data packets to the MU (UID2). In this phase, the FAR of CU needs to perform the Location Query (LQ) operation with LM. An example of data transport scenario from UID1 (bill@microsoft) to UID2 (steve@google) is illustrated in the figure below.

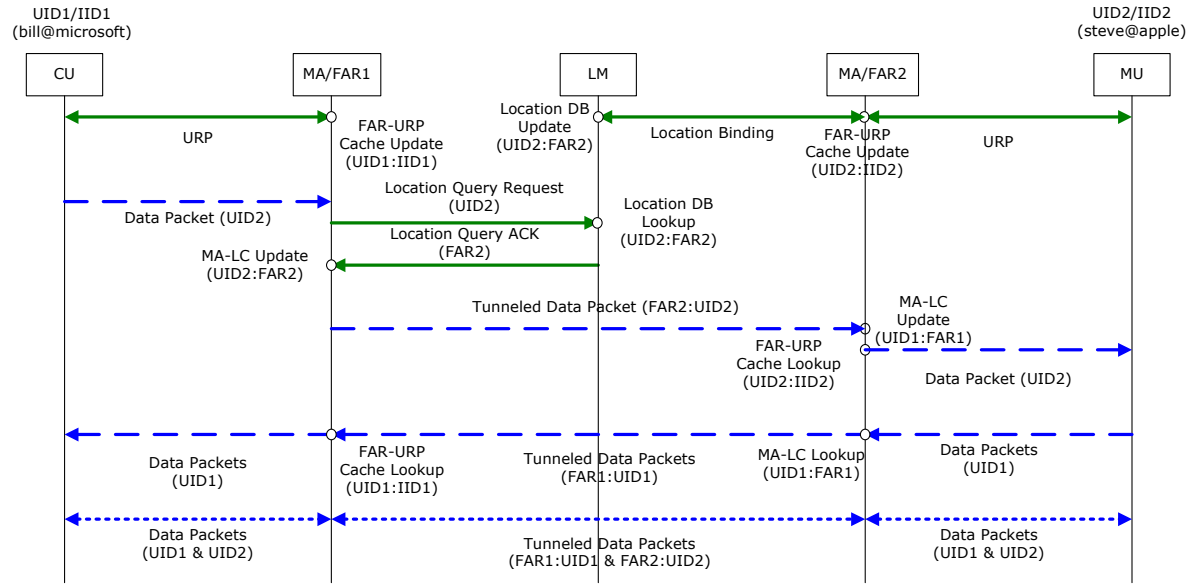


Figure 20 – Data Transport with Location Query

Then the data transport procedures could be done as follows:

1) Initially, CU (UID1) and MU (UID2) are bound to FAR1 and FAR2 via URP operations, in which the associated FAR-URP caches are updated with UID1:IID1 and UID2:IID2.
2) CU sends an initial data packet to MU via its attached FAR1;
3) MA/FAR1 will first look up its Location Cache (LC) table to find the locator of UID2; if yes, FAR1 can deliver the data packet to the identified FAR2 (LOC2), which is not shown in the figure.
4) If MA1 cannot find the locator of UID2 in the LC table, it shall perform the Location Query operation by sending an LQR message to LM. In response to the LQR message, the LM will lookup its Location DB to identify the locator of UID2, and then it sends the LQA message to the MA1. Based on the received LQA message, MA1 will update its LC table by creating the entry for UID2 and FAR2 (LOC2);
5) FAR1 will send the tunnelled data packet to the FAR2 (LOC2);
6) On reception of the tunnelled data packet from FAR1, the FAR2 extracts the original user data packet from the tunnelled packet. In this process, MA2 will update its LC table by creating a new entry for UID1 and FAR1 (LOC1). This is done for FAR2 to deliver the data packets from MU to CU.
7) Then, FAR2 forwards the data packets to the MU (UID2). To do this, MA2 will lookup its FAR-URP cache to identify the IID associated with the UID2.
8) Up to now, the MA1-LC and MA2-LC have been constructed. Based on this information, MU can also send data packets to CU. That is, MU (UID2) and CU (UID1) can now exchange data packets by referring to the established URP caches and Location Caches of MA/FAR1 and MA/FAR2.

The following figure shows the abstract information flows of Location Binding and Location Query for the previous example.

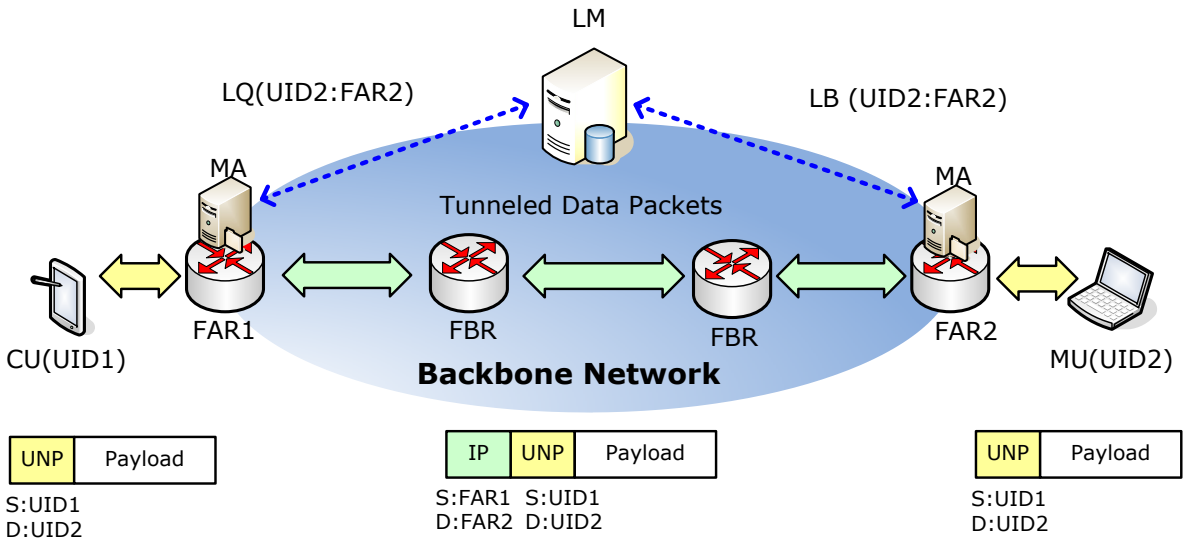


Figure 21 – Location Binding and Location Query

For data transport, the MA-LC maintains the list of the corresponding (remote) users that the local users are communicating with. On the other hand, FAR-URP Cache is used to forward the data packets to the attached local user.

For the initial data packet, if the LOC of MU is not in the MA-LC table, it may take some time to get the location information through the LQ operation. In this period, the data packet will be buffered by FAR, until the LQ operation is completed, which may give an impact on the data transmission performance and buffering overhead of FAR. To solve this issue, CU may first ask FAR to identify the LOC of UID, just before CU begins to transmit data packets to FAR. This requires an additional signalling operation between CU and FAR. The detailed operation for this is for further study.

5.2.3 ROUTING UPDATE FOR HANDOVER SUPPORT

Handover control is performed to provide service continuity for on-going sessions of mobile user. When a mobile user moves into a new FAR region while its session is still active, the movement will be detected with the help of the underlying link-layer triggers such as Link-Up (LU), Link-Down (LD), Link-Going-Down (LGD), and Link Coming-Up (LCU), etc. At present, we will focus on the LU trigger only. The other triggers can also be examined to provide seamless handover.

We consider the following handover scenario.

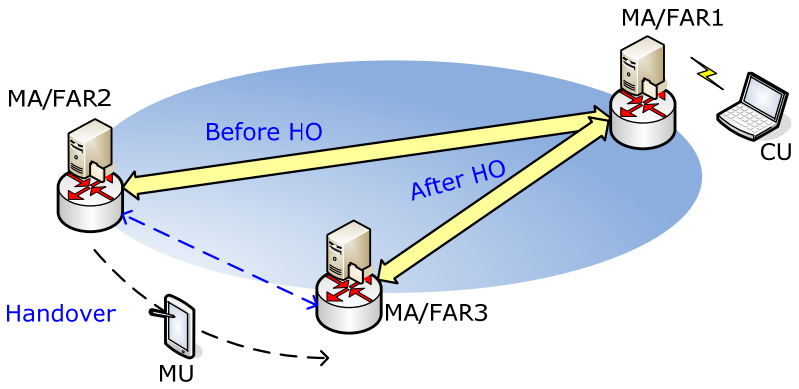


Figure 22 –Handover by movement

Based on the handover event, the handover control operations will be performed as follows.

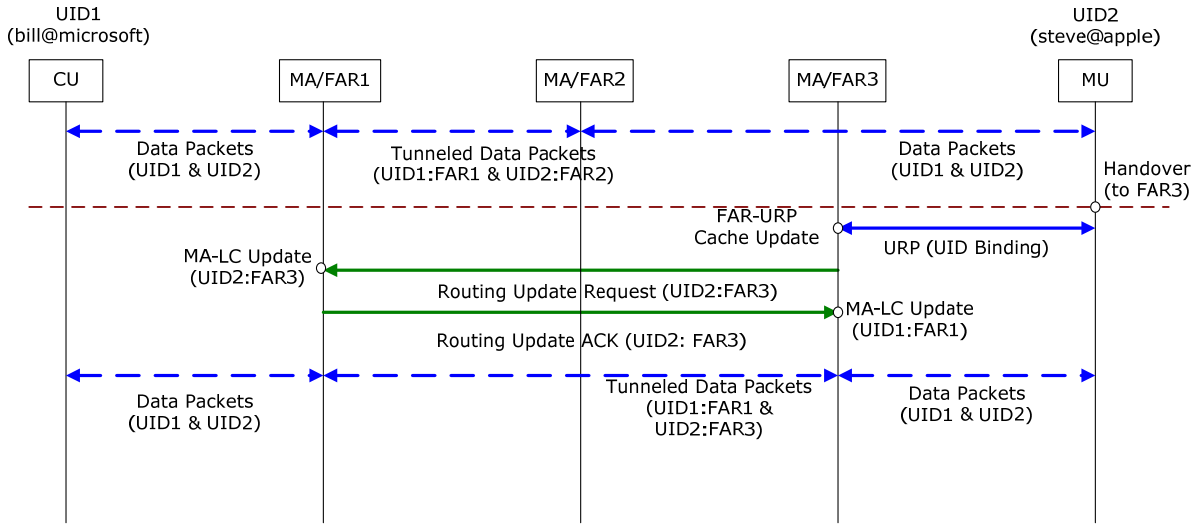


Figure 23 – Routing Update by Handover

1) We assume that CU and MU are communicating via FA1 and FAR2 before handover. The MU now gets the LU trigger from the network. On the LU trigger, MU performs the URP operation with its newly attached FAR.
2) The new FAR (FAR3) will update its URP cache table for UID2.
3) The FAR3 sends the Routing Update Request (RUR) message to the FAR of CU. On reception of the RUR message, FAR of CU will update its LC table with 'UID2:FAR3' to 'FAR3:UID2'.
4) In response to the RUR message, the FAR of CU will send the Routing Update ACK (RUA) message to the nFAR. On reception of the RUA message, the FAR3 update its Location Cache (LC) table by creating the UID1:FAR1 entry.
5) The data path between MU and CU is now changed to MU ⇔ FAR1 ⇔ FAR3 ⇔ CU.

In addition, the FAR will perform the Location Binding operation, which is not shown in the figures. This LB operation is for the newly incoming session to MU, which is performed independently of the handover control.

5.3 Further Optimization Issues

In addition to the basic mobility control operations described in the previous section, some more optimization needs to be taken.

5.3.1 Optimization of Location Query Operations

When a FAR receives a new ANP data packet from UE, it performs the Location Query operation with LM to get the correspondent LOC. The associated **Location Query Delay** may be much larger, as the number of users increases in the network, which may be a problem for some applications (e.g., for data-driven applications such as WWW).

To address this problem, the following considerations need to be taken:

- An additional signalling for location query (e.g., for call/session setup, as shown in the SIP-based multimedia communications) may be performed between UE and FAR, just before UE transmits the data packets to the network, which will be helpful to reduce the Location Query Delay.
- Location Query delay will depend on the time required for lookup of the location DB. The Location Query operations may also be concerned with the scalability issue at LM due to a large amount of control (signalling) traffic. For support of more efficient query operations, LM and location DBs may be hierarchically configured in the distributed manner, which is still for further study.

5.3.2 Optimization for Seamless Handover

To provide the seamless handover for mobile users, the following considerations need to be taken (which are still for further study):

- Proactive use of the other link-layer triggers such as LD, LGD, LCU, etc;
- Establishment of handover tunnel between old FAR and new FAR;
- Fast update of old LM-LC and old FAR-URP cache by handover, which may be done by using a timer or an explicit message.

5.3.3 Consideration of Heterogeneous Access Networks

It is expected that Future Internet consists of a variety of heterogeneous network environments. In this context, the following issues need to be considered:

- Multi-homing mobile devices need to be considered, together with the issue of vertical handover.
- Delay-Tolerant Networks (DTN) or unreliable wireless links needs to be considered in the mobility point of view.

5.4 PACKETS

5.4.1 PACKET FORMAT

The overall packet structure of MCP packet is shown below.

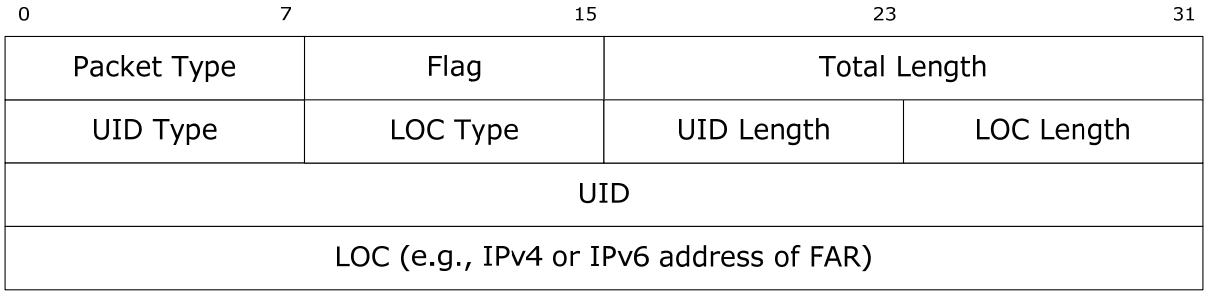


Figure 24 – MCP Packet Format

Packet Field Description:

- Packet Type (8 bits): indicates the type of MCP packet, which will be described later;
- Flag (8 bits): flag bits to be used for additional information, which is reserved for future use;
- Total Length (16 bits): the length of this packet in byte;
- UID Type (8 bits): the type of UID (e.g., NAI, telephone number, etc), the detailed type code is for further study;
- LOC Type (8 bits): at present, IPv4 address (type = 1) or IPv6 address (type = 2) will be used for a locator;
- UID Length (8 bits): the length of UID of UE in byte;
- LOC Length (variable): the length of LOC in byte (at present, 4 for IPv4, 16 for IPv6);
- UID (variable): UID of UE (e.g., NAI, telephone number, etc);
- LOC (variable): Locator of UE; IPv4 or IPv6 address of FAR.

5.4.2 PACKET TYPES

The following table shows the list of the packets used for MCP.

Table 8 – Types of MOFI/MCP Packets

Packet Type	Full Name	From	To
LBR	Location Binding Request (LBR)	MA	LM
LBA	Location Binding ACK (LBA)	LM	MA
LQR	Location Query Request (LQR)	MA	LM
LQA	Location Query ACK (LQA)	LM	MA
RUR	Routing Update Request (RUR)	MA	MA
RUA	Routing Update ACK (RUA)	MA	MA

Some more packets may be added, as the work is progressed.

6. COMPARISONS

The following table shows the comparison of the MOFI/MCP with the existing mobility protocols.

Table 9 – Comparison of characteristics among the mobility control protocols

Features	Mobile IP	Cellular MM (GSM-MAP)	MOFI/MCP
Relevant Area	Internet	Telecom (Cellular)	Future Internet (or Future network)
Related SDOs	IETF	3GPP	Project-based (e.g., FIND, FP7, etc)
Basic user/host type	Static	Mobile	Mobile
Control/data path	Combined	Separated	Separated
ID/LOC separation	Combined	Separated	Separated
ID (example)	IP address (HoA)	User (IMSI)	User (UID)
Locator (example)	IP address (CoA)	- Idle: Location Area ID - Active: Cell ID	IP address of FAR (LOC)
Locator type	Host	Network	Network
Who performs location update	Host	Network	Network
Necessary information for communication	Correspondent host's IP address (HoA)	Correspondent user's telephone number (MSISDN)	Correspondent user's UID
Separation of access/backbone	No	Yes	Yes (ANP, BNP)
Mobility control function implementation	Patch-on	Built-in	Built-in
Type of mobility control	Host-based (or network-based)	Network-based (also assisted by host)	Network-based
Location privacy	Need extensions	Guaranteed	Guaranteed
Route optimization	Need additional signalling	Intrinsic	Intrinsic
Idle mode support	No	Yes	Will be

As summarized in the table above, MOFI has a lot of distinctive features from the existing Internet. On the other hand, the cellular mobility management (MM) is very similar to MOFI. MOFI is designed for Future Internet. It is envisioned that the current boundary between Internet and telecom network will eventually be disappeared with the strong network convergence trend.

MOFI basically assumes a user host is mobile, and thus tries to be optimized to the mobile environment like the cellular network. Note that current Internet was originally designed for the fixed hosts.

In MOFI, the data and control messages are processed separately by using logically different paths. This plane separation will bring many beneficial features for Future Internet such as the provision of more reliable transmissions for control messages, and the easy deployment of the various data and control schemes. Note in Mobile IP that the mobility agents, such as Foreign Agent (FA) and Home Agent (HA), are the single common point of communication for both data and control.

The need of ID/LOC separation is generally accepted in the mobile environment. In MOFI, ID is allocated to a user, whereas LOC is used only in the backbone network including FARs. IP address will be used as a locator in the backbone network. This location information of a mobile user is required to be managed only in the backbone network, which ensures that a user does not need to know the corresponding user's location (i.e. ID-based communication).

Compared to the existing Internet, where a single protocol is used throughout the network in the end-to-end fashion, MOFI uses different protocols in the access and backbone networks. This is based on the observation that the network conditions are different for the access and backbone networks. In this context, we may design a more mobile-efficient ANP. MOFI may have an advantage for migration from the current Internet to the Future Internet, in that we use the existing IP protocols as the BNP protocol.

The mobility control functions of MOFI is built-in the basic architecture of Future Internet, rather than added-on the current Internet, which ensures that the mobility control operations can be designed more effectively. In addition, the mobility control operations will be processed only in the network side. This feature is useful for easy deployment of the mobility functionality in the network, as seen in the example of the Proxy Mobile IP.

The location privacy provisioning is a feature of MOFI, which comes from the design goals of the ID/LOC separation and the ID-based communication. The **intrinsic** route optimization can be regarded as another benefit of MOFI, as also shown in the cellular networks. Also the idle mode hosts will be supported, as done in the cellular MM, which is still for further study.

7. CONCLUSION

In this memo, we have described architecture of Future Internet for mobility optimization, MOFI, and presented a set of protocols to realize the MOFI architecture. The MOFI can be viewed as a clean-slate approach for Future Internet, in which Access Network Protocol (ANP) is newly designed for data transport. The MOFI can also be regarded as an incremental approach in that the Backbone Network Protocol (BNP) uses the current IP protocol.

The MOFI has been designed with an aim that it can be considered as a building block component for overall design of Future Internet in the perspective of mobility. It is noted that there are still a lot of works to do for more engineering the proposed architecture and protocols, including further optimization and experimental validations of the MCP protocol.

REFERENCES

[1] IETF RFC 3344, IP Mobility Support for IPv4, August 2002.

[2] IETF RFC 3775, Mobility Support in IPv6, June 2004.

[3] eMobility Project, http://www.emobility.eu.org/

[4] 4WARD Project, http://www.4ward-project.eu/

[5] Trilogy Project, http://www.trilogy-project.org/

[6] Global Environment for Network Innovations (GENI), http://www.geni.net/

[7] Future Internet Design (FIND), http://www.nets-find.net/

[8] Ericsson, "Why Test the Next Generation Wireless Network with Your Grandfathers Internet Protocols?" Cross Forum Meeting, 26 March 2008

[9] IETF RFC 5213, Proxy Mobile IPv6, August 2008.

[10] John Day, Patterns in Network Architecture, Prentice Hall, 2008

[11] IETF Host Identity Protocol (HIP) WG, http://www.ietf.org/html.charters/hip-charter.html

[12] IETF Locator/Identifier Separation Protocol WG, http://www.ietf.org/html.charters/lisp-charter.html

[13] IETF RFC 1498, On the Naming and Binding of Network Destinations, August 1993

ABBREVIATIONS

ANP	Access Network Protocol
AR	Access Router
ARP	Address Resolution Protocol
ACK	Acknowledgement
BNP	Backbone Network Protocol
CU	Corresponding User
ESC	Easiness, Safety, and Cheapness
FAR	Future Internet Access Router
FBR	Future Internet Backbone Router
FI	Future Internet
ID	Identifier
IID	Interface Identifier
IP	Internet Protocol
LB	Location Binding
LBR	Location Binding Request
LBA	Location Binding ACK
LC	Location Cache
LM	Location Manager
LOC	Locator
LQ	Location Query
LQA	Location Query ACK
LQR	Location Query Request
MCP	Mobility Control Protocol
MIP	Mobile IP
MOFI	Mobile Optimized Future Internet
MU	Mobile User
NDP	Neighbour Discovery Protocol
PoA	Point of Attachment
SID	Service ID
UE	User Equipment
UID	User Identifier
URP	UID Resolution Protocol
RU	Routing Update
RUR	Routing Update Request
RUA	Routing Update ACK