MIP6 Working Group
Internet-Draft
Expires: August 5, 2007

R. Wakikawa
Keio University
M. Aramoto
Sharp
February 2007

Elimination of Proxy NDP from Home Agent Operations
draft-wakikawa-mip6-no-ndp-00.txt

Status of this Memo

Copyright Notice

Abstract

This document summarizes operations of home agent without using the proxy NDP. The Proxy NDP is mainly used to intercept packets by a Home Agent on Mobile IPv6 and NEMO.

Table of Contents

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 extended home prefix, the extended home prefix and the virtual home prefix. Proxy NDP is useless specially when the extended 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.

2. Terminology

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 [3]

Readers are expected to be familiar with all the terms defined in the RFC3753 [4] and the NEMO Terminology draft [5]

No new additional term is defined in this document.

3. Use Case

3.1. Mobile IP6: Virtual Home Link

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 on the home link by the Proxy NDP. On the other hand, the Home agent intercepts all the packets sent by a Correspondent node. The correspondent node is always located on the Internet (i.e. not home link). To do so, the Home agent is configured as an external router at the routing functions 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.

For this operation, the Home Agent SHOULD send Router Advertisements which on-link flag is unset. A node receiving the Router Advertisements does not maintain a prefix route (on-link route) and always uses a default route to send packets. Even if a destination node is on-link node, the node sends packets through its default route (i.e. Home Agent in this case). The detail operation is explained in Section 5.2.

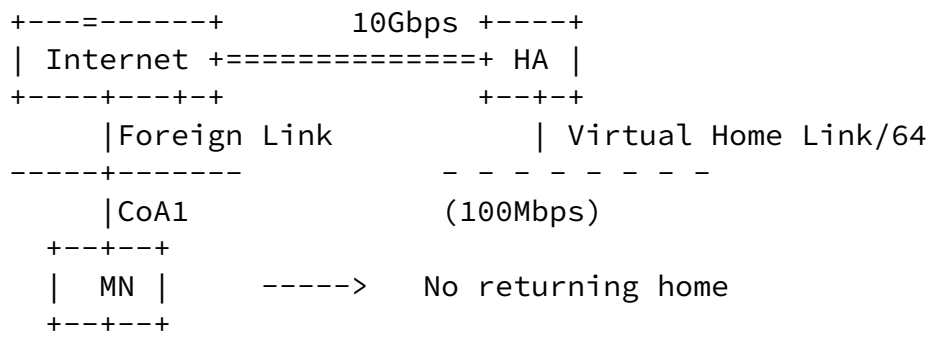


Figure 1: MIP

3.2. Network Mobility: Aggregated Home Link

The NEMO specification [6] allows that a home link is configured as the aggregated home prefix. The Home Agent manages the aggregated network address blocks and assigns an internal network prefix(es) to a Mobile Router as shown in Figure 2. In such a deployment scenario, 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. After the Home Agent receives packets meant for the mobile network prefix, it routes packets based on binding caches to the target mobile router.

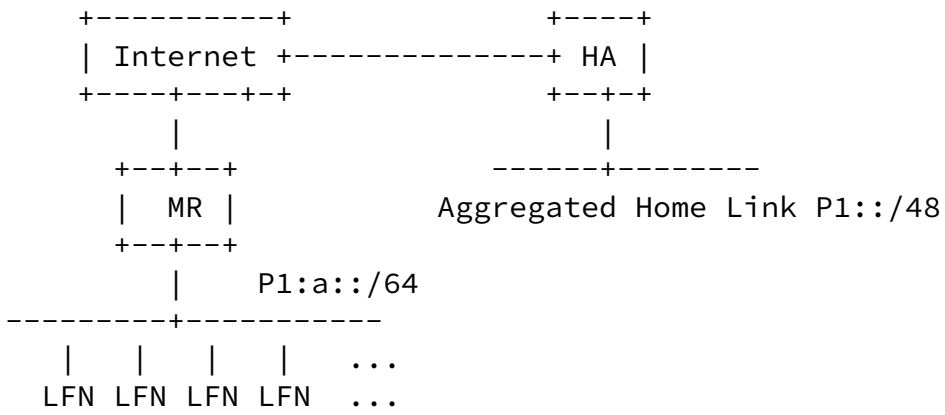


Figure 2: Aggregated Home Link

3.3. Monami6: Simultaneous Use of Home and Foreign Link

According to the Multiple Care-of Address Registration [2], when a multihomed mobile node returns home, it MUST choose one operation from following options:

- The mobile node returns home by an interface attached to the home link. It de-registers all its bindings from the Home Agent.

After the de-registration, the mobile node sends and receives all the packets via the interfaces attached to the home link.

o The mobile node does not return home and intentionally disables the interfaces attached to the home link. The mobile node sends and receives all its packets via the interfaces attached to foreign links.

The current specification 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 is related to 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. This will causes address duplication problem at the end.

This document recommends not to use the Proxy NDP for the scenario shown in Figure 3. If the proxy NDP is disabled, the main problem can be solved. In the Multiple Care-of Address Registration case, the elimination of Proxy NDP enable that Mobile Node and Home Agent maintain multiple bindings, one of the Mobile Node's interface is attached to the home link and the other is attached to the foreign link.

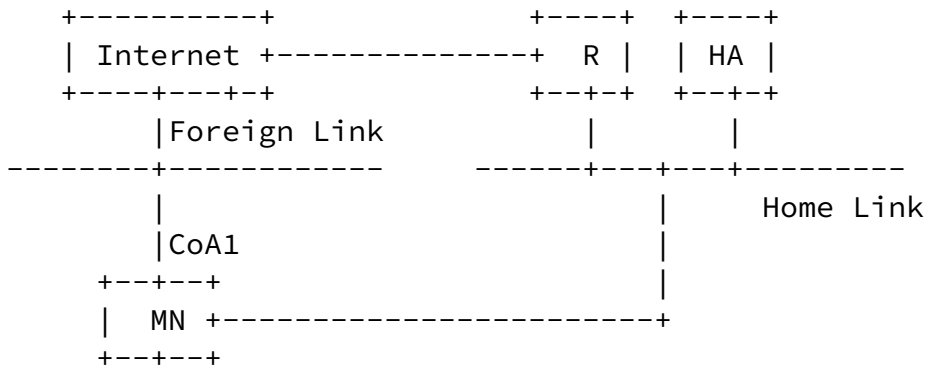


Figure 3: MCoA

4. Home Agent Configuration

In Mobile IPv6 and NEMO, two possible placements of Home Agents are originally introduced. The difference between them is whether the Home Agent acts as an external router or not as shown in Figure Figure 4.

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 discovery protocol. The Home Agent intercepts packets according to the IP routing. All the packets toward the home prefix will be routed to the Home Agent first. 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. If a binding cache is found for the packets' destination, it then tunnels the packets to the mobile node according to the binding cache entry. Otherwise, the Home Agent routes packets to the home link.

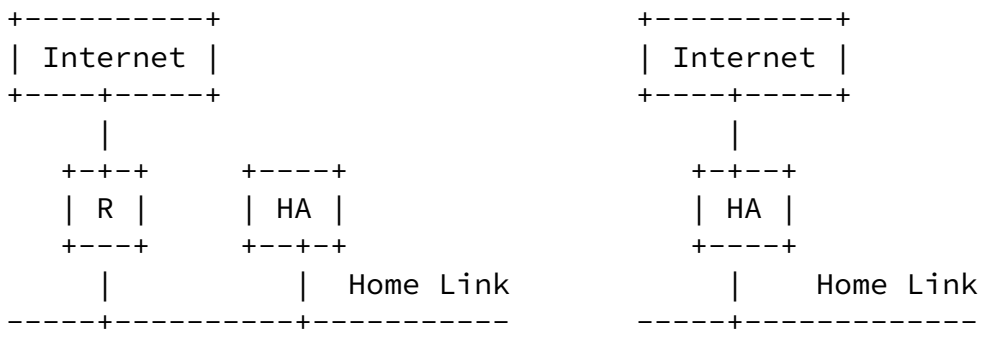


Figure 4: Home Agent Placements

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]. Since the home agent intercepts packets based on IP routing, it must be external router. It is harder to achieve load-balancing by utilizing multiple home agents on the home link. However, for the purpose of the home agent reliability, the Home Agent Reliability protocol can be operated with the specific configuration in Figure 5. In this case, upper router can switch the routing based on the HA survivability as shown in Figure 5

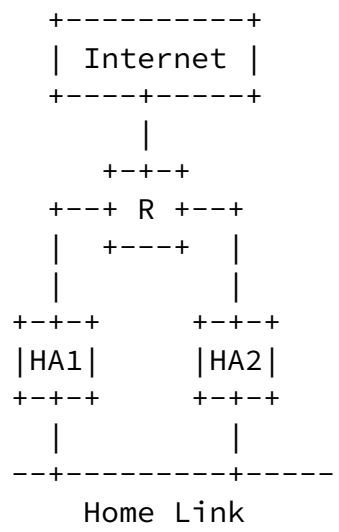


Figure 5: Multiple Home Agents Placement

5. Home Agent Operation

5.1. Duplicate Address Detection

RFC3775[7] uses the Proxy NDP to defend a Home Address of a Mobile Node when the Mobile Node is away from the Home Link. When the Mobile Node is away from the Home and registers its Care-of Address to the Home Agent, the Home Agent defends the Home Address by the proxy NDP for the Home Address. 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 specially on a physical configured home link, the uniqueness of a home address should be carefully verified. 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 traffic is 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 can 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.

5.2. 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. 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 6. 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.

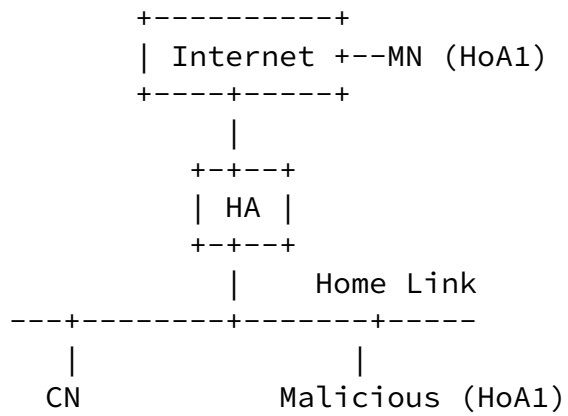


Figure 6: Malicious Node communicating with CN on the home link

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.

5.3. Deliverying Packets to the Mobile Node

Although the Home Agent intercepts packets by IP routing, how to tunnel packets to the Mobile Node 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 5.2. 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 to the Home Link. In this case, the Home Agent MUST NOT generate ICMP Redirect message to the sender.

5.4. Filtering Packets for Home Addresses

The Home Agent MUST operate the binding de-registration carefully if the Proxy NDP is disabled on a physical home link. As soon as a Mobile Node returns home, the Mobile Node can do DAD before binding update for de-registration. It means the Home Agent cannot distinguish whether either a right Mobile Node or a malicious node operates DAD on the Home Link. Home Agent MUST prevent routing

packets of a Home Address during binding cache of the Home Address is active so that it drops packets when the malicious node acquires the Home Address of other Mobile Node.

All traffic is through the Home Agent (see Section 5.2), the Home Agent MUST drop all the packets originated from the Home Link unless the binding is deleted. When the binding is active, any packets which source address is the Home Address MUST NOT generate from the Home Link. For incoming packets from the external network (ex. Internet), the Home Agent MUST NOT route the packets meant for a Home Address to the Home Link when the binding cache for the Home Address is active. If the packets meant for the Home Address are arrived from a Correspondent Node located on the Home Link, it can tunnel packets to the Mobile Node according to the Binding Cache. Otherwise, it can routes packets to the Mobile Node located on the Home Link. Figure 7 and Figure 8 show the example routing rules of the Home Agent.

```
HoA:= Home Address
BC:= Binding Cache for HoA
source:= IPv6 Source Address Field
dest:= IPv6 Destination Address Field

If (BC == true) {
   if (source == HoA) {
       /* drop the packet */
   } else if (dest == HoA) {
       /* tunnel the packet */
   }
} else if (BC == None) {
   if (source == HoA) {
       /* route the packet to the destination*/
   } else if (dest == HoA) {
       /* route the packet to the Home Link */
}
```

Figure 7: Rules for Packets meant for a Home Address Received from the Home Link


```
HoA:= Home Address
innersource:= IPv6 Source Address Field of Inner IPv6 Header
source:= IPv6 Source Address Field
dest:= IPv6 Destination Address Field
BC:= Binding Cache for the innersource
tunneled:= IPv6-IPv6 Encapsulation Packet

if (tunneled == true && innersouce == HoA) {
/* for tunneled packets (i.e. packets to CN from MN) */
   if (BC == true) {
      /*
```

```
            * Route to the Destination after depacauslatition.
            *
            * It's required the outer source address (CoA)
            * verification, too.
            */
        } else { /* BC == none */
            /* drop the packet */
        }
    } else {
    /* for no tunneled packets (i.e. packets to MN from CN) */
        if (source == HoA) {
            /* drop the packet, something odd happened. */
        } else if (dest == HoA) {
            if (BC == true) {
                /* Tunnel to the Mobile Node */
            } else if (BC == none) {
             /* Route to the Home Link */
            }
        }
    }
```

Figure 8: Rules for Packets meant for a Home Address Received from the external network (ex. Internet)

5.5. Returing Home

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

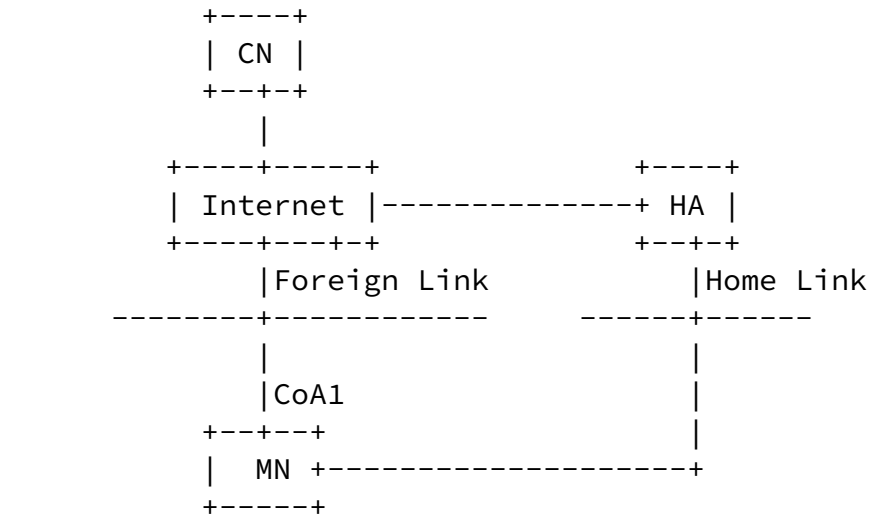
6. Mobile Node & Correspondent Node Operation

No modification is required. This Specification is transparent to Mobile Nodes and Correspondent Nodes

7. Multiple Care-of Address Registration

In the Multiple Care-of Address Registration [2], the Mobile Node MUST disable either the interface attached to the home link or the interfaces attached to the foreign link. This is because the Home Agent defends the home address of the Mobile Node by proxy neighbor advertisements. So as to avoid the home address duplication at the home link, the Mobile Node MUST select whether it returns home or not. If a binding is active for the Mobile Node, all packets routed to the home link are intercepted by the Home Agent. On the other hand, if the Mobile Node returns home, the Home Agent no longer intercept packets and cannot tunnel the packets to the Mobile Node's interface attached to the foreign link.

Figure 9 depicts the scenario where Mobile Node activates the interface attached to the home link and the foreign link, and communicates with all of the interfaces. Since the Home Agent does not use Proxy Neighbor Advertisement to intercept packets, the Mobile Node can utilize both of interfaces attached to the home link and the foreign link simultaneously. The Home Agent can intercept packets by IP routing, but not by proxy Neighbor Discovery.

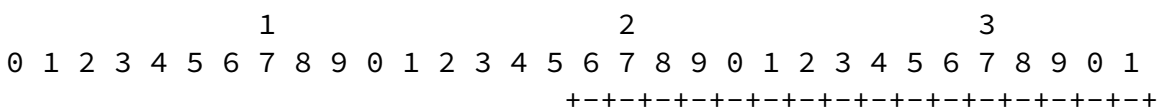



```
  Binding Cache Database:
     Home Agent's binding (No Proxy neighbor advertisement)
           binding [a:b:c:d::EUI  a:b:c:d::EUI      BID1] (Home BC)
           binding [a:b:c:d::EUI  Care-of Address1  BID2]
     Correspondent Node's binding
           binding [a:b:c:d::EUI  a:b:c:d::EUI      BID1] (Home BC)
           binding [a:b:c:d::EUI  Care-of Address1  BID2]
                     or
           None
```

Figure 9: Utilizing of both an interface attached to the Home Link and an interface attached to the Foreign Link

When the Mobile Node returns home, it de-registers a binding for the interface. While the bindings for the interfaces attached to the foreign link are still active. Intercepting packets, the Home Agent can decide whether it tunnels to the foreign interface or routes to the home interface of the Mobile Node. To do so, the Home Agent must know that the Mobile Node is back to the home link. However, if the binding is deleted according to [7], there is no way for the Home Agent to know that the Mobile Node is at the home, too. The Home Agent SHOULD invalidate the binding for the interface attached to the home link and MAY NOT delete it. It can alternatively mark that the Mobile Node is at the home link, too. In this document, as an example, the Home Agent inserts the Home Address of the Mobile Node in the Care-of Address field of the Mobile Node. The binding is named "Home Binding" in this doc. The Home Agent MAY manage this home binding as same as the other binding entry in terms of lifetime validation, etc. The Mobile Node MAY send multiple binding de-registration to keep this home binding active. Alternatively, the Home Agent can use infinity lifetime for the lifetime of the home binding. When the Mobile Node leaves the Home Link, it can update the home binding to the normal binding. Before that, the Home Agent believes the Mobile Node is at the home and may route packets for the Mobile Node to the Home Link.

For this operation, the Binding Unique Identifier sub-option is modified as described in Figure Figure 10. The new Home flag is introduced. When the H flag is set, the Home Agent MUST treat the binding as the home binding. After intercepting the packets, the Home Agent may tunnel the packets according to the active binding cache(s) or route the packets to the home link according to the home binding cache. Note that the H flag MUST be used only for the binding de-registration. Note that the same mechanism is used for the correspondent node.



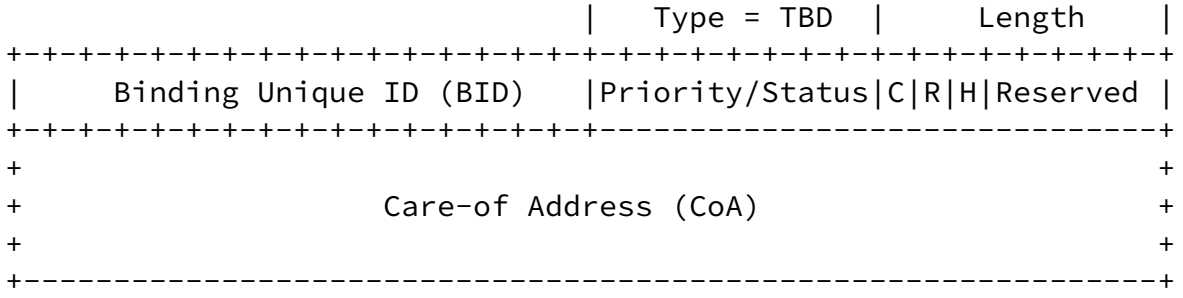


Figure 10: BID Sub-Option

Home Binding (H) flag

When this flag is set, a home agent stores a Home Address in the Care-of Address field of the binding cache entry. This flag must be used only for binding de-registration. This flag is not used in the bulk registration mode.

Reserved

5 bits Reserved field. Reserved field must be set with all 0.

8. Related Information

Related Documents can be found in the Informative Reference section

9. IANA considerations

This document does not require any IANA action.

10. Security Considerations

No security vulnerability is not introduced in this specification.

11. References

11.1. 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] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[4] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[5] Ernst, T. and H. Lach, "Network Mobility Support Terminology", draft-ietf-nemo-terminology-06 (work in progress), November 2006.

[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.

11.2. Informative Reference

[9] Ng, C., "Analysis of Multihoming in Network Mobility Support", draft-ietf-nemo-multihoming-issues-06 (work in progress), June 2006.

Appendix A. Change Log From Previous Version

- Initial Documentation

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 Inc.
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/

Full Copyright Statement

Intellectual Property

Acknowledgment

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