Mobility Ability Negotiation

draft-yan-dmm-man-00

Abstract

Based on IPv6, multiple mobility management protocols have been developed and generally they can be classified into two types: network-based and host-based. Different protocols have different functional requirements on the network element or the terminal and then a scheme should be used in order to support the negotiation and selection of adopted mobility management protocol when a terminal accesses to a new network. In this draft, this issue is considered and analyzed.

Status of This Memo

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

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

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

This Internet-Draft will expire on June 24, 2017.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect...
to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction .................................................. 2
2. Motivation .................................................. 3
3. Scenarios .................................................. 3
4. Possible solutions .......................................... 4
5. Security Considerations ...................................... 5
6. IANA Considerations .......................................... 5
7. References .................................................. 5
Authors’ Addresses .............................................. 6

1. Introduction

As the Mobile IPv6 (MIPv6) [RFC6275] protocol standardization suite, there are multiple extension protocols have been standardized. These protocols can be classified into two types: protocols for the function extension and protocols for the performance enhancement. The protocols for the function extension is proposed to support some specific scenarios or functions, such as: Dual-stack Mobile IPv6 (DSMIPv6) [RFC5555] for mobility of the dual-stack nodes, Multiple Care-of-address (MCoA) [RFC5648] for mobile nodes of multi-interface and Network Mobility (NEMO) [RFC3963] for mobility of sub-network. The other type is proposed to enhance the performance of the mobility management, such as Fast Mobile IPv6 (FMIPv6) [RFC5268] for fast handover, Hierarchical Mobile IPv6 (HMIPv6) [RFC5380] for hierarchical mobility optimization. MIPv6 and these extensions are called host-based mobility management protocols because the location update is initiated by the terminal and the tunnel is terminated at the terminal.

In order to reduce the protocol cost and enhance the handover performance further, the network-based mobility management schemes were proposed and Proxy Mobile IPv6 (PMIPv6) [RFC5213] was standardized as a basis. Based on PMIPv6, a series of its extensions were proposed, such as Dual-stack Proxy Mobile IPv6 (DS-PMIPv6) [RFC5844], Distributed Mobility Management Proxy Mobile IPv6 (DMM-PMIPv6) [RFC7333] and so on. Be different from the host-based schemes, the location update in PMIPv6 is triggered by the network entity and the tunnel is established between network entities. And the terminal needs to do nothing about the signaling exchange during the movement, particularly, the mobility is transparent to the IP layer of the terminal.
In reality, these protocols will be co-existing and multiple protocol daemons will be configured on the network entities or terminal. That means a scheme is needed to support the negotiation and selection of mobility management protocol when the terminal accesses into a new network initially or handover happens.

This document tries to analyze this problem with the possible scenarios should be supported by the further solution.

2. Motivation

As illustrated above, these protocols may co-exist in reality and simultaneously used in an access network or even the same entity. Due to their different requirements on the network entity or terminal, a scheme is needed to support the negotiation and selection of adopted mobility management protocol when the terminal accesses to a new network.

Generally, two problems should be solved:

- Which entity (network or terminal) will initiate the protocol negotiation and selection?
- What principles should be followed for the protocol negotiation and selection?

This scheme is needed because different entity and terminal will have different abilities and preferences (may be decided by the ability and mobility pattern of the mobile node). This scheme can guarantee that the optimum and most suitable protocol will be used.

3. Scenarios

In order to illustrate the necessity of the mobility ability negotiation and protocol selection, the following scenarios are taken as typical examples:

1) Network supports MIPv6, host supports only PMIPv6

In this case, the network supports only host-based scheme, while the host does not have any mobility management function. Then only the PMIPv6 can be used to support the mobility management of the host, but the network does not deploy the PMIPv6 protocols and this will cause the mobility failure because no available protocol can be used.

2) Network supports both MIPv6 and PMIPv6, host supports only PMIPv6

In this case, the network deploys both host-based and network-based schemes, while the host supports only PMIPv6. When the host accesses
to the network, PMIPv6 will be used. Actually, PMIPv6 should be adopted as a default mobility management scheme considering its optimized performance. Once the PMIPv6 can be supported by the network, it will be adopted as the default scheme.

3) Network supports both MIPv6 and PMIPv6, host supports MIPv6

In this case, the network deploys both host-based and network-based schemes, and the host also supports MIPv6. Because PMIPv6 has no requirement on the host, both PMIPv6 and MIPv6 can be used in this case. Then the host can use PMIPv6 as default, and use MIPv6 for the global mobility.

4) Network and host support all the extention protocols

In this case, the network has deployed multiple extensions to support more complex requirements, so does the host. And then the host and network can negotiate a protocol for the optimized performance or special requirement, for example, FMIPv6 may be selected in order to support fast handover, HMIPv6 may be selected in order to reduce the signaling cost, NEMO may be selected in order to support the subnet mobility.

4. Possible solutions

Two different schemes may be used for the protocol negotiation and selection: MN-initiated and Network-initiated. Within the MIP/PMIP protocols, the priority of the function-extension protocols should be higher than the performance-enhancement protocols. Generally, the following principles and general procedure may be followed:

- During initiation, PMIPv6 may be used as a default mobility management protocol once the network supports it.
- If the host prefers host-based scheme, a negotiation is executed to handover from PMIPv6 to MIPv6 style.
- After initial attachment, a profile will be generated in the management store to record the selected protocol of this host.
- When the handover happens, the network will check the selected protocol during the authentication process. But the network also needs to notify the host if the selected protocol cannot be supported herein.

In order to fulfill the above principles, some extensions should be supported, for example:

1) Extended negotiation messages
In order to negotiate the mobility management protocol between host and network, a new signaling message or an extended message (e.g., ICMPv6, Diameter, and RADIUS) should be used. Except these, some other protocols may also be used in some specified scenarios, such as extended IEEE 802.21 primitives.

2) Extended management store

When the terminal accesses to the network, an authentication should be executed before the mobility management service is provided. In order to support the mobility management protocol selection, a new information should be recorded by the network after the successful authentication during the initial attachment. The newly introduced information shows the selected mobility management protocol and should be updated when the used protocol changes.

5. Security Considerations

Generally, this function will not incur additional security issues. The detailed influence should be analyzed in the future.

6. IANA Considerations

A new ICMP option or authentication option or other signaling message may be used with a new code number.

7. References


Authors’ Addresses

Zhiwei Yan
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing  100190
China
Email: yan@cnnic.cn

Jong-Hyouk Lee
Sangmyung University
31, Sangmyeongdae-gil, Dongnam-gu
Cheonan
Republic of Korea
Email: jonghyouk@smu.ac.kr