

MIP6 Working Group
Internet-Draft
Expires: May 21, 2008

R. Wakikawa
Keio University
M. Aramoto
Sharp
P. Thubert
Cisco
November 18, 2007

Elimination of Proxy NDP from Home Agent Operations
draft-wakikawa-mip6-no-ndp-02.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of 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/lid-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 May 21, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Internet-Draft

HA Limited Proxy NDP

November 2007

Abstract

This document summarizes how to eliminate the Proxy NDP from the Home Agent's operations. Although the Proxy NDP is mainly used to intercept packets by a Home Agent on Mobile IPv6 and NEMO, it brings several limitations to the protocols.

Table of Contents

1.	Introduction	3
2.	Use Case	4
2.1.	Mobile IP6: Virtual Home Link and Performance	4
2.2.	Network Mobility: Aggregated Home Link	4
2.3.	Monami6: Simultaneous Use of Home and Foreign Link	5
3.	Home Agent Configuration	6
4.	Home Agent Operation	7
4.1.	Duplicate Address Detection	7
4.2.	Sending Router Advertisement	7
4.3.	Delivering Packets to the Mobile Node	8
4.4.	Returning Home	8
5.	IANA considerations	9
6.	Security Considerations	10
7.	References	10
7.1.	Normative reference	10
7.2.	Informative Reference	10
	Authors' Addresses	11
	Intellectual Property and Copyright Statements	12

[1.](#) Introduction

In Mobile IPv6, one of design limitations is the use of Proxy Neighbor Discovery on Home Agent. Mobile IPv6 uses the proxy Neighbor Discovery Protocol (proxy NDP) to intercept packets meant for mobile nodes on a home agent at a home link. When the proxy NDP is used, a home prefix must be strictly configured at the physical link which the home prefix is defined in the Internet topology. Moreover, the performance of NDP may effect that of Mobile IPv6 if the number of mobile nodes are served by a home network prefix.

Elimination of the Proxy NDP from Mobile IPv6 and NEMO may bring some advantages such as flexible home prefix configuration, reduction of NDP overhead, disengagement from the home link bandwidth. In NEMO Working Group, [\[1\]](#) introduces various home prefix configurations such as the aggregated home prefix, the aggregated home prefix and the virtual home prefix. Proxy NDP is useless specially when the aggregated home prefix is used. Finally, the fact that packets are captured by NDP shows that the maximum bandwidth for all the mobile nodes are limited to the home link bandwidth.

We introduce special use case for Monami6 work. When a mobile node returns home with multiple interfaces, it can only activate either an interface attached to the home link or an interface attached to a foreign link [\[9\]](#). If it tries to active both interfaces, the Home Agent and the Mobile Node will defend the Home Address by NDP simultaneously. Consequently, it leads DAD problem. This problem has been discussed on the Multiple Care-of Address Registration [\[2\]](#) in Monami6 Working Group. By eliminating Proxy NDP, the mobile node can utilize both of interfaces attached to the home and the foreign link at the same time.

This document shows the possible configuration and modification when a home agent stop the proxy NDP for Mobile IP and NEMO. The Mobile Node is transparent to this NDP elimination, though it may skip several steps from returning home operation.

Readers are expected to be familiar with all the terms defined in the [RFC3753](#) [3] and the NEMO Terminology draft [4]

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [5]

[2.](#) Use Case

[2.1.](#) Mobile IP6: Virtual Home Link and Performance

The first case is that home prefix is configured as the virtual home link on Home Agent as shown in Figure 1. The operator may choose this deployment scenario to reduce NDP overhead caused by number of Mobile Nodes at the home link.

The home link is not configured at the physical link and all of the Mobile Nodes moves only in foreign links and never come back to the home link. The Home Agent does not intercept packets from a Mobile Node and to the Mobile Node on the home link by the Proxy NDP. The Home agent is configured as an external router in order to intercept packets without the proxy NDP.

Even if the home link is configured at the physical link, the proxy NDP can be skipped. This is also useful scenario for Mobile IP operators, because the performance of packet interception is released from the limitation of the home link bandwidth. Even if the external link toward the Internet is high speed network like 10Gbps, the performance is limited to the home link bandwidth on the regular Mobile IP and NEMO. The operator needs not to invest to the home link bandwidth with our modified operation. In addition to this, plenty of Proxy NDP entries are burden to a Home Agent, if the number of Mobile Nodes are served by the Home Agent. Our proposal can remove this burden from the Home Agent.

+----=-----+ 10Gbps +----+

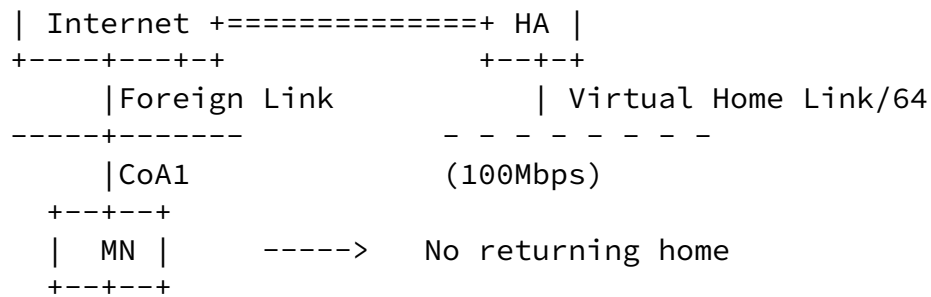


Figure 1: MIP

2.2. Network Mobility: Aggregated Home Link

The NEMO Basic Support [6] allows that a home link is configured as the aggregated home prefix. The Home Agent assigns an internal network prefix(es) to a Mobile Router as shown in Figure 2. The Home Agent cannot intercept the packets meant for the mobile network prefix by the proxy NDP, because the Proxy NDP assumes /64 prefix length on a link. This is not explicitly described in the NDP

specification, but the NDP specification implies this. It is necessary for Home Agent to intercept the packets without using Proxy NDP.

It is also useful that the Home Agent is configured as an external router of the aggregated home networks and the Home Agent intercepts packets according to the IP routing. There is no reasons to use Proxy NDP for intercepting mobile nodes' packets.

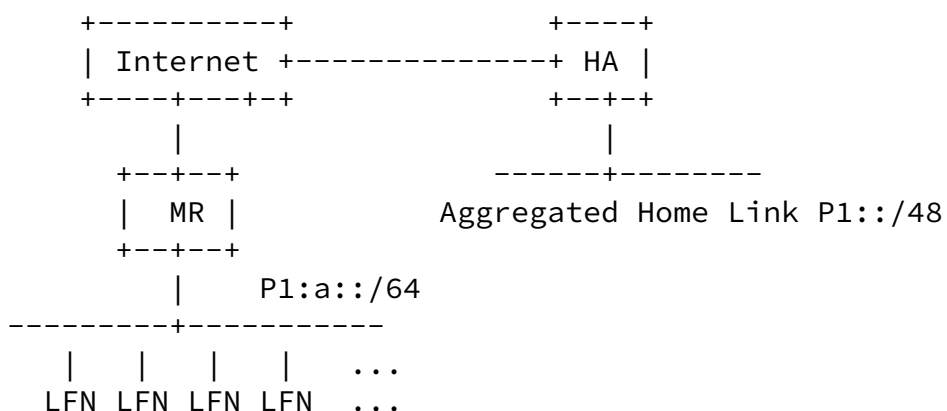


Figure 2: Aggregated Home Link

[2.3.](#) Monami6: Simultaneous Use of Home and Foreign Link

The Multiple Care-of Address Registration [2] does not allow to maintain multiple bindings that one is attached to the home link and the other is attached to the foreign link simultaneously. This restriction has been derived from the Proxy NDP operation on a Home Agent. The Home Agent needs to defend a mobile node's home address by the proxy NDP for packet interception, while the mobile node defends its home address by regular NDP to send and receive packets at the interface attached to the home link. Two nodes, Home Agent and Mobile Node, compete ND state, so that it causes address duplication problem consequently.

This document recommends not to use the Proxy NDP in order to support simultaneous use of home and foreign link. If the proxy NDP is disabled, the main problem, address duplication problem can be solved. In this Multiple Care-of Address Registration case, Mobile Node and Home Agent can maintain multiple bindings, the binding of the Mobile Node's interface is attached to the home link and the other(s) is attached to the foreign link.

[3.](#) Home Agent Configuration

In Mobile IPv6 and NEMO, two possible placements of Home Agents are possible. The difference between them is whether the Home Agent acts as an external router or not as shown in Figure Figure 3.

In this document, HA is always an external router so that it can intercept all the packets meant for mobile nodes without the proxy neighbor advertisement. The Home Agent intercepts packets according to the IP routing. All the packets toward the home prefix will be routed to the Home Agent. When the Home Agent receives packets meant for the home prefix, it then route packets based on routing information and binding cache to the target mobile node. .

+-----+

+-----+

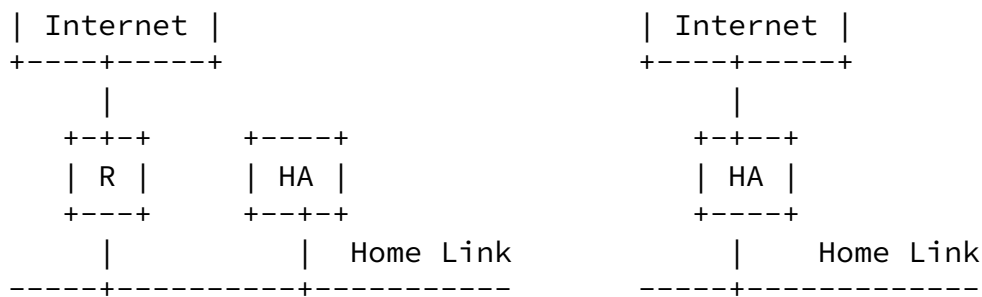


Figure 3: Home Agent Placements

Note that there is one drawback when a HA is placed as an external router. Operators cannot utilize multiple home agents for a same home prefix at a home link as introduced in [7]. For the purpose of the home agent reliability, the Home Agent Reliability protocol can be operated with the specific configuration in Figure 4. In this case, upper router can switch the routing information based on the HA survivability as shown in Figure 4

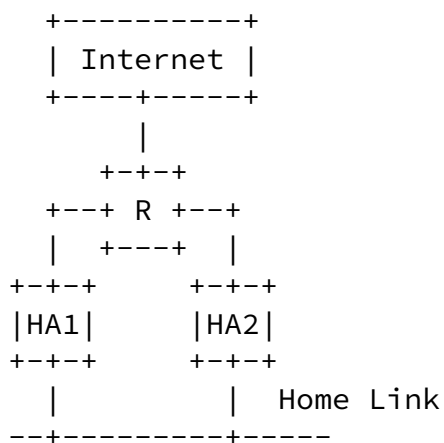


Figure 4: Multiple Home Agents Placement

4. Home Agent Operation

4.1. Duplicate Address Detection

[RFC3775](#)[7] also uses the Proxy NDP to defend a Home Address of a Mobile Node when the Mobile Node is away from the Home Link. Thus, non of other nodes can pick the Home Address at the Home Link even if the Mobile Node is not visible on the Home Link.

When the Proxy NDP is eliminated, the uniqueness of a home address should be carefully examined. If a Mobile Node is away from the Home, its home address can be picked by other Mobile Nodes on the Home Link because of no Proxy ND entry of the Home Address. To prevent address duplication, the Home Agent can filter the packets originated from the Home Link based on the Binding Cache. Since the Home Agent is an external router, all the packets are passed through the Home Agent. When the Home Agent intercepts packets from the Home Link and finds an active binding cache entry for the same address with the packet's source address, it MUST drop packets. For incoming packets, the Home Agent can prioritize the binding cache database first and can tunnel packets to the Mobile Node. The packets are never reached to the malicious node who takes the home address of other mobile nodes. As a result, although a third node (malicious node) can obtain a home address which is already taken by other Mobile Node, it cannot send and receive packets by using the home address.

4.2. Sending Router Advertisement

The Home Agent SHOULD send a Router Advertisement to the Home Link for two purposes: address assignment and home link detection. The Mobile Node generates a home address from the received router advertisement. It also uses this to detect the home link.

In this document, the Home Agent MUST route all the incoming and outgoing packets of the home link. Even for communication with a Correspondent Node located on the home link, the packets MUST be routed via the Home Agent. Otherwise, a malicious node can steal a Home Address of the other Mobile nodes and communicates with Correspondent nodes located on the Home Link by using the stolen Home Address (HoA1) as shown in Figure 5. If the packet is always routed to the Home Agent first, the packets sent by Correspondent Node will be routed correctly to the right Mobile Node.

For doing so, the Home Agent MUST generate Router Advertisement which the on-link flag (L flag) [8] is unset, so that all the packets will be routed via the Home Agent. Malicious nodes may directly route the packets with the stolen home address, but packets sent by

Correspondent Node will reach to the right Mobile Node. Moreover,

when the Home Agent receives packets which destination and source are both located on the home link, it MUST NOT generate ICMP redirect to the sender.

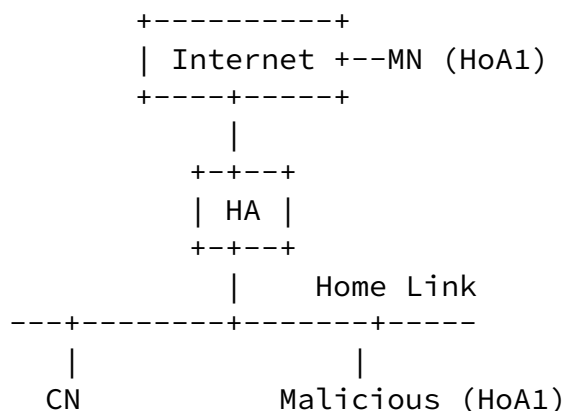


Figure 5: Malicious Node communicating with CN on the home link

4.3. Delivering Packets to the Mobile Node

Home Agent intercepts packets meant for mobile node by IP routing (See [Section 3](#) and [Section 4.2](#)). How to deliver packets is same as [7]. The Home Agent refers the Binding Cache and encapsulates packets according to the binding cache entry.

If a correspondent node is located at the home link, the node routes packets to the Home Agent first because the on-link flag of Router Advertisement is unset (See [Section 4.2](#)). The Home Agent intercepts packets and tunnels packets to the Mobile Node only when the binding cache entry for the packet's destination is available. Otherwise, it can re-send the packet back to the Home Link.

However, Home Agent MUST drop the packets by the malicious node who steal the Home Address (See [Section 4.1](#)). For incoming packets from the external network (ex.Internet), when the binding is not active, Home Agent MUST drop the packets which source address is Mobile Node itself. On the other hand, for incoming packets from the Home Link, when the binding is active, Home Agent MUST drop the packets which source address is Mobile Node itself.

4.4. Returning Home

For Returning home, no modification is given in this specification.

[5.](#) IANA considerations

This document does not require any IANA action.

Internet-Draft

HA Limited Proxy NDP

November 2007

[6.](#) Security Considerations

No security vulnerability is not introduced in this specification.

[7.](#) References

[7.1.](#) Normative reference

- [1] Thubert, P., "NEMO Home Network models", [draft-ietf-nemo-home-network-models-06](#) (work in progress), February 2006.
- [2] Wakikawa, R., "Multiple Care-of Addresses Registration", [draft-ietf-monami6-multiplecoa-00](#) (work in progress), June 2006.
- [3] Manner, J. and M. Kojo, "Mobility Related Terminology", [RFC 3753](#), June 2004.
- [4] Ernst, T. and H. Lach, "Network Mobility Support Terminology", [draft-ietf-nemo-terminology-06](#) (work in progress), November 2006.
- [5] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [6] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", [RFC 3963](#), January 2005.
- [7] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [8] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", [RFC 2461](#), December 1998.

[7.2.](#) Informative Reference

- [9] Ng, C., "Analysis of Multihoming in Network Mobility Support",

Wakikawa, et al.

Expires May 21, 2008

[Page 10]

Internet-Draft

HA Limited Proxy NDP

November 2007

Authors' Addresses

Wakikawa Ryuji
Keio University
Department of Environmental Information, Keio University.
5322 Endo
Fujisawa, Kanagawa 252-8520
Japan

Phone: +81-466-49-1100
Fax: +81-466-49-1395
Email: ryuji@sfc.wide.ad.jp
URI: <http://www.wakikawa.org/>

Aramoto Masafumi
SHARP Corporation.
Advanced Telecommunication Laboratory
Corporate Reserach And Development Group
Sharp Corporation.
22-22 Nagaike-cho
Abeno-ku, Osaka, Osaka 545-0013
Japan

Phone: +81-43-299-8532
Fax: +81-43-299-8719
Email: aramoto.masafumi@sharp.co.jp
URI: <http://sharp.co.jp/>

Pascal Thubert
Cisco Systems

Village d'Entreprises Green Side
400, Avenue de Roumanille
Batiment T3
Biot - Sophia Antipolis 06410
FRANCE

Phone: +33 4 97 23 26 34
Email: pthubert@cisco.com

Wakikawa, et al.

Expires May 21, 2008

[Page 11]

Internet-Draft

HA Limited Proxy NDP

November 2007

Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information

on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).