DMM Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 14, 2017

Z. Yan
CNNIC
J. Lee
Sangmyung University
X. Lee
CNNIC

March 13, 2017

# Home Network Prefix Renumbering in PMIPv6
# draft-ietf-dmm-hnprenum-07

Abstract

In the basic Proxy Mobile IPv6 (PMIPv6) specification, a Mobile Node (MN) is assigned with a Home Network Prefix (HNP) during its initial attachment and the MN configures its Home Address (HoA) with the HNP. During the movement of the MN, the HNP remains unchanged to keep ongoing communications associated with the HoA. However, the current PMIPv6 specification does not specify related operations when an HNP renumbering has happened (e.g. due to change of service provider, change of site topology, etc.). In this document, a solution to support the HNP renumbering is proposed, as an optional extension of the PMIPv6 specification.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL","SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]

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 September 14, 2017.

Table of Contents



## 1. Introduction

Network managers currently prefer Provider Independent (PI) addressing for IPv6 to attempt to minimize the need for future possible renumbering. However, a widespread use of PI addresses will cause Border Gateway Protocol (BGP) scaling problems [RFC7010]. It is thus desirable to develop tools and practices that make IPv6 renumbering a simpler process to reduce demand for IPv6 PI space [RFC6879]. In this document, we aim to solve the HNP renumbering problem when the HNP in PMIPv6 [RFC5213] is a PI prefix.

## 2. Usage Scenarios

There are a number of reasons why the HNP renumbering support in PMIPv6 is useful and some scenarios are identified below:

- Scenario 1: the HNP set used by a PMIPv6 service provider is assigned by a different Internet Service Provider (ISP), and then

the HNP renumbering MAY happen if the PMIPv6 service provider switches to a different ISP.

- Scenario 2: multiple Local Mobility Anchors (LMAs) MAY be deployed by the same PMIPv6 service provider, and then each LMA MAY serve for a specific HNP set. In this case, the HNP of an MN MAY change if the current serving LMA switches to another LMA but without inheriting the assigned HNP set [RFC6463].

- Scenario 3: the PMIPv6 HNP renumbering MAY be caused by the re-building of the network architecture as the companies split, merge, grow, relocate, or reorganize. For example, the PMIPv6 service provider MAY reorganize its network topology.

In the scenario 1, we assume that only the HNP is renumbered while the serving LMA remains unchanged and this is the basic scenario considered in this document. In the scenario 2 and scenario 3, more complex results MAY be caused, for example, the HNP renumbering MAY happen due to the switchover of a serving LMA.

In the Mobile IPv6 (MIPv6) protocol, when a home network prefix changes, the Home Agent (HA) will actively notify the new prefix to its MN and then the renumbering of the Home Network Address (HoA) can be well supported [RFC6275]. In the basic PMIPv6, the PMIPv6 binding is triggered by a Mobile Access Gateway (MAG), which detects the attachment of the MN. A scheme is also needed for the LMA to immediately initiate the PMIPv6 binding state refreshment during the HNP renumbering process. Although this issue is also mentioned in Section 6.12 of [RFC5213], the related solution has not been specified.

## 3. HNP Renumbering Procedure

When the HNP renumbering happens in PMIPv6, the LMA MUST notify a new HNP to the MAG and then the MAG MUST announce the new HNP to the attached MN accordingly. Also, the LMA and the MAG MUST update the routing states for the HNP and the related addresses. To support this procedure, [RFC7077] can be adopted which specifies an asynchronous update from the LMA to the MAG about specific session parameters. This document considers the following two cases:

(1) HNP is renumbered under the same LMA

In this case, the LMA remains unchanged as in the scenario 1 and scenario 3. The operation steps are shown in Figure 1.

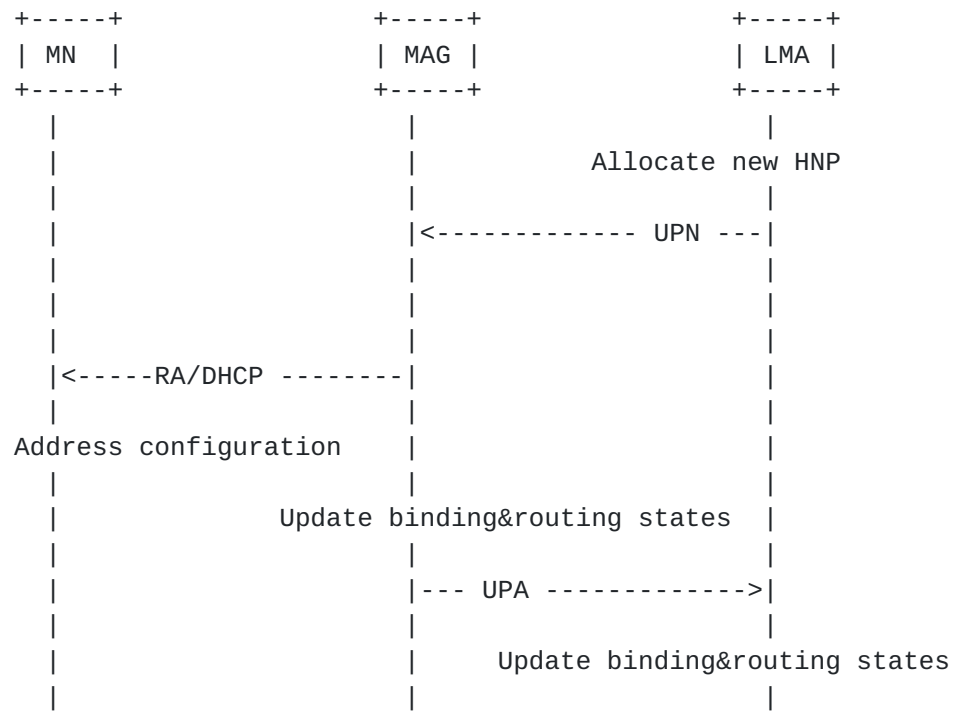


Figure 1: Signaling call flow of the HNP renumbering

- When a PMIPv6 service provider renumbers the HNP set under the same LMA, the serving LMA SHOULD initiate the HNP renumbering operation. The LMA allocates a new HNP for the related MN.

- The LMA sends the Update Notification (UPN) message to the MAG to update the HNP information. If the Dynamic Host Configuration Protocol (DHCP) is used to allocate the address, the new HNP MUST be also notified to the DHCP infrastructure.

- Once the MAG receives this UPN message, it recognizes that the related MN has the new HNP. Then the MAG MUST notify the MN about the new HNP with a Router Advertisement (RA) message or allocate a new address within the new HNP through a DHCP procedure.

- After the MN obtains the HNP information through the RA message, it deletes the old HoA and configures a new HoA with the newly allocated HNP.

- When the new HNP is announced or the new address is configured to the MN successfully, the MAG MUST update the related binding and routing states. Then the MAG sends back the Update Notification Acknowledgement (UPA) message to the LMA for the notification of successful update of the HNP, related binding state, and routing state. Then the LMA updates the routing and binding information corresponding to the MN to replace the old HNP with the new one.

(2) HNP renumbering caused by the LMA switchover

Since the HNP is assigned by the LMA, the HNP renumbering MAY be caused by the LMA switchover, as in the scenario 2 and scenario 3.

The information of LMA is the basic configuration information of MAG. When the LMA changes, the related profile SHOULD be updated by the service provider. In this way, the MAG initiates the registration to the new LMA as specified in [RFC5213]. When the HNP renumbering is caused in this case, the new HNP information is sent by the LMA during the new binding procedure. Accordingly, the MAG withdraws the old HNP of the MN and announces the new HNP to the MN as like the case of the HNP is renumbered under the same LMA.

## 4. Session Connectivity

The HNP renumbering may cause the disconnection of the ongoing communications of the MN. Basically, there are two modes to manage the session connectivity during the HNP renumbering.

(1) Soft-mode

The LMA will temporarily maintain the state of the old HNP during the HNP renumbering (after the UPA reception) in order to redirect the packets to the MN before the MN reconnects the ongoing session and notifies its new HoA to the Correspondent Node (CN). This mode is aiming to reduce the packet loss during the HNP renumbering but the binding state corresponding to the old HNP should be marked for example as transient binding [RFC6058]. And the LMA MUST stop broadcasting the routing information about the old HNP if the old HNP is no longer anchored at this LMA.

(2) Hard-mode

If the HNP renumbering happens with the switchover of the LMA, the hard-mode is recommended to keep the protocol simple. In this mode, the LMA deletes the binding state of the old HNP after it receives the UPA message from the MAG and the LMA silently discards the packets destined to the old HNP.

## 5. Message Format

(1) UPN message

In the UPN message sent from the LMA to the MAG, the notification reason is set to 2 (UPDATE-SESSION-PARAMETERS). Besides, the HNP Option [RFC5213] containing the new HNP and the Mobile Node Identifier Option [RFC4283] carrying identifier of MN are contained

as Mobility Options of UPN. The order of HNP Option and Mobile Node Identifier Option in the UPN message is not mandated here.

(2) UPA message

The MAG sends this message in order to acknowledge that it has received an UPN message with the (A) flag set and to indicate the status after processing the message. When the MAG did not successfully renumber the HNP which is required in the UPN message, the Status Code of 128 is set in the UPA message and the following operation of LMA is PMIPv6 service provider specific.

(3) RA Message

When the RA message is used by the MAG to advise the new HNP, two Prefix Information Options are contained in the RA message [RFC4861] [RFC4862]. In the first Prefix Information Option, the old HNP is carried and the related Preferred Lifetime is set to 0. In the second Prefix Information Option, the new HNP is carried with the Valid Lifetime and Preferred Lifetime set to larger than 0.

(4) DHCP Message

When the DHCP is used in PMIPv6 to configure the addresses for the MN, new IPv6 address(es) (e.g., HoA) will be generated based on the new HNP and the related DHCP procedure is also triggered by the reception of UPN message [RFC3315].

## 6. Other Issues

In order to maintain the reachability of the MN, the Domain Name System (DNS) resource record corresponding to this MN may need to be updated when the HNP of MN changes [RFC3007]. However, this is beyond the scope of this document.

## 7. Security Considerations

This document causes no further security problem for the signaling exchanges. The UPN and UPA messages in this document MUST be protected using end-to-end security association(s) offering integrity and data origin authentication as speficied in [RFC5213] and [RFC7077].

When the HNP renumbering is triggered, a new HNP SHOULD be allocated to the MN. The LMA MUST follow the procedure of PMIPv6 to make sure that only an authorized HNP can be assigned for the MN. In this way, LMA is ready to be the topological anchor point of the new HNP and the new HNP is for that MN's exclusive use.

[RFC4862] requires an RA to be authenticated for the Valid Lifetime in a Prefix Information Option to be set to less than 2 hours. Thus, when the old HNP that is being deprecated is included in an RA from the MAG, it will normally be expected that the Valid Lifetime SHOULD be set to 2 hours (and the Preferred Lifetime set to 0) for a non-authenticated RA. However, if the legality of the signaling messages exchanged between MAG and MN can be guaranteed, it MAY be acceptable to also set the Valid Lifetime to 0 for a non-authenticated RA.

## 8. IANA Considerations

This document presents no IANA considerations.

## 9. References

### 9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3007] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, DOI 10.17487/RFC3007, November 2000, <http://www.rfc-editor.org/info/rfc3007>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <http://www.rfc-editor.org/info/rfc3315>.

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, DOI 10.17487/RFC4283, November 2005, <http://www.rfc-editor.org/info/rfc4283>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <http://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <http://www.rfc-editor.org/info/rfc4862>.

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

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

[RFC6463] Korhonen, J., Ed., Gundavelli, S., Yokota, H., and X. Cui, "Runtime Local Mobility Anchor (LMA) Assignment Support for Proxy Mobile IPv6", RFC 6463, DOI 10.17487/RFC6463, February 2012, <http://www.rfc-editor.org/info/rfc6463>.

[RFC7077] Krishnan, S., Gundavelli, S., Liebsch, M., Yokota, H., and J. Korhonen, "Update Notifications for Proxy Mobile IPv6", RFC 7077, DOI 10.17487/RFC7077, November 2013, <http://www.rfc-editor.org/info/rfc7077>.

## 9.2. Informative References

[RFC6058] Liebsch, M., Ed., Muhanna, A., and O. Blume, "Transient Binding for Proxy Mobile IPv6", RFC 6058, DOI 10.17487/RFC6058, March 2011, <http://www.rfc-editor.org/info/rfc6058>.

[RFC6879] Jiang, S., Liu, B., and B. Carpenter, "IPv6 Enterprise Network Renumbering Scenarios, Considerations, and Methods", RFC 6879, DOI 10.17487/RFC6879, February 2013, <http://www.rfc-editor.org/info/rfc6879>.

[RFC7010] Liu, B., Jiang, S., Carpenter, B., Venaas, S., and W. George, "IPv6 Site Renumbering Gap Analysis", RFC 7010, DOI 10.17487/RFC7010, September 2013, <http://www.rfc-editor.org/info/rfc7010>.

## 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 31066
Republic of Korea

EMail: jonghyouk@smu.ac.kr

Xiaodong Lee
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing 100190
China

EMail: xl@cnnic.cn