DMM Working Group
Internet Draft
Expires: July 2015

Zhiwei Yan
CNNIC
Jong-Hyouk Lee
Sangmyung University
Xiaodong Lee
CNNIC

January 9, 2015

# Home Network Prefix Renumbering in PMIPv6
# draft-yan-dmm-hnprenum-00.txt

## Abstract

In the basic Proxy Mobile IPv6 (PMIPv6) specification, a Mobile Node (MN) is assigned a 64-bit Home Network Prefix (HNP) during the initial attachment for the Home Address (HoA) configuration. During the movement of the MN, this prefix is unchanged and unnecessary for the MN to reconfigure the HoA. However, the current protocol does not specify related operations to support the MN to timely receive and configure a new HNP when the allocated HNP changes. In this draft, this problem is discussed and a possible solution is proposed based on RFC 7077.

## 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 to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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".

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html

This Internet-Draft will expire on July, 2015.

Copyright Notice



Table of Contents



## 1. Introduction

Network managers currently prefer to Provider Independent (PI) addressing for IPv6 to attempt to minimize the need for future renumbering. However, widespread use of PI may create very serious BGP scaling problems. It is thus desirable to develop tools and practices that may make renumbering a simpler process to reduce demand for IPv6 PI space [1]. In this draft, we aims to solve the HNP renumbering problem when the HNP in PMIPv6 [2] is not a PI type.

Then the HNP renumbering may happen at least in the following three cases:

In the first case, the PMIPv6 service provider is assigned the HNP set from the (uplink) ISP, and then the HNP renumbering will happen if the PMIPv6 service provider switches to a different ISP.

In the second case, 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 a MN may change if the current serving LMA switches to another LMA but without inheriting the assigned HNP [3].

In the last case, 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.

For the Mobile IPv6 (MIPv6), when the home network prefix changes (maybe due to the above reasons), the Home Agent (HA) will actively notify the new prefix to the MN and then the renumbering of the HoA can be well supported [4]. While in the basic PMIPv6, the PMIPv6 binding is triggered by the Mobile Access Gateway (MAG), which detects the attachment of the MN. When the HNP renumbering happens in the first case or the LMA and HNP both changes in the second or third cases, a scheme is needed for the LMA to immediately initiate the PMIPv6 binding state refreshment. Although this issue is also discussed in the RFC 5213 (section 6.12), the related solution is not specified.

## 2. HNP renumbering support

RFC 7077 [5] specifies a scheme to support the asynchronously update from the LMA to the MAG about changes related to a mobility session. With this protocol, the HNP renumbering can be easily supported and the basic operation is summarized as following:

1) When the PMIPv6 service provider renumbers the HNP set or the serving LMA switches to another one but does not inherit the related HNP, the current LMA (or new LMA) will initiate the HNP renumbering operation. Firstly, it should allocate a new HNP for the related MN.

2) The LMA sends the Update Notification (UPN) message to the MAG. In the UPN message, the Notification reason is set to 2 (UPDATE-SESSION-PARAMETERS). Besides, HNP option containing the new HNP and the Mobile Node Identifier option carrying MN'ID are contained as Mobility Options of UPN.

3) After the MAG receives this UPN message, it will recognize that the related MN has a new HNP now. Then the MAG sends the old HNP in the RA with zero-valued lifetime to the MN and sends the new HNP in the RA with lifetime larger than zero.

4) Besides, the MAG sends back the Update Notification Acknowledgement (UNA) to the LMA for the notification of successful update of the related binding state, routing state and RA settings.

5) For the MN, it deletes the old HoA due to the zero-valued lifetime RA advertisement and configures a new HoA with the meaningful HNP.

The detailed protocol operation and signaling message extensions will be specified further.

## 3. DNS update

In order to maintain the reachability of the MN, the DNS resource record corresponding to this MN may need to be updated when the HNP of MN changes. Although this operation in PMIPv6 has not been specified by the current protocols, we here list two important issues to be considered for this operation.

1) Since the DNS update must be performed securely in order to prevent attacks or modifications from malicious ones, the node performing this update must share a security association with the DNS server [6]. If the MN does not share a security association with the DNS server and the DNS entry update can be performed by the network entities, such as Authentication, Authorization and Accounting (AAA) server or LMA.

2) For the dynamic update, another important issue should be considered is the TTL setting when the HNP renumbering is possible. The TTL should be set according to the possible lifetime of the HNP.

## 4. Security Considerations

The security considerations in PMIPv6 protocol are enough for the basic operation of this draft.

Besides, the security dynamic DNS should be supported whatever the DNS update is executed by network entities or MN itself. In other words, the security association should always be established between the DNS server and updater.

Other security issues will be added further.

## 5. References

[1] S. Jiang, B. Liu, and B. Carpenter, "IPv6 Enterprise Network Renumbering Scenarios and Guidelines", RFC 6879, February 2013.

[2] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[3] J. Korhonen, S. Gundavelli, H. Yokota, and X. Cui, "Runtime Local Mobility Anchor (LMA) Assignment Support for Proxy Mobile IPv6", RFC 6463, February 2012.

[4] C. Perkins, D. Johnson, and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[5] S. Krishnan, S. Gundavelli, M. Liebsch, H. Yokota and J. Korhonen, "Update Notifications for Proxy Mobile IPv6", RFC 7077, November 2013.

[6] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.

## Authors' Addresses

Zhiwei Yan
China Internet Network Information Center
No.4 South 4th Street, Zhongguancun
Beijing, P. R. China
Email: yan@cnnic.cn

Jong-Hyouk Lee
Department of Computer Science and Engineering
Sangmyung University
31, Sangmyeongdae-gil, Dongnam-gu
Cheonan, Republic of Korea
E-mail: jonghyouk@smu.ac.kr

Xiaodong Lee
China Internet Network Information Center
No.4 South 4th Street, Zhongguancun
Beijing, P. R. China
Email: xl@cnnic.cn

## Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.