DMM Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 2, 2018

Z. Yan
G. Geng
CNNIC
J. Lee
Sangmyung University
H. Chan
Huawei Technologies
October 29, 2017

Mobility Capability Negotiation and Protocol Selection
draft-yan-dmm-man-02

Abstract

The draft analyzes the issue that multiple mobility management protocols have been developed according to different requirements. These different protocols have different functional requirements on the network element or the host. A scheme is then proposed to support the negotiation and selection of adopted mobility management protocol when a host accesses a new network.

Status of This Memo

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

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

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

This Internet-Draft will expire on May 2, 2018.

Table of Contents

1. Introduction

A large number of multiple protocols have been developed. In order to clearly analyze the possible cases, these mobility management protocols can be categorized as follows:

- Mobile IPv6 (MIPv6) protocol: the mobility management scheme based on [RFC6275].
- Proxy Mobile IPv6 (PMIPv6) protocol: the mobility management scheme based on [RFC5213].
- MIPv6 suite protocols: based on MIPv6, there are multiple extension protocols have been standardized. These protocols can be classified into two types: protocols for functional extension and protocols for performance enhancement. The protocols for functional extension are 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 hosts with multiple access interfaces and Network Mobility (NEMO) [RFC3963] for mobility of sub-network. The other type is proposed to enhance performance of the mobility management, such as Fast Mobile IPv6 (FMIP6) [RFC5268] for fast handover, Hierarchical Mobile IPv6 (HMIPv6) [RFC5380] for hierarchical mobility optimization. In the MIPv6 suite protocols, location update is initiated by the host and the tunnel is also terminated at the host.
- PMIPv6 suite protocols: in order to reduce the protocol cost and enhance the handover performance further, the network-based mobility management protocols were proposed and PMIPv6 was

standardized as a base protocol. Based on PMIPv6, a series of its extensions were proposed, such as Dual-stack Proxy Mobile IPv6 (DS-PMIPv6) [RFC5844], and Distributed Mobility Management Proxy Mobile IPv6 (DMM-PMIPv6) [RFC7333]. Being different from the MIPv6 suite protocols, the location update in PMIPv6 suite protocols is triggered by the network entity and the tunnel is established between network entities. Then the host needs to do nothing about signaling exchange during the movement, particularly, the mobility support is transparent to the IP layer of the host.

- Network-based protocols: generally, they refer to the mobility management protocols which do not require the involvement of the host to support mobility. They include the PMIPv6 suite protocols and other network-based solutions, such as GPRS Tunnelling Protocol (GTP) [TS.29274][TS.29281].
- Host-based protocols: generally, they refer to the mobility management protocols which require the involvement of the host in order to support mobility. They include the MIPv6 suite protocols and other host-based solutions, such as Host Identity Protocol (HIP) [RFC7401] and IKEv2 Mobility and Multihoming Protocol (MOBIKE) [RFC4555].

Figure 1 illustrates the scopes of the above different categories.

Figure 1: Scopes of different protocol categories

In deployment, the host-based protocols and network-based protocols will be co-existing and multiple protocol deamons will be configured on the network entities or host. There is then a gap in how to determine which protocol to use. A scheme is therefore needed to support the negotiation and selection of mobility management protocol when the host initially attaches or hands over to a new network [Paper-CombiningMobilityStandards].

This document tries to present the principles for the protocol selection and analyze the possible scenarios which should be supported by the subsequent mobility solution.

2. Motivations

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

- What principles should be followed for the protocol negotiation and selection?
- What procedure should be adopted for the protocol negotiation and selection?

This scheme is needed because the network entity and the host may have different capabilities and preferences (may be decided by the capability and mobility pattern of the host). This scheme aims to guarantee that the optimum and most suitable protocol will be used.

3. Possible Cases

From both host and network aspects, there are multiple cases in their capacities of mobility management as shown in Figure 2. We mainly analyze the cases where that host and network support a single protocol. If multiple protocols are supported simultaneously by the host or network side, multiple cases exist at the same time but the logic is the same as that in the case with single protocol supported. Specifically, the following cases should be considered.

1) Network supports network-based protocol, host supports network-based protocol

In this case, there are the following sub-cases:

a) Host supports PMIPv6 suite protocol, Network supports PMIPv6 suite protocol

- if host supports PMIPv6 and network supports PMIPv6, PMIPv6 will be selected.
- if host supports PMIPv6 and network supports extended PMIPv6 protocol, extended PMIPv6 is selected if no host involvement is needed, otherwise the plain PMIPv6 is selected (we assume that the extension protocols are backward-compatible with the related plain protocol).
- if host supports extended PMIPv6 protocol and network supports PMIPv6, PMIPv6 is selected (we assume that the extension protocols are backward-compatible with the related plain protocol).

o if host supports extended PMIPv6 protocol and network supports extended PMIPv6 protocol, the identical extension protocol is selected, otherwise, the plain PMIPv6 is selected (we assume that the extension protocols are backward-compatible with the related plain protocol).

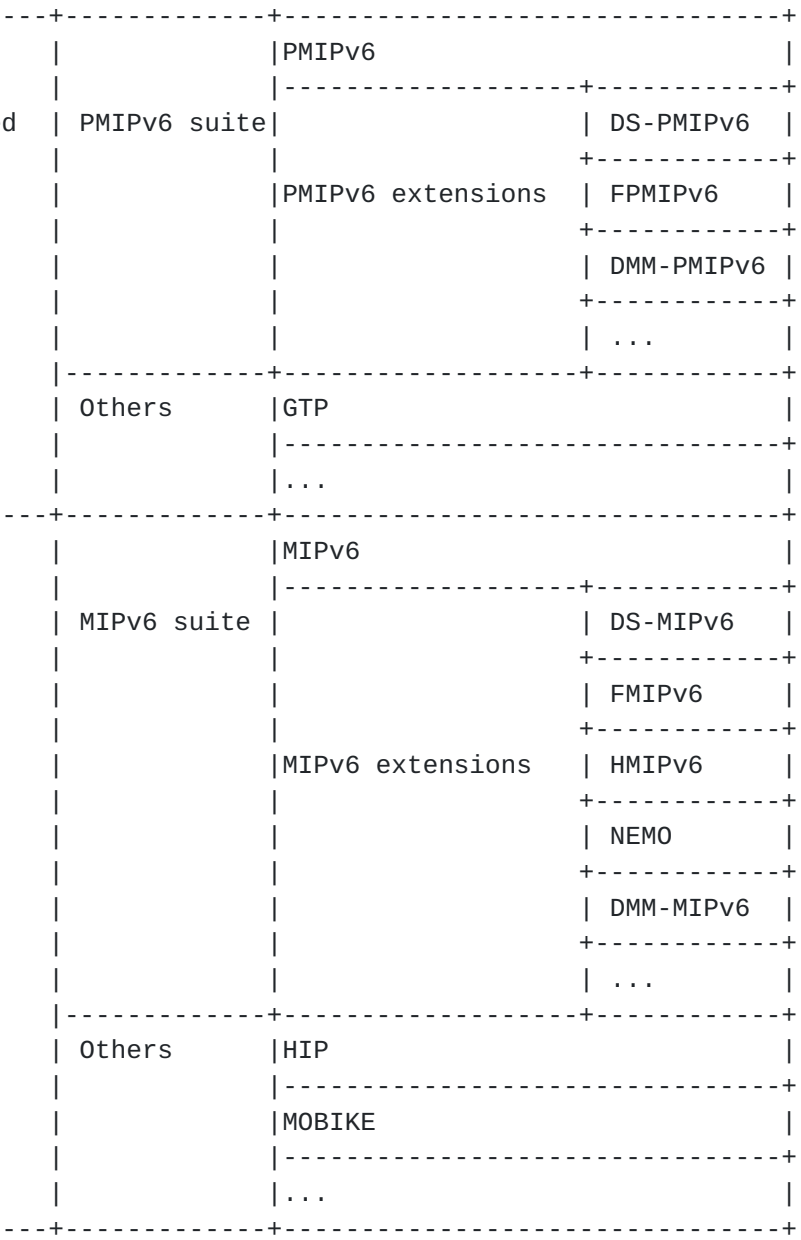

Figure 2: Possible capacities of mobility support by the host and network

b) Host supports PMIPv6 suite protocol, Network supports other network-based protocol

- o if host supports PMIPv6 and network supports other network-based protocol, other network-based protocol is selected if no host involvement is needed, otherwise failure.
- o if host supports extended PMIPv6 protocol and network supports other network-based protocol, other network-based protocol is selected if no host involvement is needed, otherwise failure.

c) Host supports other network-based protocol, Network supports PMIPv6 suite protocol

- o if host supports other network-based protocol and network supports PMIPv6, PMIPv6 is selected.
- o if host supports other network-based protocol and network supports extended PMIPv6 protocol, extended PMIPv6 protocol is selected if no host involvement is needed, otherwise failure.

d) Host supports other network-based protocol, Network supports other network-based protocol

- o the identical protocol is selected, otherwise follow network ability if the protocols are different.

2) Network supports network-based protocol, host supports host-based protocol

In this case, there are the following sub-cases:

a) Host supports PMIPv6 suite protocol, Network supports MIPv6 suite protocol

- o if host supports PMIPv6 and network supports MIPv6, failure.
- o if host supports PMIPv6 and network supports extended MIPv6 protocol, failure.
- o if host supports extended PMIPv6 protocol and network supports MIPv6, failure.
- o if host supports extended PMIPv6 protocol and network supports extended MIPv6 protocols, failure.

b) Host supports PMIPv6 suite protocol, Network supports other host-based protocol

- o if host supports PMIPv6 and network supports other host-based protocol, failure.
- o if host supports extended PMIPv6 protocol and network supports other host-based protocol, failure.

c) Host supports other network-based protocol, Network supports MIPv6 suite protocol

- o if host supports other network-based protocol and network supports MIPv6, failure.
- o if host supports other network-based protocol and network supports extended MIPv6 protocol, failure.

d) Host supports other network-based protocol, Network supports other host-based protocol

- o failure.

3) Network supports host-based protocol, host supports network-based protocol

In this case, there are the following sub-cases:

a) Host supports MIPv6 suite protocol, Network supports PMIPv6 suite protocol

- o if host supports MIPv6 and network supports PMIPv6, PMIPv6 is selected in default and MIPv6 is selected if host prefers it.
- o if host supports MIPv6 and network supports extended PMIPv6 protocol, extended PMIPv6 is selected in default, then PMIPv6 is selected with the lower priority and MIPv6 is selected if host prefers it.
- o if host supports extended MIPv6 protocol and network supports PMIPv6, PMIPv6 will be selected in default, then extended MIPv6 is selected if host prefers it and network also supports, otherwise MIPv6 is selected with the lowest priority.
- o if host supports extended MIPv6 protocol and network supports extended PMIPv6 protocol, extended PMIPv6 is selected in default, then PMIPv6 is selected, then extended MIPv6 is selected if host prefers and network also supports, otherwise MIPv6 is selected with the lowest priority.

b) Host supports MIPv6 suite protocol, Network supports other network-based protocol

- o if host supports MIPv6 and network supports other network-based protocol, other network-based protocol is selected if no host involvement is needed, otherwise failure.
- o if host supports extended MIPv6 protocol and network supports other network-based protocol, other network-based protocol is selected if no host involvement is needed, otherwise failure.

c) Host supports other host-based protocol, Network supports PMIPv6 suite protocol

- o if host supports other host-based protocol and network supports PMIPv6, PMIPv6 is selected in default, otherwise failure.
- o if host supports other host-based protocol and network supports extended PMIPv6 protocol, extended PMIPv6 protocol is selected if no host involvement is needed, otherwise failure.

d) Host supports other host-based protocol, Network supports other network-based protocol

- o other network-based protocol is selected if no host involvement is needed, otherwise failure.

4) Network supports host-based protocol, host supports host-based protocol

In this case, there are the following sub-cases:

a) Host supports MIPv6 suite protocol, Network supports MIPv6 suite protocol

- o if host supports MIPv6 and network supports MIPv6, MIPv6 is selected.
- o if host supports MIPv6 and network supports extended MIPv6 protocol, MIPv6 is selected.
- o if host supports extended MIPv6 protocol and network supports MIPv6, MIPv6 is selected.
- o if host supports extended MIPv6 protocol and network supports extended MIPv6 protocols, the identical protocol is selected, otherwise MIPv6 is selected.

b) Host supports MIPv6 suite protocol, Network supports other host-based protocol

- o if host supports MIPv6 and network supports other host-based protocol, failure.
- o if host supports extended MIPv6 protocol and network supports other host-based protocol, failure.

c) Host supports other host-based protocol, Network supports MIPv6 suite protocol

- o if host supports other host-based protocol and network supports MIPv6, failure.
- o if host supports other host-based protocol and network supports extended MIPv6 protocol, failure.

d) Host supports other host-based protocol, Network supports other host-based protocol

- the identical other host-based protocol is selected, otherwise failure.

5) Network supports host-based protocol and network-based protocol, host supports host-based protocol and network-based protocol

- follow the network based protocol in default if the host can support, otherwise select the protocol both network and host can support if host prefers.

4. Principles and Possible Procedure

Two different schemes may be used for the protocol negotiation and selection: host-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 should be followed:

- Priority 1: Follow network ability
- Priority 2: Follow host preference
- Priority 3: Support the functional extensions
- Priority 4: Support the performance enhancements
- In default: network based scheme if it can be supported

And the general procedure for the protocol selection should be:

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

5. Extensions

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

1) Extended negotiation messages

The protocol negotiation may be included in the MN_ATTACH Function [MN-AR.IF] and the implementation may be based on a new signaling

message or extended messages (e.g., ICMPv6, Diameter, and RADIUS). Besides 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 host accesses the network, 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.

6. Security Considerations

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

7. IANA Considerations

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

8. References

8.1. Normative References

[MN-AR.IF] Laganier, J., Narayanan, S., and P. McCann, "Interface between a Proxy MIPv6 Mobility Access Gateway and a Mobile Node", draft-ietf-netlmm-mn-ar-if-03, February 2008.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, DOI 10.17487/RFC3963, January 2005, <https://www.rfc-editor.org/info/rfc3963>.

[RFC4555] Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", RFC 4555, DOI 10.17487/RFC4555, June 2006, <https://www.rfc-editor.org/info/rfc4555>.

[RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <https://www.rfc-editor.org/info/rfc5213>.

[RFC5268] Koodli, R., Ed., "Mobile IPv6 Fast Handovers", RFC 5268, DOI 10.17487/RFC5268, June 2008, <https://www.rfc-editor.org/info/rfc5268>.

[RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, DOI 10.17487/RFC5380, October 2008, <https://www.rfc-editor.org/info/rfc5380>.

[RFC5555] Soliman, H., Ed., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, DOI 10.17487/RFC5555, June 2009, <https://www.rfc-editor.org/info/rfc5555>.

[RFC5648] Wakikawa, R., Ed., Devarapalli, V., Tsirtsis, G., Ernst, T., and K. Nagami, "Multiple Care-of Addresses Registration", RFC 5648, DOI 10.17487/RFC5648, October 2009, <https://www.rfc-editor.org/info/rfc5648>.

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, DOI 10.17487/RFC5844, May 2010, <https://www.rfc-editor.org/info/rfc5844>.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <https://www.rfc-editor.org/info/rfc6275>.

[RFC7333] Chan, H., Ed., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, DOI 10.17487/RFC7333, August 2014, <https://www.rfc-editor.org/info/rfc7333>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <https://www.rfc-editor.org/info/rfc7401>.

[TS.29274] "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3", 3GPP TS 29.274 8.10.0, June 2011.

[TS.29281] "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)", 3GPP TS 29.281 10.3.0, September 2011.

8.2. Informative References

[Paper-CombiningMobilityStandards]
Oliva, A., Soto, I., Calderon, M., Bernardos, C., and M. Sanchez, "The costs and benefits of combining different IP mobility standards", Computer Standards and Interfaces, February 2013.

Authors' Addresses

Zhiwei Yan
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing 100190
China

Email: yan@cnnic.cn

Guanggang Geng
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing 100190
China

Email: ggg@cnnic.cn

Jong-Hyouk Lee
Sangmyung University
31, Sangmyeongdae-gil, Dongnam-gu
Cheonan
Republic of Korea

Email: jonghyouk@smu.ac.kr

H. Anthony Chan
Huawei Technologies
5340 Legacy Dr. Building 3
Plano, TX 75024
USA

Email: h.a.chan@ieee.org