Mobile-Oriented Future Internet (MOFI): Architecture and Protocols

(Release 1.2)

July 2010

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 study is motivated from the observation that future Internet would be evolved toward 'mobile-oriented' network environment, but current Internet was historically designed for 'static' network environment and thus it is inevitably subject to some architectural limitations in the viewpoint of 'mobile-oriented' future network. This document presents the architecture of Mobile-Oriented Future Internet (MOFI) to support the future mobile-oriented networks. The MOFI architecture is featured by 'built-in' support of the seamless mobility, separation of Host Identifier (HID) and Network Locator (LOC), HID-based communications with LOC-based routing, functional separation of mobility control and data delivery, and protocol separation for data delivery in access and backbone networks. Based on the MOFI architecture, we will identify a set of relevant protocols: HID Communication Protocol (HCP) for end-to-end communication; Access Delivery Protocol (ADP) and Backbone Delivery Protocol (BDP) for data delivery; and HID Binding Protocol (HBP) and LOC Management Protocol (LMP) for mobility control. The MOFI is purposed to be used as a building block component for overall design of future Internet architecture.

Acknowledgement

Special thanks is given to the following colleagues for their valuable comments:

- Byung Cheol Kim (CNU: Chungnam National University)
- Jae Yong Lee (CNU: Chungnam National University)
- Youn Hee Han (KUT: Korea University of Technology and Education)
- Pyung Soo Kim (KPU: Korea Polytechnic University)
- Juyoung Park (ETRI: Electronics and Telecommunications Research Institute)
- Jung Im Kim (ETRI: Electronics and Telecommunications Research Institute)
- Dae Young Kim (CNU: Chungnam National University)
- Sung Heok Byun (ETRI: Electronics and Telecommunications Research Institute)

Change Log

The following changes have been made from the MOFI 1.1 to this MOFI 1.2:

1) Terms are revised for functional entities and protocols;
2) The document structure is slightly modified.

TABLE OF CONTENTS

1. INTRODUCTION

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 networks now become the key driver toward the future Internet. It was reported that there were 4 billion mobile users (from 2.7 billion in 2006), using 570 million Internet-enabled handheld devices. The number of people who surf the network on their phones has doubled since 2006. By 2012, there will likely be more mobile and wireless users than wired ones [1]. 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 the mobile network environment. This has enforced Internet to add a lot extensional features to satisfy the requirements for mobile networks, as shown in the example of Mobile IP (MIP) [2, 3]. However, this patch-on approach seems to be just a temporal heuristic to the problems in the mobile environment, rather than an optimization approach to substantially solve the mobile-related issues.

Based on these observations, some activities already started to design the future Internet for mobile environment rather than fixed environment. A typical example is eMobility [4] which is a project of EU FP7. eMobility says that the first generation Internet had been developed mainly for research purpose, however, 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.'

The 4WARD [5], another FP7 project for design of future Internet architecture, is also targeted to effectively support the mobile environment. In [6], the authors describe a key driving force for the design of future Internet architecture as follows:

> "Design from a mobile and wireless perspective. The Internet was invented for fixed network use. But now more users in the world gain access to the network via mobile networks than via fixed networks. This increases the pressure to go beyond the Internet's assumption of continuous connectivity and static attachment points, and to fully address and profit from the specifics of wireless transmissions."

We also note many FIND projects, which are very closely related with wireless/mobile environments [7]. Especially, we note that the "mobile first" project is recently proposed as a candidate approach for future Internet in the recent NSF future Internet summit, which is a part of FIND activity [8]. This proposal is with the recognition that Internet is changing very rapidly from fixed hosts to mobile devices, in which it is stated that a future Internet architecture should support mobile devices as 'first-class' users and also provide a variety of new applications efficiently, securely, and at a large scale.

GENI [9], a representative testbed project for future Internet, also agrees that wireless/mobile will be the major access means for future Internet. We note that some design documents of GENI already covers the issues including ad-hoc and sensor networks.

AKRAI [10] is a representative future Internet activity in Japan, which deals with the issues on ID/Locator split architecture and a managed mesh to support mobile environment. Especially, the

ID/Locator split architecture covers the primary issues in mobile environment such as mobility and multi-homing, etc.

In addition, 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 [11].

With these observations, we will try to design the architecture of Mobile-Oriented Future Internet (MOFI) to support the future Internet's mobile environment. Our primary goal is to develop the overall architecture of MOFI. However such architectural design works include a lot of technical issues such as mobility, QoS, security, network management, traffic engineering, AAA, etc. Accordingly, those issues could not be covered at one time. Therefore, from the mobility perspective, we will first discuss the following question, "how to effectively deliver data packets in the mobile-oriented future Internet environment."

2. PROBLEMS OF CURRENT INTERNET IN MOBILE ENVIRONMENTS

In the historical perspective, Internet was designed mainly for fixed environment, which results in some limitations. In this section, we discuss some problems of Internet from the viewpoint of mobile-oriented future Internet.

2.1 OVERLOADED SEMANTICS OF IP ADDRESS

First of all, an IP address has overloaded semantics as Identifier (ID) and Locator (LOC). In mobile environment, however, the location of mobile host is likely to continue to change by movement. This means that the static allocation of LOC (IP address) to a host may become problematic in mobile networks. In the meantime, the ID needs to be kept persistently (without change) to maintain an on-going sessions against movement of a host. Accordingly, ID and LOC should be separated to support the mobility in future Internet.

Another critical concern is that IP address, as an ID, is allocated to a network interface of a host, rather the host itself. Accordingly, if a host has multiple interfaces, multiple IP addresses must be allocated to a single host. This may give serious inefficiency to a multi-homing host, since the same host has to use different IDs for communication. Therefore, ID needs to be allocated to a host itself rather than its network interface.

As for the allocation of LOC or IP address, it does not make sense to allocate IP address to a mobile host, since it may continue to move on. Accordingly, in mobile environments, it is suggested that an address or LOC should be allocated to a certain fixed node in the network, rather than the host itself.

2.2 ASSUMPTIONS ON LINK AND HOST

In Internet, it is implicitly assumed that the existence of stable connection between host and network. However, in mobile environment, the connection is subject to dynamics of the network, in particular, due to high error rates and intermittent connections, depending on characteristics of wireless networks. Accordingly, special considerations should be taken for lossless and reliable communications in such network environments.

In addition, in mobile environment, we should be able to support idle mode hosts to save their electric power. Nonetheless, in Internet we assume that most of the hosts are always on active state. This naturally requires some advanced capability, such as paging.

2.3 HOST-BASED PROTOCOLS

In Internet, many TCP/IP protocols have been implemented within a host, based on the so-called ‘end-to-end’ principle. However, in mobile environment, most of hosts are relatively subject to hardware limitations in terms of computing power consumption and scarce wireless link resources. This is quite a different feature from the fixed host. Accordingly, each end host needs to be implemented as lightly as possible in the functionality and operation points of view. In this context, it is desired that some part of intelligence (or functionality) of end host should be moved to the network side.

In addition, we note that the network-based protocol is preferred to the host-based protocol in the perspective of deployment and performance, as seen in the comparison of Mobile IP [3] and Proxy Mobile IP [12]. This also implies that a portion of intelligence or functionality of communication needs to be implemented in the network side rather than in the host side.

2.4 User location privacy

In Internet, an IP packet header contains the current location of a user in the form of source IP address, which may be regarded as a 'private' information, in case that the sender does not want to reveal its location to the correspondent. To provide the location privacy of a user, ID and LOC need to be separated, and LOC shall be used only in network, not in end hosts.

2.5 Mobility control in the form of patch-on

In mobile environment, the mobility control is regarded as an essential requirement, not an additional feature. In the meantime, TCP/IP protocols have so far focused on fixed hosts, and thus the mobility control has been considered as just a special or additional functionality. This leads to development of some mobility protocols (e.g., Mobile IP) in the form of patch-on the TCP/IP protocols. This kind of mobility control tends to induce unexpected performance degradation such as triangle routing, overuse of proxy agent, etc. Accordingly, in the mobile-oriented future Internet, the mobility control should be provisioned in the form of 'built-in' (intrinsically) rather than 'patch-on' (subsidiary).

2.6 Integration of data and control functionality

In general, the control information for signalling is mission-critical and thus needs to be delivered more urgently and more reliably, compared to normal user data. In this context, it is desired that the control functionality should be separated from the data transport functionality, as seen in the 2G or 3G wireless mobile communication systems.

In Internet, it is noted that the data and control functionalities are integrated. For example, in Mobile IP, Home Agent (HA) exchanges both user data and mobility control information (e.g., binding update) with a mobile node over the same path (by using the same IP address), which may be subject to performance degradation. Accordingly, the separation of control and data functionality shall be considered in mobile-oriented future Internet.

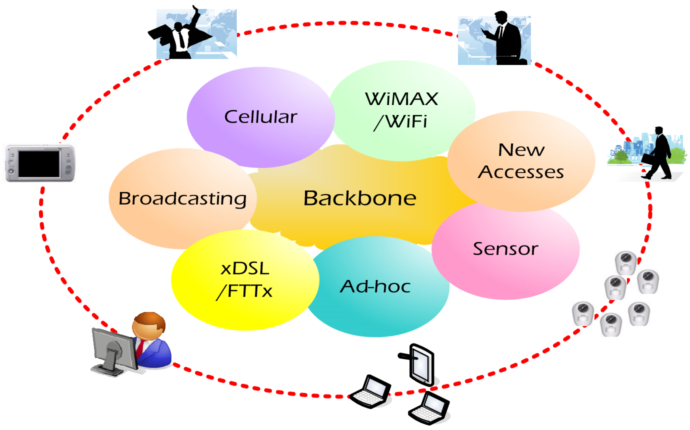
2.7 Others

In addition to the problems described above, some more issues may be identified and discussed in the design of future Internet. Those issues include QoS enhancement in mobile environment with limited bandwidth of wireless link and frequent handovers by movement. Security may be another critical issue.

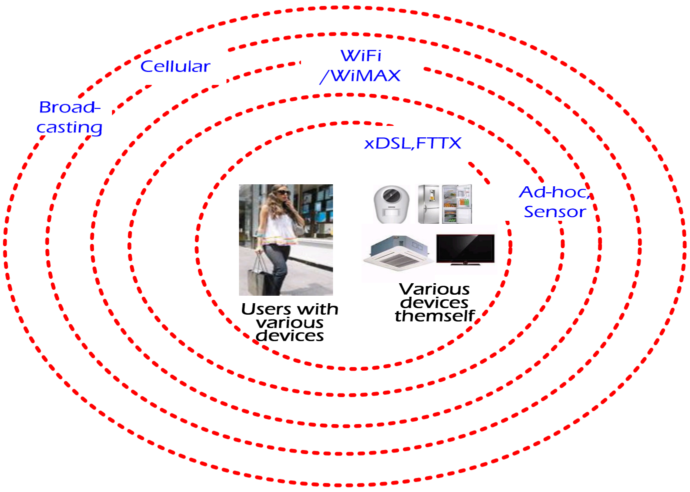
3. Design Considerations

3.1 Network Environment in Future Internet

To design the future Internet architecture, we first need to consider the network environment that could be envisioned in the future Internet. Figure 1 illustrates our view to future Internet in the perspectives of network and users/things, which 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 in Future Internet

As illustrated in the figures, in future Internet, users/things will benefit from a variety of access ways to the network anytime, anywhere, and through any interfaces. In particular, it is expected that 'mobile' users/things, rather 'fixed' ones, will become more dominant 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 oriented future Internet (MOFI).

3.2 Design Approaches

The MOFI is mainly designed with the following fundamental philosophy.

3.2.1 Future Internet as an ultimate convergence network

With a recent trend of network convergence, it is expected that the all kinds of networks will be evolved or revolved toward a unified network, i.e., 'mobile-oriented convergence network' as shown in Figure 2, including computer or telecommunication networks.

We note that computer (i.e., Internet) and telecom networks have quite different design philosophy and their own pros and cons, respectively. From the perspective of the convergence trends, future Internet should be designed to make full use of the pros of both computer and telecommunication networks.

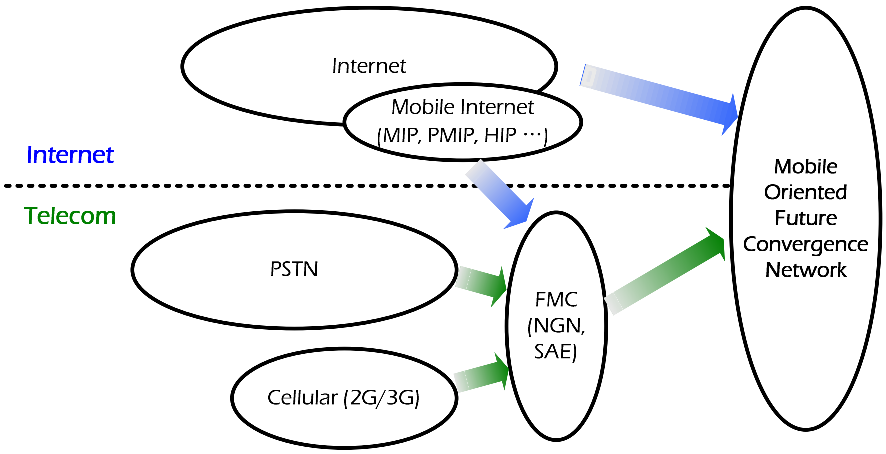


Figure 2 – Future network convergence towards a single type of network

In addition, we note that the current cellular system is a very successful model and provides a lot of desirable features to support the mobile environment. Therefore, we will readily exploit those useful features in the design of future Internet architecture, to the extent possible.

3.2.2 Intelligent network support to provide easy access

We see that Internet is now regarded as a kind of 'social infrastructure' beyond a mere technology or service. This trend will be more accelerated in the future Internet. Thus, all the users of future Internet shall be able to use every kind of Internet services more easily. To do this, the network should guarantee an easy access of every user. The easy access could be accomplished with the help of intelligent access nodes (e.g., router and agent in the network) that will perform many complicated operations on behalf of users. While keeping the traditional end-to-end concept of current Internet, the mobile-oriented future Internet will get a lot of benefits from the intelligent network support.

3.3 Technical Design Principles

With the design philosophy described above, we identify a set of design principles for MOFI.

3.3.1 Mobile-oriented and Static-allowed

The current Internet basically assumes that a host 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 that also allows static users/hosts at the same time.

In this sense, the mobility control functionality to support seamless services for mobile users should be provided as a basic function, not a supplement one. It means that the future Internet should be designed with the assumption that all the users are moving on.

3.3.2 ID-based Communication with LOC-based Routing

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 objects (or users) for communication without knowledge of its locator (LOC). The detailed mapping between ID and LOC will be managed by network.

In the context of ID-based communication, the following considerations will be taken:

1) Separation of Identifier and Locator

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 or delivery in the network.

In the current Internet, an IP address is used as identifier as well as locator in the network because it has focused on the fixed network. In future mobile oriented network environment, a user (or object) identifier needs to be separated from its locator, since the locator may change by movement, but the identifier should not change to keep the on-going session. That is, an identifier should be used only to identify an object in the viewpoint of service provisioning, whereas a locator should be used so as to effectively locate the object and to deliver packets in the network.

2) Address-free Host

In terms of mobility, another problem of the current Internet is that a 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 host does not configure its own address, so as to reduce the handover delay. This is in the same line with the design goal, "ID-based communication."

3) ID-based End-to-end Global Communications and LOC-based Local Routing

In MOFI, the end-to-end communication between two end hosts will be performed based on the host ID. Each host ID shall be globally unique in the network, and it will use an appropriate socket interface that consists of a host ID and a port number.

On the other hand, the routing for packet delivery will be done using the LOCs. The associated LOCs may be local and private in the network. Furthermore, one or more LOCs and different routing schemes may be used along the path until the data packets are delivered to the final end hosts.

3.3.3 Protocol Separation for Access and Backbone Networks

In MOFI, the protocols used in access and backbone networks will be separated in the data transport and control perspectives. In future Internet environment, each access network and the backbone network may have quite different characteristics. For example, access networks might consist of the wireless links with relatively low bandwidth and unreliable transmissions, whereas the backbone network will be the optical network with high bandwidth to provide reliable transmissions. Accordingly, the protocol requirements for the access and backbone networks may be quite different. This implies that the protocols used in the access network need to be designed by considering the wireless link characteristics, whereas the protocols used in the backbone network may be designed to be as simple as possible by considering the optical networks.

The access networks should be able to guarantee easy access of users, whereas the backbone network is primarily purposed to provide effective delivery of packets. In this context, we need to separate the protocols used for access and backbone networks in the design of MOFI.

In particular, we also note that the current IPv4/v6 protocols can be used in the backbone network, as an incremental approach (or a tentative solution) to deployment of future Internet. This is because the backbone network is quite difficult to replace with a completely new protocol at a stretch, compared to the access network. This approach will also be helpful for migration from the current Internet to the clean-slate future Internet.

3.3.4 Functional Separation for Mobility Control and Data Delivery

We note that the control information (e.g., for mobility control) is usually mission-critical and thus requires the fast and reliable delivery in the network. Accordingly, the control plane (or function) needs to be performed differently from the user data plane (function) in MOFI, as done in the current cellular systems.

In particular, MOFI will be designed for network-based mobility control, since the network-based mobility scheme is preferred to the host-based mobility scheme in the viewpoint of resource utilization, protocol performance and deployment, as shown in the comparison of MIPv6 [3] and Proxy MIPv6 (PMIPv6) [12]. In addition, the mobility control of MOFI will provide the 'intrinsic' route optimization, by which the direct path should be used between two hosts from the beginning of communication with the help of the mobility control.

4. FUNCTIONAL ARCHITECTURE

4.1 NAME, HOST IDENTIFIERS AND LOCATOR

The most essential elements associated with communication include name, identifier and locator. A name represents "who it is." An identifier is used to represent "what it is" and a locator is to represent "where it is."

In MOFI, as depicted in Figure 3, the two types of mapping are used: 1) mapping from Name to Host ID (HID), which is managed by Name-HID Mapping System (NMS), and 2) binding between HID and Locator (LOC), which is managed by LOC Binding System (LBS). By using these mapping and binding systems, the name shall be eventually translated to Locator (LOC) via HID for end-to-end communications.

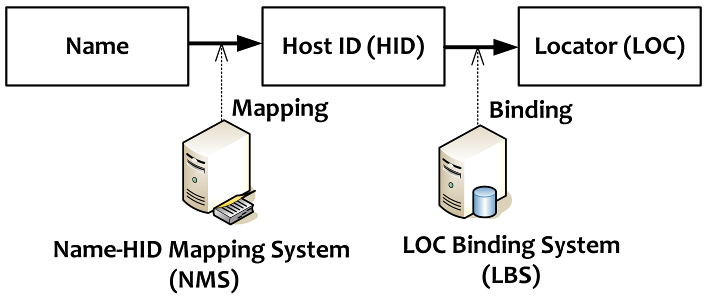


Figure 3 – Name, HID and LOC

NMS provides decoupling of user/service/data (object's name) from the host (HID). For example, we can access to a particular object with multiple hosts (HIDs), or a host (HID) may be shared by multiple objects (name). An object (name) may be moved or copied from a host to another (HID).

LBS will also provide decoupling of location (LOC) from host (HID), in particular, in the mobile networks. Note that the LOC is subject to change by movement of mobile host, but HID is persistent. A host is identified by HID, and the changeable LOC is used for routing of packets in the backbone network.

4.1.1 NAME

Name is used by a human user to uniquely identify a corresponding (communicating) object in the network. An object may be human, device, data, service, etc. For human's understanding, Name should be human-readable, i. e., alphanumeric.

A string of characters or numbers that are human readable or understandable are used to represent a name. The specific format of name may depend on services and applications deployed in future Internet. So far, some promising formats of name include a host name (e.g., www.google.com), Network Access Identifier (NAI) such as user@realm and telephone number such as 12-345-5679. Some more formats of name may be defined additionally in the future.

(Note) For scalable naming, a hierarchical structure of name can be considered, which may consist of the diverse components such as service provider, users, applications/services, etc.

4.1.2 HOST ID (HID)

A human, service or data identified by name will be served on an end host. For delivery of data, the end host should be identified by HID in a static and secure manner, because each HID is used for communication and may be revealed to an unknown user. We may consider a fixed-length (e. g., 128-bit) and cryptographic HID.

At present, we consider the format of 128-bit HID. This may be similar to the Host Identity Tag (HIT) of Host Identity Protocol (HIP) [13], which generated based on the Overlay Routable Cryptographic Hash Identifiers (ORCHID) [14]. As described in [13, 14], these HID formats two advantages of using a hash function in protocols. First, its fixed length makes for easier protocol coding and also better manages the packet size cost of this technology. Second, it presents the identity in a consistent format to the protocol independent of the cryptographic algorithms used. A specific mechanism of how to implement these HIDs in MOFI is still for further study.

The mapping from name to HID is managed by the Name-HID Mapping System (NMS), which may be implemented with a server or a hierarchical system of servers. Note that the legacy Domain Name System (DNS) may be regarded as an example of NMS in that it maintains the mapping between hostname (name) and IP address, if IP address is used as HID. The mapping information between name and HID contained in NMS may be statically configured or dynamically updated. For example, if an object (data/service) is moved from one host to another, the associated mapping entry of NMS will be dynamically updated.

(Note)Similar to naming scheme, the HID can also be in the hierarchical format for scalable management of HIDs in the world-wide scale. This is still for further study.

4.1.3 LOCATOR (LOC)

Locator (LOC) is used to represent the location of an object in the network. An LOC may contain the information about topological or geographical location of the user in the network. LOC is also used for delivery of data packets between objects in the network.

In MOFI, an IP address of the access router (attached to the end host) is used as LOC of the end host. Other formats of LOC are still for further study. A locator is used only in the 'backbone' network in the form of IP address, whereas the HID is used for communication only in the access network. In mobile environments, a host with a single HID may change its LOCs by movement.

4.1.4 LINK ID (LID)

In addition, we consider Link ID (LID) to identify a link (connection point or interface) of a host to the access network, which is needed for data packet delivery between the access router and a host. Examples of LID include the IEEE 802 MAC address and any other link-layer physical addresses of hosts for wired/wireless network interfaces.

An LID is given for each network interface of a host, and thus a multi-homing host may have two or more LIDs. The specific format of LID depends on the associated link-layer access technologies. At present, we consider the following LIDs:

- IEEE 802 MAC address (for LAN or WLAN);
- GPRS Tunnel ID (for cellular networks);

- IPv6 or IPv4 address (for overlay network).

In a certain case, a LID may consist of a sequence of two or more IDs for an access router to identify the host in the access network (for example, one or more PoAs are located between host and access router).

4.2 Functional Reference Model

We consider the following functional reference model of MOFI, as shown in the figure below.

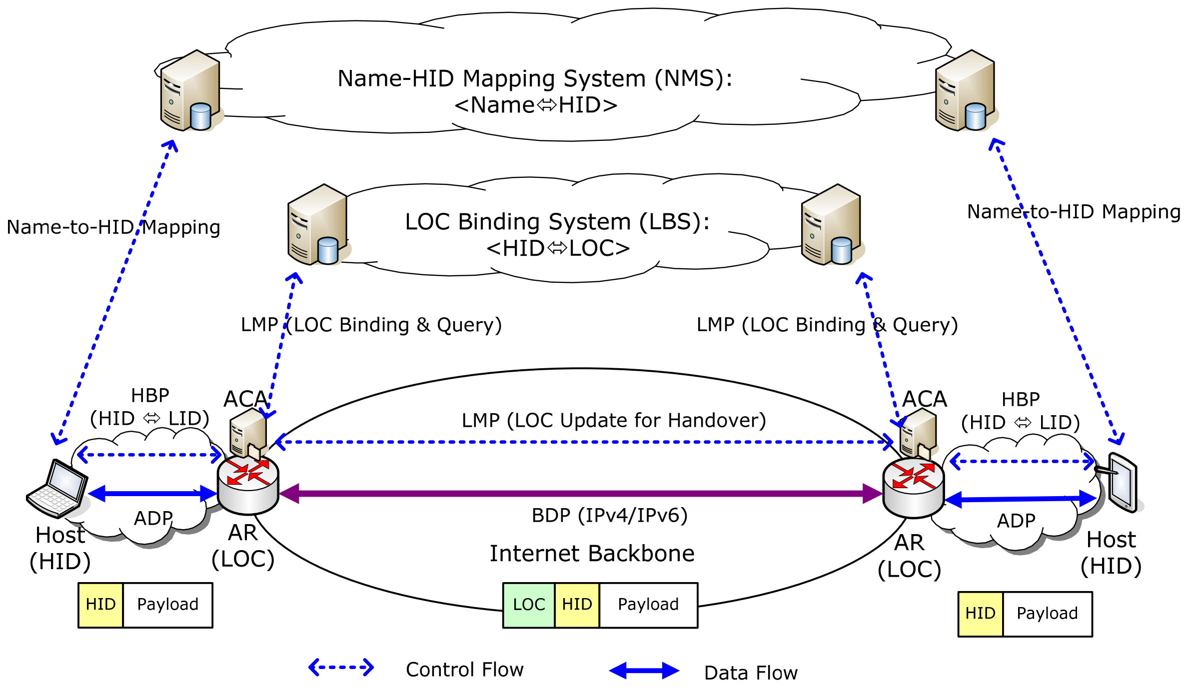


Figure 4 – Functional reference model of MOFI

In the figure the following notations are used:

- NMS: Name-HID Mapping System;
- LBS: LOC Binding System;
- HBP: HID Binding Protocol;
- ADP: Access Delivery Protocol, which is optionally used;
- AR: Access Router;
- ACA: Access Control Agent;
- LMP: LOC Management Protocol.

4.3 Functional Entities

4.3.1 Name-HID Mapping System (NMS)

NMS is responsible for mapping between the names of objects (or users) and the HIDs of hosts. In MOFI, each calling user has only to know the name of the corresponding user. To get an HID of the corresponding host, the calling host may consult with NMS, on behalf of the calling user. NMS may need to dynamically update the HIDs for the name of an object according to "contents mobility" such as file copy/move, server/host change, etc.

The NMS can be a logical overlay network that may consist of a lot of distributed servers in the world-wide scale, as shown in the current DNS architecture. For scalable management of NMS, a hierarchical name format may be used, which is for further study.

4.3.2 Hosts

In MOFI, it is assumed that an object (or user) is identified by a name and has its own host that is identified by HID. A name is service-specific and mapped onto one or more HID. This operation will be performed between a host and NMS.

A host has one or more Link Identifiers (LIDs), depending on whether the host has a single or multiple network interfaces for host multi-homing. For communication, a host shall be attached to an AR in the network. When a host is attached to an AR, its HID and LID(s) shall be registered with AR. This operation is called 'HID Binding Protocol (HBP).'

4.3.3 Access Router (AR)

In future Internet, there may be a variety of wired/wireless access networks between hosts and AR. Depending on the underlying access network, one or more Point of Attachments (PoAs) or routers may be located between host and AR, as shown in the example of wireless ad hoc, sensor, or wireless mesh networks.

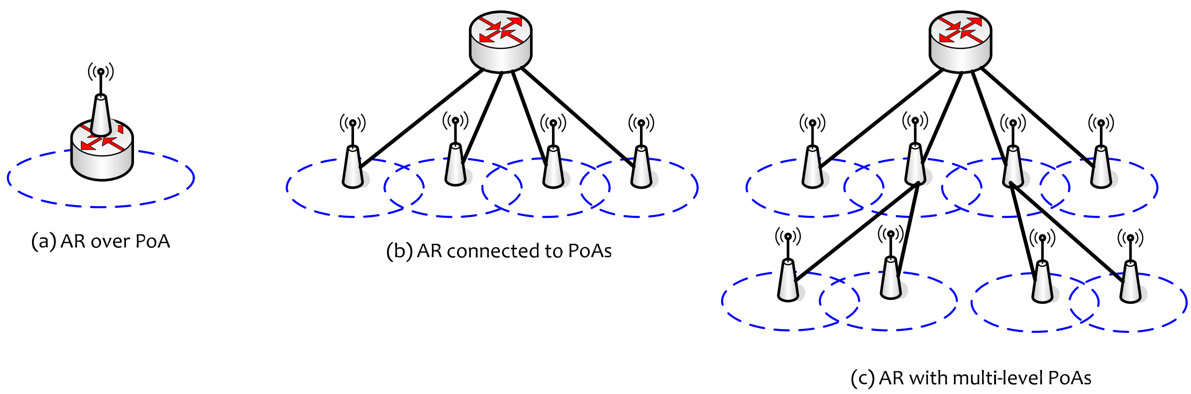


Figure 5 – Configuration of AR and PoA

In the deployment perspective of an access network, as shown in Fig. 5, an AR may be located over the underlying link-layer Point of Attachment (PoA), in which host is directly connected to

AR in the link layer (Fig. 5(a)). Alternatively, one or more PoAs may be connected to the AR, as shown in Fig. 5(b). In this case, a host communicates with AR via one of candidate PoAs, in which the mobility of host across two neighbouring PoAs will be managed by the corresponding link-layer mobility management scheme, which is outside the scope of MOFI. In a certain case, a tree hierarchy of PoAs with two or more levels may be configured in the network, as seen in the wireless mesh networks of IEEE 802.11s.

With network attachment, a host shall bind its HID and LID to AR via the HBP protocol. After that, the host sends or receives data packets to or from AR by using the Access Delivery Protocol (ADP). That is, AR receives the data packets from its local host and forwards them to the correspondent host in the network by using the legacy IPv4/IPv6 protocols. When AR receives data packets from the remote AR, it will deliver those packets to the local hosts by using the ADP.

In the perspective of mobility control, AR uses its Access Control Agent (ACA).

4.3.4 INTERNET BACKBONE

In MOFI, the backbone network represents the legacy Internet that consists of a lot of site networks, ISPs, and network providers. In the Internet backbone network, the data delivery mechanisms will follow the currently used IPv4/IPv6 protocols.

4.3.5 ACCESS CONTROL AGENT (ACA)

ACA is an agent located with AR, which is in charge of control operations such as LOC binding and query. Each ACA is likely to be implemented with AR. That is, AR and ACA may be just logically (or functionally) separated, but physically co-located over the same equipment, as shown in the example of MSC and VLR in the GSM system.

Each ACA performs LOC binding and query operations with LBS by using the LOC Management Protocol (LMP), which is used to get the information of LOC for data delivery. LMP is also used for handover control of mobile hosts, which is performed between ACAs.

4.3.6 LOC BINDING SYSTEM (LBS)

The LBS provides a database for binding between HID and LOC. When LBS receives an LOC binding request message from an ACA, it creates or updates the HID-LOC binding information in the database. In addition, when an ACA asks LBS for the HID-LOC binding information to a specific HID, LBS will reply with the corresponding LOC information to the ACA. LBS may maintain a database that contains information about users' service profile and authentication.

The LBS is a logical overlay network that may consist of a lot of distributed servers in the world-wide scale. For load sharing and/or scalability enhancement of control operations, the LBS may be configured in the hierarchical or distributed manner. In addition, for scalable management of LBS system in the mobile environments, Home LBS and Visited LBS may be used, as seen in the example of Home Location Register (HLR) and Visited Location Register (VLR) in the GSM system.

(Note) For scalable LBS management, a hierarchical format of HID may be considered.

4.4 MOFI PROTOCOLS

4.4.1 HID-BASED COMMUNICATION PROTOCOL (HCP)

MOFI is featured by HID-based communications and LOC-based routing. The details of end-to-end communication will be governed by the HID-based Communication Protocol (HCP), in which HIDs of the two end hosts are used as identifiers.

4.4.2 ACCESS DELIVERY PROTOCOL (ADP)

ADP is a data delivery protocol that is used to deliver data packets between host and AR in the access network, in which LIDs of hosts are used for packet delivery. The details of ADP will be described later.

4.4.3 BACKBONE DELIVERY PROTOCOL (BDP)

BDP is a data delivery protocol that is used to deliver data packets between ARs over Internet backbone network, in which LOC (IP address of AR) will be used for packer routing. At present, we use the current IPv4/IPv6 routing schemes as BDP.

4.4.4 HID BINDING PROTOCOL (HBP)

HBP is a control protocol that is used to bind the HID and LID of a host to the associated AR. The details of HBP will be described later.

4.4.5 LOC MANAGEMENT PROTOCOL (LMP)

LMP is a mobility control protocol. LMP is performed between ACA and LBS to bind the HID and LOC of a host to LBS, or to query the LOC of a correspondent host. LMP is also performed between two ARs to support seamless handover and LOC update by handover. The details of LMP will be described later.

4.5 DATA TRANSPORT MODEL

In this section, the data represents the user data packets for communications between hosts.

4.5.1 PROTOCOL STACK FOR DATA TRANSPORT

MOFI will take a layered model similar to the current Internet architecture in the protocol stack point of view. It is noted that the layering architecture and relevant protocol design of future Internet includes a lot of issues to be considered simultaneously, which still needs significant challenges with further researches and experimentations. Therefore, as an initial step, MOFI will focus on the network layer, i.e. IP layer, rather than the other layers. That is, we will propose a simplified protocol model as a basis to design the MOFI in the network layer, which could possibly be integrated as a building block component into the overall design of future Internet.

MOFI considers a protocol stack for data transport, as shown in the figure below.

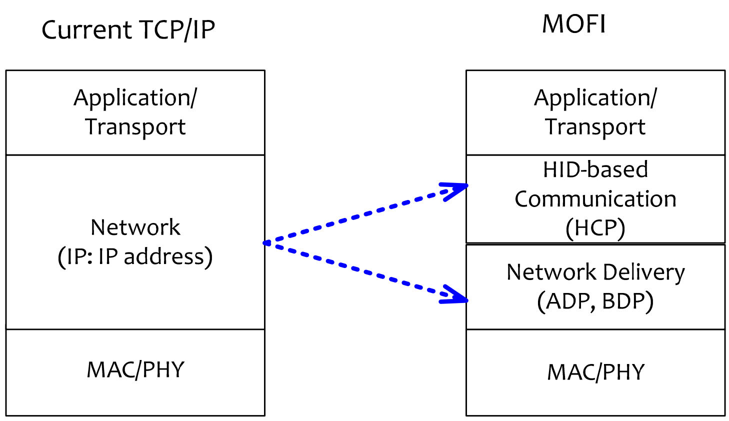


Figure 6 – Comparison of protocol stacks for data transport: TCP/IP versus MOFI

- **Application/Transport Layers**

  At present, the current application-layer and transport-layer protocols are used in MOFI, which requires further considerations in the engineering perspective of future Internet.

- **Network Layer**

  In MOFI, the network later is divided into the two sub-layers: HID-based communication and network delivery. HID Communication Protocol (HCP) is newly defined for end-to-end communication based on HID. HCP is responsible for end-to-end user data communications between two end hosts, which include interaction with transport layer protocols (TCP, UDP) and the provisioning of socket interface with applications.

  The routing protocols for data delivery are divided into ADP (optional) and BDP. The current IP is used as BDP for data delivery over Internet, whereas ADP is optionally used for routing in access networks. For example, ADP is omitted in the IEEE 802-based access networks, whereas the Point-to-Point Protocol (PPP) may be used as ADP between host and AR in the 3G/4G cellular systems.

- **MAC/PHY Layers**

  These layers depend on the underlying link technology, which are outside the scope of MOFI.

Fig. 7 summarizes the protocol stacks associated with data delivery between two end hosts.

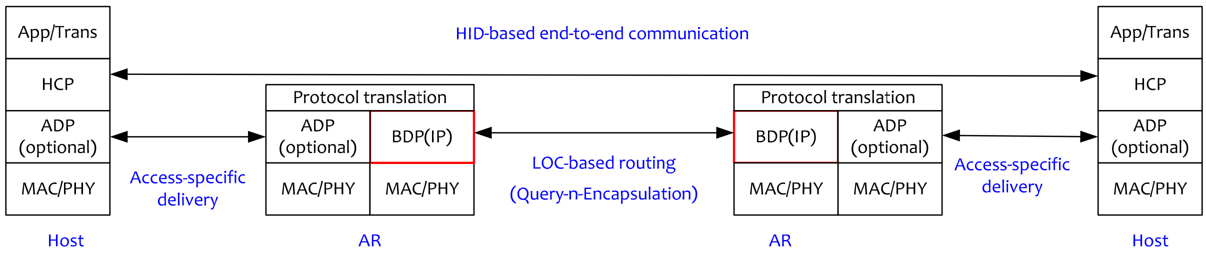


Figure 7 – Protocol model for data delivery

HCP will define the protocol operations and packet format that are used for end-to-end communication between two end hosts. Each AR or intermediate routers are not aware of the HCP. Instead, they may refer to the HID value for translation of the data delivery protocol between ADP and BDP (IP).

ADP is specific to the underlying access network technology, which may be one-hop or multi-hop networks. In case of multi-hop access networks, the LID will be used for data packet delivery between host and AR, possibly via one or more PoAs or internal routers in the access network.

4.5.2 DATA TRANSPORT PROCEDURES

In MOFI, data communications will be essentially accomplished with HID, not IP address that is used in the current Internet. More technically, a user will initiate a communication session with a name of the corresponding object. The name of the corresponding user will be converted to the associated HID with the help of NMS, before data transport operation. LOC (i.e. IP address of AR) is used only for data delivery in backbone network.

For discussion, we consider a simple communication scenario in which a sending host (SH) wants to communicate to a receiving host (RH). If SH has the information on HID of RH, which will be performed with the help of NMS, the overall data transport operations are performed, as shown in the figure below.

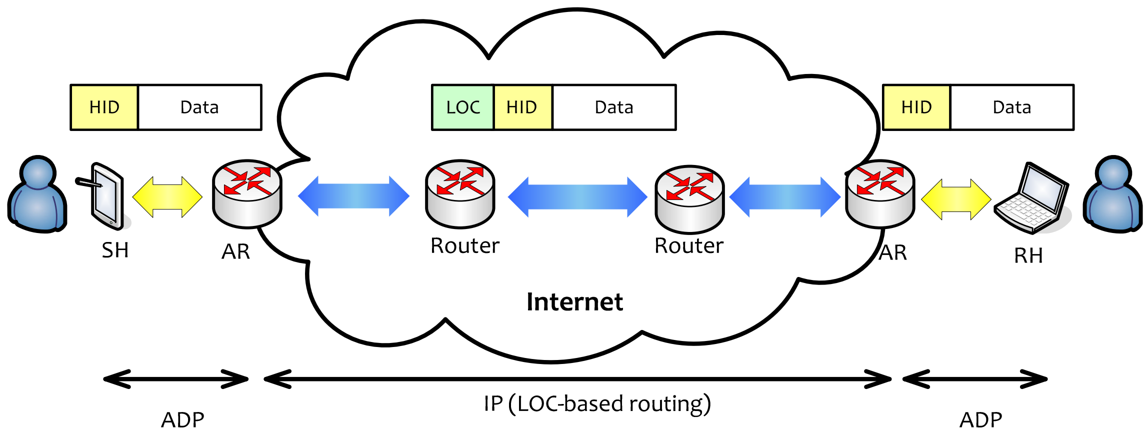


Figure 8 – Data transport procedures in MOFI

The data packet transport operations are summarized as follows:

1) Data transmission (SH ⇔ AR)

SH sends the data packets to AR by using HID of RH. It is noted that SH does not need to know the LOC of RH (that is, the IP address of AR that is attached to RH).

2) Query and encapsulation (AR of SH)

On reception of data packets from SH, the AR of SH will first identify the LOC of RH by using the LMP protocol, which will be described later. Then, AR of SH will encapsulate the data packets by adding the LOC of RH (IP address of AR of RH) into the outer header of the data packet.

3) Packet delivery in the backbone network

The encapsulated data packets are delivered from AR of SH to AR of ER by using the current IP routing/forwarding, possibly via one or more routers in the backbone network.

4) Decapsulation (AR of RH)

On reception of the encapsulated data packets, the AR of RH will extract the original data packets by decapsulation, and then forward them to RH.

5) Data reception (AR ⇔ RH)

Finally, the RH can receive the original data packets transmitted by SH.

4.6 Mobility Control Model

In MOFI, the following control operations are supported:

- HID Binding between host and AR;
- LOC Binding and Query between ACA and LBS;
- Handover Control between ACAs.

To support these control operations, we define the HID Binding Protocol (HBP) and LOC Management Protocol (LBP). HBP is used to bind the LID and HID of host to AR, whereas LMP is used for LOC binding and query with LBS and for handover control of mobile hosts between ACAs.

4.6.1 HID Binding

The HBP is used to bind the HID and LID of host to AR. Fig. 9 shows the protocol stack of HBP between host and AR.

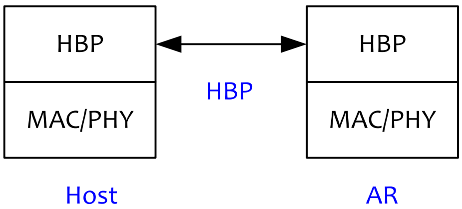


Figure 9 – HBP between host and AR

4.6.2 LOC Binding and Query

When a host is connected to AR, the corresponding ACA will bind the LOC and HID of host to LBS. For data delivery, each ACA will contact with LBS so as to get the LOC information of the corresponding host. Fig. 10 shows the protocol stack of LMP for LOC binding and query between ACA and LBS.

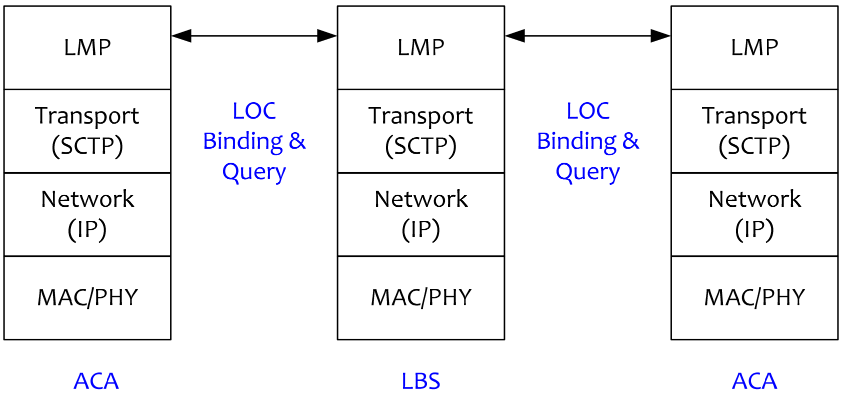


Figure 10 – LMP for LOC Binding and Query between ACA and LBS

Note that the LMP messages will be encapsulated into the Stream Control Transmission Protocol (SCTP), rather than the TCP/UDP.

4.6.3 HANDOVER CONTROL

LMP is also used to support the fast handover for mobile hosts. For handover control, the LMP is performed between two ACAs and the associated control messages are encapsulated into the SCTP, as shown in the figure below. Note that the LMP operates based on the IEEE 802.21 Media Independent Handover (MIH) between host and AR, in which appropriate link-layer triggers will be used such as Link-Up, Link-Down, Link-Coming-Up, Link-Going-Down.

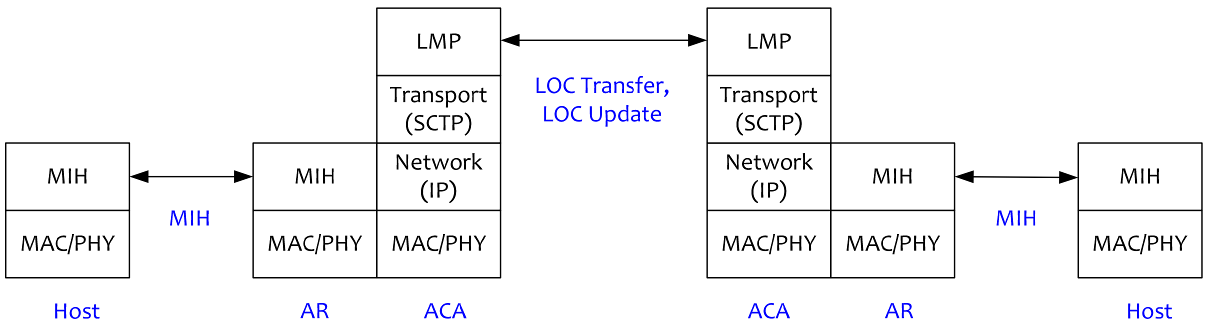


Figure 11 – Handover Control Protocol with MIH

For handover control, the LOC Transfer (LT) operation is performed between the two neighbouring ACAs associated with mobile host, and the LOC Update (LU) operation is used between local ACA and remote ACA to update the LOCs in communication. The details of handover control will be described in the subsequent section.

5. PROTOCOLS

5.1 HID COMMUNICATION PROTOCOL (HCP)

In MOFI, the HCP is newly defined for end-to-end communication between two hosts. This is NOT for data delivery or routing, BUT for communication. That is, the HID is not used for routing of data packets in the network. Instead, it will be used for end-to-end communication using the upper layer transport layer protocol (TCP/UDP) and a socket interface with an application program.

5.1.1 HCP HEADER FORMAT

For design of HCP packet format, we refer to the current IPv6 header format for backward compatibility. An HCP packet has the following abstract packet format:

0	4	16	24	31
Version	Reserved			
Payload Length		Next Header	Reserved	
Source HID (128 bits)				
Destination HID (128 bits)				
Payload extension headers + Data packet from the upper layer (e.g., TCP, UDP)				

Figure 12 – Abstract Format of HCP Header

Packet Field Description:

- Version (4 bits): indicates this version of HCP, which may be used to make it compatible with the current IP version;
- Reserved (12 bits): reserved for future use, and set to 0;
- Payload Length (16 bits): the length of user payload (in byte) following this FIP header;
- Next Header (8 bits): this is the same with the Next Header of IPv6 header.
- Reserved (8 bits): reserved for future use, and set to 0;
- S-HID (128 bits): Source HID
- D-HID (128 bits): Destination HID.

5.1.2 Encapsulation for Data Delivery

For data delivery, the HCP packet will be encapsulated into the corresponding delivery protocol, ADP or IP, as shown in the figure below.

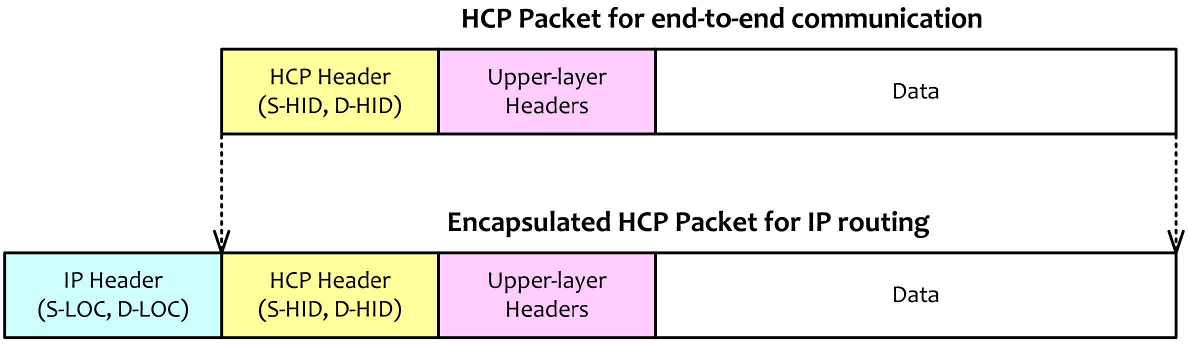


Figure 13 – Structure of data packets

5.2 Access Delivery Protocol (ADP)

ADP can be optionally used for data transport between host and AR. If a host is directly connected to AR with a single hop, the ADP may be omitted depending on the underlying access network (e.g., in the IEEE 802.3 access networks). More detailed operations and packet formats of ADP are still for further study.

5.3 Backbone Delivery Protocol (BDP)

In MOFI, the current IPv4/IPv6 routing/forwarding schemes are used as BDP at present. Thus, the semantics and operations of BDP will follow the current IPv4/IPv6.

5.4 HID BINDING PROTOCOL (HBP)

5.4.1 OPERATIONS

When a host is attached to the network, it will establish the network connection with the concerned PoA via an appropriate link-layer connection establishment process. 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 so outside the scope of the MOFI.

With the network attachment of host, the HID binding operation is required, in which HID and LID of the host will be registered with AR attached to the host. AR will maintain and update its cache table, called “HID Cache” (HC) that contains the information of bindings between HIDs and LIDs for all of the hosts attached to the AR.

In MOFI, we assume that the HID binding will be performed with the underlying ‘access link layer’ protocol, implicitly or explicitly, as shown in the figure below.

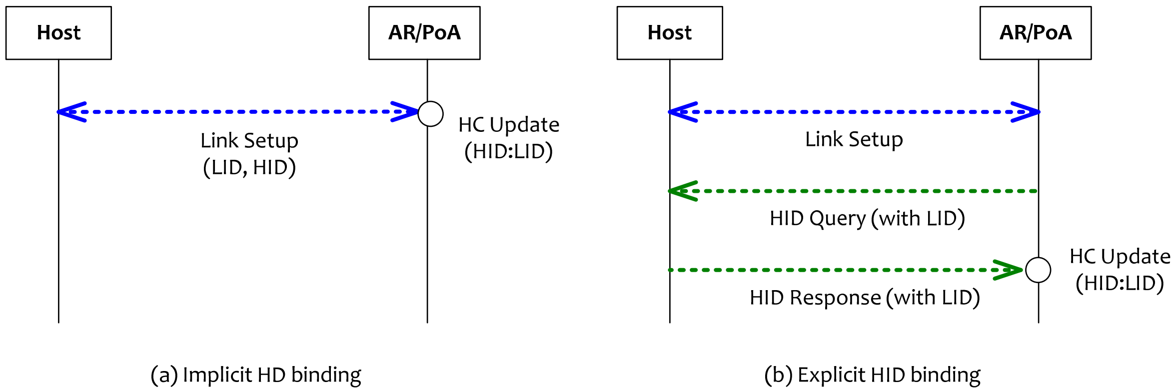


Figure 14 – HID binding between host and AR/PoA

In the implicit HID binding, the binding between HID and LID will be done during the underlying link-layer attachment process. In the explicit HID binding, after the link setup, the AR may request the HID information to the host explicitly by sending the HID query message (in multicast or broadcast), and then the host will respond with its HID to AR (in unicast).

5.4.2 HID CACHE (HC)

In the HID binding operation, AR maintains and updates its own HID cache by recording the HIDs and LIDs associated with the hosts in the local subnet. The abstract format of the HID cache table is shown below.

Table 1 – HID Cache

No.	HID	LID	Link Information	Status	Type
1	HID1	LID1	…	Idle	Static
2	HID2	LID2	…	Active	Static
3	HID3	LID3	…	Idle	Mobile
4	HID4	LID4	…	Active	Mobile
5	…	…	…	…	…

The cache information will be referred to by AR for delivery of the data packets that are destined to the hosts in the local subnet. In the table, the status field (idle or active) represents whether or not the host is in the active data communication with a certain other corresponding host. That is, 'active' means the HID is bound to the network and also in communication with the other host(s), while 'idle' implies that the host is bound but not in communication. In addition, the HC cache may indicate the type of host (static or mobile), and the information associated with the link may be used, (e.g., information of contact with the PoA of host, etc), which is for further study.

5.5 LOC Management Protocol (LMP)

In MOFI, LMP is used for LOC binding and query between ACA and LBS, and for handover control between two ACAs. For this purpose, LBS is with LOC database, and ACA is with LOC Cache (LC).

5.5.1 LBS with LOC Database (DB)

LBS is used to manage the LOC information of all of the users in the network. For this purpose, LBS maintains the location database, which contains information of mapping between HIDs and LOCs for all of the hosts.

When a host moves into a new AR, its ACA will perform the LOC Binding (LB) operation with LBS. From this LB operation, HID and LOC of a host will be registered with LBS. Accordingly, LBS will maintain the following Location DB, as shown in the table below.

Table 2 – LBS LOC Database

No.	HID	LOC	Service Profile
1	HID1	LOC1	Related data
2	HID2	LOC2	Related data
3	…	…	…

5.5.2 ACA with LOC Cache (LC)

For data delivery, each ACA performs the LOC Query (LQ) operations with LBS. When a host wants to communicate with another host, the associated ACA/AR will perform the LQ operation with LBS so as to get the LOC of the corresponding HID. From this LQ operation, each ACA maintains the LOC Cache (LC) for each of the corresponding (remote) HIDs, as shown in the table below.

Table 3 – ACA LOC Cache

No.	Remote HID	Remote LOC
1	HID1	LOC1
2	HID2	LOC2
3	…	…

5.5.3 LOCATION BINDING (LB) OPERATIONS

When an AR detects a new host in its network region, its associated ACA shall perform the LB operation by sending a LB Request (LBR) message to the LBS. The LBR message shall include the HID and LOC of the host. LBS responds with the corresponding LB ACK (LBA) message to ACA. This LB operation will be performed each time a host moves into a new AR area, as shown in the figure below.

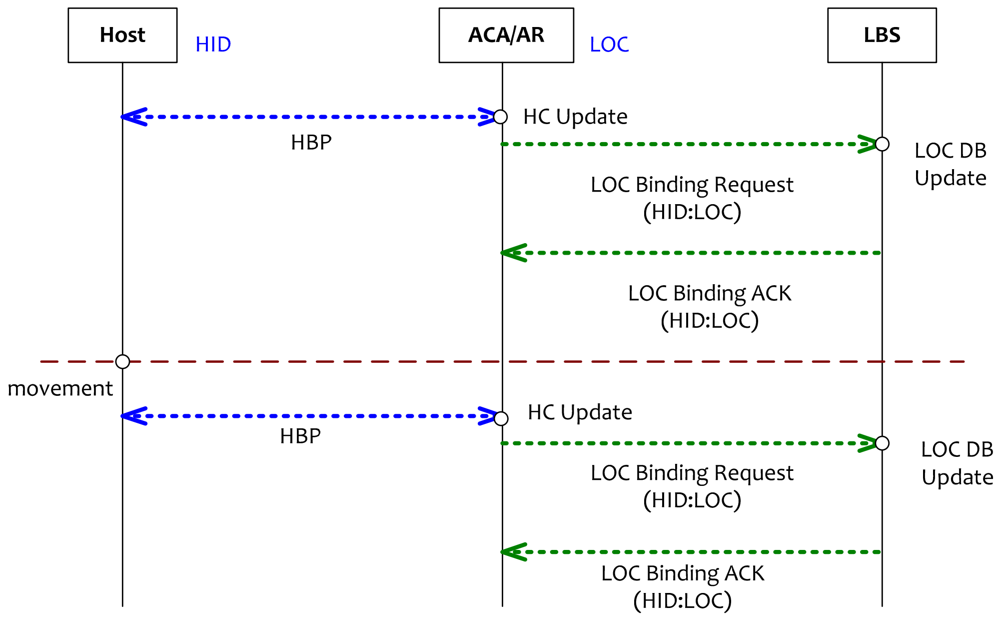


Figure 15 – LOC Binding Operations of LMP

5.5.4 LOC QUERY OPERATIONS

We assume that the corresponding host has completed its LB operation. Let us consider Sending Host (SH) with S-HID that sends data packets to the Receiving Host (RH) with R-HID. In this phase, the AR of SH needs to perform the LQ operation with LBS. An example of data delivery from SH to RH is illustrated in the figure below.

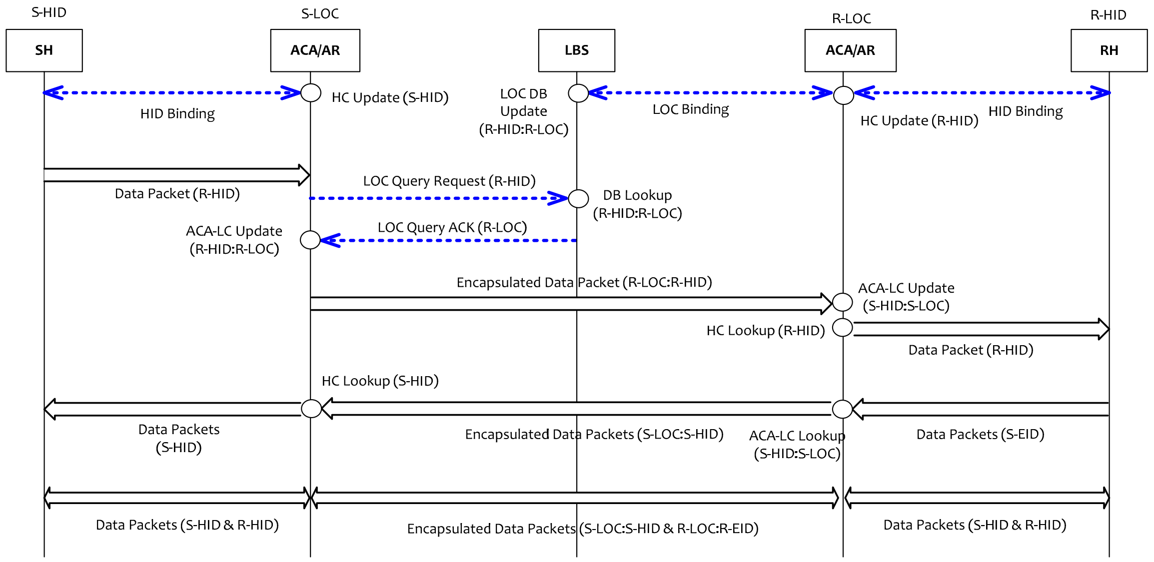


Figure 16 – Location Query of LMP for Data Delivery

Then the data delivery procedures could be done as follows:

1) Initially, both SH and RH are bound to S-AR and R-AR by using the respective HBP protocols, in which the associated HBP caches are updated with S-HID:S-LID and R-HID:R-LID. It is also assumed that the LB operations for R-HID and R-LOC have been completed between R-ACA and LBS.
2) SH sends an initial data packet to RH via its attached S-AR;
3) ACA/AR of SH will first look up its LOC Cache (LC) table to find the LOC of R-HID; if yes, S-AR can deliver the data packet to the identified R-AR (R-LOC), which is not shown in the figure.
4) If ACA/AR of SH cannot find the LOC of R-HID in the ACA-LC table, it shall perform the LOC Query operation by sending an LQR message to LBS. In response to the LQR message, the LBS will lookup its Location DB to identify the R-LOC of R-HID, and then it sends the LQA message to the ACA of SH. Based on the received LQA message, ACA of SH will update its LC table by creating the entry for R-HID and R-LOC;
5) AR of SH will send the encapsulated data packets to the AR of RH (R-LOC);
6) On reception of the encapsulated data packets from AR of SH, the AR of RH extracts the original data packets from the encapsulated packets. ACA of RH will update its LC table by creating a new entry for S-HID and S-LOC. This is done for AR of RH to deliver the data packets from RH to SH in the future.
7) Then, AR of RH forwards the data packets to RH. To do this, ACA of RH will lookup its HBP cache to identify the LID of R-HID.
8) Up to now, the ACA-LC of SH and ACA-LC of RH have been constructed. Based on this information, RH can also send data packets to SH. That is, RH (R-HID) and SH (S-HID) can now exchange data packets by referring to the established HBP caches and ACA-LCs.

The following figure shows the abstract information flows of LB and LQ in the previous example.

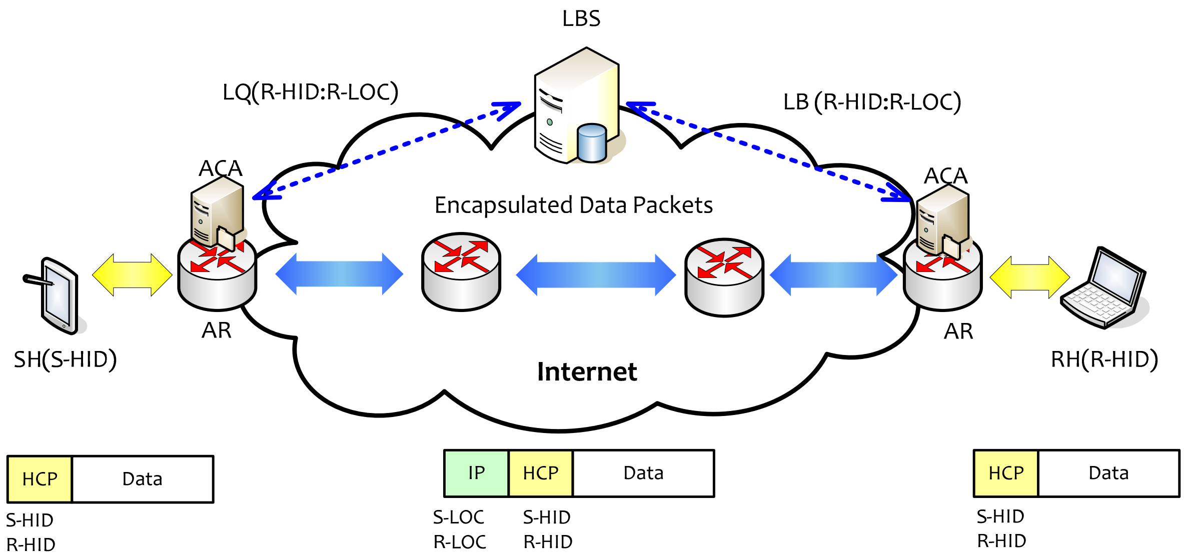


Figure 17 – Location Binding and Query for data delivery

For data transport, the ACA-LC maintains the list of the corresponding (remote) hosts that the local hosts are communicating with. On the other hand, HBP cache is used to forward the data packets to the attached local hosts.

5.5.5 HANDOVER CONTROL OPERATIONS

Handover control is used to provide service continuity for on-going sessions, especially in mobile environment. We note that some existing/future services require high level handover performance (i.e. low packet loss/latency) and some additional considerations should be given to support seamless handover. In this context, MOFI assumes the use of link-layer information such as Link-Up (LU), Link-Down (LD), Link-Going-Down (LGD), and Link Coming-Up (LCU), which are defined in the IEEE 802.21 MIH. At present, we will focus on the LU trigger only. The other triggers can also be examined to provide seamless handover.

We first consider the following simple handover scenario in which Mobile Host (MH) is communicating with Correspondent Host (CH), and it is moving from AR_old to AR_new.

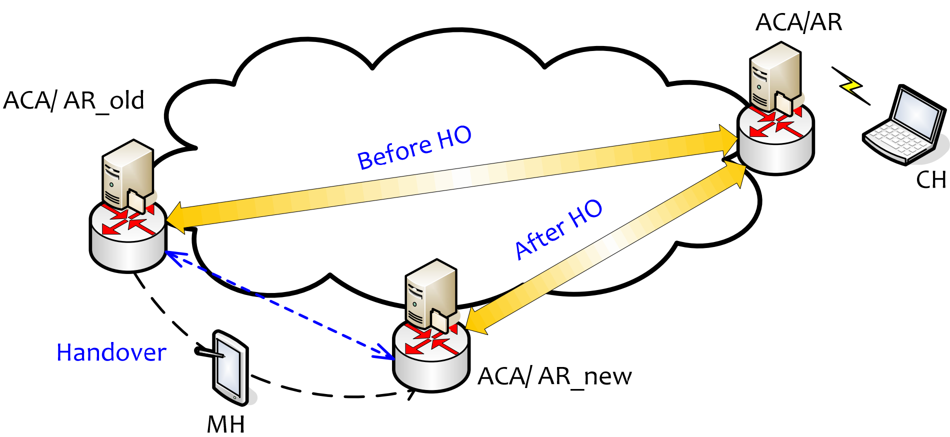


Figure 18 –Handover scenario

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

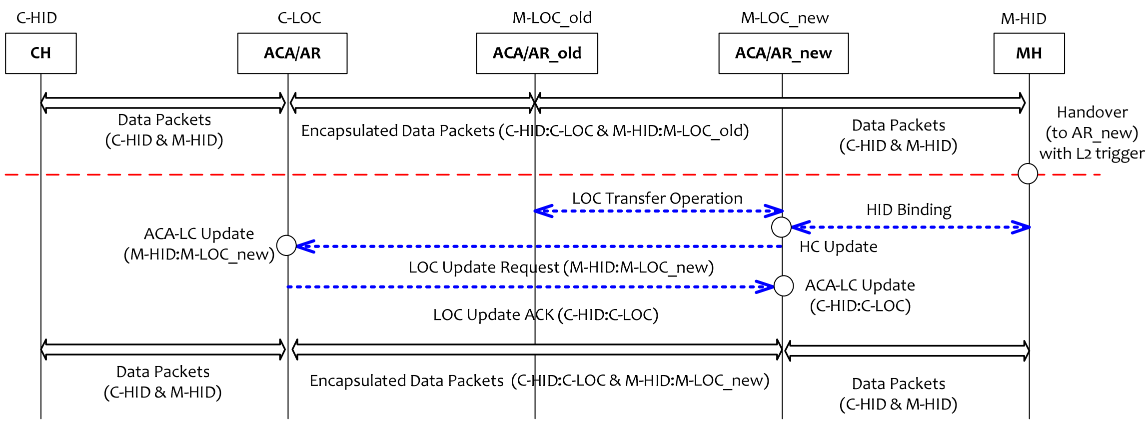


Figure 19 – Handover control by HCP

1) We assume that CH and MH (in AR_old) are communicating before handover. By handover, ACA_old (or ACA_new) of MH will get an LU trigger from the network. After that, ACA_old will exchange LOC Transfer Request (LTR) and LOC Transfer ACK (LTA) messages with ACA_new for handover control, which shall include the information of M-HID, C-HID, C-LOC.
2) AR_new of MH performs HBP with the newly attached MH, and the AR_new will update its HBP cache table for MH.
3) Now, the ACA_new of MH sends the LOC Update Request (LUR) message to the ACA of CH. On reception of the LUR message, ACA of CH will update its LC table with M-HID:M-LOC_old to M-HID:M-LOC_new.
4) In response to the LUR message, the ACA of CH will send the LOC Update ACK (LUA) message to the ACA_new of MH. On reception of the LUA message, the ACA_new updates its LC table by creating the C-HID:C-LOC entry.
5) The data path is now changed to CH ↔ AR of CH ↔ AR_new of MH ↔ MH.

In addition, the ACA will perform the LB operation after handover, which is not shown in the figures. This LB operation is for the newly incoming session to MH, which is performed independently of the handover control.

5.5.6 LMP PACKETS

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

Table 4 – Types of LMP Packets

Packet Type	Full Name	From	To
LBR	LOC Binding Request	ACA	LBS
LBA	LOC Binding ACK	LBS	ACA
LQR	LOC Query Request	ACA	LBS
LQA	LOC Query ACK	LBS	ACA
LTR	LOC Transfer Request	ACA	ACA
LTA	LOC Transfer ACK	ACA	ACA
LUR	LOC Update Request	ACA(local)	ACA(remote)
LUA	LOC Update ACK	ACA(remote)	ACA(local)

6. Further Issues

Some further optimization issues are listed below.

6.1.1 Scalability Issue of LBS

LBS is a single central server for mobility control. If the number of mobile hosts under the control of the LBS increases, the scalability issues may arise. For solve the problem, a hierarchical LBS structure could be considered, as we can see in Hierarchical MIPv6 [18].

Another concern of LBS scalability comes from "global HID". That is, LBS will be responsible for all the HIDs in the world-wide scale. To deal with this problem, a HID may be configured in th hierarchical manner, which is for further study.

6.1.2 Optimization for Seamless Handover

To provide seamless handover for mobile users, the following considerations need to be taken:

- 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 LBS-ACA and old FAR cache by handover, which may be done by using a timer or an explicit message.

6.1.3 Considerations of Heterogeneous Wireless 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.
- The idle mode host for saving the electrical power will be a substantial feature in the wireless/mobile communications. How to support idle mode hosts effectively need to be considered.
- Delay-Tolerant Networks (DTN) or unreliable wireless links needs to be considered in the mobility point of view.
- Consideration of wireless mesh network such as IEEE 802.11s.

6.1.4 Anonymous Access Support

Just as done in the current Internet, an anonymous access to the network will be essentially required even in the future Internet. Together with the higher manageability and controllability for efficient communication, we have to consider how to guarantee the anonymous access in the future Internet. For example, a free and anonymous access only with a pre-paid card could be supported, as done in the current cellular system.

7. COMPARISONS

7.1 ARCHITECTURE PERSPECTIVE

The following table briefly summarizes the comparison of HIP, LISP and MOFI in the architecture perspective of ID-LOC separation. The associated discussion is omitted.

Table 5 – Comparison of HIP, LISP, and MOFI

Features	HIP	LISP	MOFI
Approach	Host-based	Network-based	Network-based
Identifier	HIT	EID (IP address)	HID
Locator	IP address (host)	RLOC (IP address of Tunnel Router)	LOC (IP address of Access Router)
IP address	Used at host	Used at host and Border Router	Used at Access Router
Main purpose	Security	Routing Scalability	Mobility
BGP Routing Scalability	Not considered	Mainly considered	Not considered
Multi-homing	Host multi-homing	Site multi-homing	Host multi-homing
Location update by movement	Done by host	Done by host (in LISP-MN model)	Done by router (ACA)
Seamless Handover	Further study	Further study	Built-in support
Associated Network Agents	Rendezvous Server (RVS)	Tunnel Router (TR), Map Server (or ALT)	ACA, LBS
Host Modification	Needed (for socket API)	Not needed	Not Needed
Name-ID Mapping	DNS+ (need extension)	DNS	NMS (DNS is used for hostname)
ID-LOC Binding	RVS	Map Server (or ALT)	LBS
Routing Schemes	IP	IP	IP (and ADP)
Related Site	IETF HIP WG	IETF LISP WG	http://www.mofi.re.kr/

7.2 Mobility Perspective

The following table shows the comparison of the MOFI with the existing mobility protocols. The associated discussion is omitted.

Table 6 – Comparison of candidate schemes from the mobility perspective

Features	Mobile IP	Cellular MM (GSM-MAP) [19, 20]	MOFI
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 (EID)
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 EID
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

8. CONCLUDING REMARKS

The study of MOFI is motivated from the observation that the future networks would be evolved to mobile-oriented environment, but the current Internet was historically designed for static network environment and thus it is inevitably subject to some architectural limitations in the perspective of mobile-oriented future Internet. This leads us to re-design of Internet architecture to play a key role in the future mobile-oriented environment.

In this document, we have described the architecture of future Internet to effectively support the mobile-oriented environment, which is named MOFI. With considerations of some primary design principles for mobile-oriented future Internet, we design the architecture of MOFI and present a set of protocols to realize the proposed MOFI architecture. MOFI can be viewed as a revolutionary (clean-slate) approach in the access network aspect, and also as an evolutional (incremental) approach in the backbone network aspect for future Internet.

It is expected that MOFI will be considered as a building block component for overall design of future Internet architecture in the perspective of mobility. It is noted that there are still a lot of works to do in the engineering perspective of the proposed architecture and protocols. The corresponding works will continue by keeping pace with the overall design of future Internet architecture.

REFERENCES

[1] DG INFSO Task Force on the Future Internet Content, Draft Report of the Task Force on Interdisciplinary Research Activities applicable to the Future Internet, http://www.future-internet.eu/, July 2009
[2] IETF RFC 3344, IP Mobility Support for IPv4, August 2002
[3] IETF RFC 3775, Mobility Support in IPv6, June 2004
[4] eMobility Project, http://www.emobility.eu.org/
[5] 4WARD Project, http://www.4ward-project.eu/
[6] 4WARD, Dissemination and Exploitation Plan, Deliverable D0.1, June 2008
[7] Future Internet Design (FIND), http://www.nets-find.net/
[8] V. Arun, "Mobility First," NSF Future Internet Summit, October 2009
[9] Global Environment for Network Innovations (GENI), http://www.geni.net/
[10] AKARI, http://akari-project.nict.go.jp/eng/
[11] Ericsson, "Why Test the Next Generation Wireless Network with Your Grandfathers Internet Protocols?" Cross Forum Meeting, 26 March 2008
[12] IETF RFC 5213, Proxy Mobile IPv6, August 2008
[13] IETF Host Identity Protocol (HIP) WG, http://www.ietf.org/html.charters/hip-charter.html
[14] IETF RFC 4843, An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID), April 2007
[15] Name-to-HID Mapping System and Protocol, working in progress, http://www.mofi.re.kr/
[16] Host ID Binding Protocol (HBP) in MOFI, working in progress, http://www.mofi.re.kr/
[17] Access Delivery Protocols (ADP) in MOFI, working in progress, http://www.mofi.re.kr/
[18] IETF RFC 5380, Hierarchical Mobile IPv6 (HMIPv6) Mobility Management, October 2008
[19] Asha Mehrotra, GSM System Engineering, Artech House, 1997
[20] Yi-Bing Lin and Ai-Chun Pang, Wireless and mobile All-IP networks, Wiley, 2005

BIBLIOGRAPHY

The documents listed below are also helpful to understand this document:

[1] David D. Clark, "The design philosophy of the DARPA internet protocols," ACM Sigcomm, August 1988
[2] IETF RFC 1498, On the naming and binding of network destinations, August 1993
[3] M. Handly, "Why the Internet only just works," BT Technology Journal Vol. 24, No.3, July 2006
[4] Hari Balakrishnan et al., "A layered naming architecture for the Internet," ACM sigcomm, August 2004
[5] ITU-T Recommendation Y.2015, General requirements for ID/Locator separation in NGN, January 2009
[6] Bengt Ahlgren, et al., "Invariants-A New Design Methodology for Network Architectures", ACM Sigcomm, August 2004
[7] Hisashi Kobayashi, "An End to the End-to End Arguments," EuroView 2009, July 28, 2009
[8] J. F. Shoch, "Inter-network Naming, Addressing, and Routing," 17th IEEE Computer Society Conference, September 1978
[9] Saltzer, J. H., "Naming and Binding of Objects in Operating Systems," Lecture notes in Computer Science, Vol. 60, Springer-Verlag, 1978
[10] Sunshine, Carl A., "Addressing Problems in Multi-Network Systems", IEEE Infocom, March, 1982
[11] S. Keshav, "Naming, Addressing, and Forwarding Reconsidered," Manuscript, August, 2005
[12] P. Mockapetris and K.J. Dunlap, "Development of the Domain Name System, ACM Sigcomm 1988, August 1988
[13] David D. Clark, Karen Sollins, John Wroclawski, Ted Faber, "Addressing reality: an architectural response to real-world demands on the evolving Internet," ACM Sigcomm workshop on Future directions in network architecture, 2003
[14] I. Stoica, D. Adkins, S. Zhuang, S. Shenker, S. Surana, "Internet Indirection Infrastructure," Proceedings of ACM Sigcomm, August, 2002
[15] Jianli Pan, Subharthi Paul, Raj Jain and Xiaohu Xu, "Hybrid transition mechanism for MILSA architecture for the next generation Interent," IEEE Globecom, December 2009
[16] Jianli Pan, Subharthi Paul, Raj Jain and Mic Bowman, "MILSA: a mobility and multihoming supporting identifier locator split architecture for naming in the next generation Internet," IEEE Globecom, December 2008
[17] Kafle, V.P., Nakauchi, K., and Inone M, "Generic identifiers for ID/locator split internetworking," First ITU-T Kaleidoscope Academic Conference, May 2008
[18] John Day, Why Loc/Id split isn't the answer, http://pouzinsociety.org/, 2008
[19] IETF RFC 1287, Toward the future Internet architecture, December 1991
[20] D. Clark et al., "Tussle in Cyberspace: Defining tomorrow's Internet," ACM Sigcomm, August 2002

ABBREVIATIONS

ACA	Access Control Agent
ADP	Access Delivery Protocol
AR	Access Router
BDP	Backbone Delivery Protocol
DB	Database
FI	Future Internet
HBP	HID Binding Protocol
HC	HID Cache
HCP	HID Communication Protocol
HID	Host Identifier
IP	Internet Protocol
LID	Link ID
LB	LOC Binding
LBP	LOC Binding Protocol
LBS	LOC Binding System
LC	LOC Cache
LMP	LOC Management Protocol
LOC	Locator
LQ	LOC Query
MOFI	Mobile-Oriented Future Internet
NMS	Name-HID Mapping System
PoA	Point of Attachment

End of Document