

MEXT Working Group  
Internet-Draft  
Intended status: Informational  
Expires: January 9, 2009

R. Wakikawa  
Toyota ITC  
July 8, 2008

**The Design Consideration of Correspondent Router**  
**draft-wakikawa-mext-cr-consideration-00.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/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 January 9, 2009.

Copyright Notice

Copyright (C) The IETF Trust (2008).

## Abstract

This document describes the protocol design consideration of the correspondent router for the NEMO Basic Support Protocol.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Design Consideration . . . . .	<a href="#">4</a>
<a href="#">2.1.</a>	Triggering Route Optimization . . . . .	<a href="#">4</a>
<a href="#">2.2.</a>	Discovering Correspondent Router . . . . .	<a href="#">4</a>
<a href="#">2.3.</a>	Registering Binding to Correspondent Router . . . . .	<a href="#">5</a>
<a href="#">2.4.</a>	Routing Packets via Correspondent Router . . . . .	<a href="#">6</a>
<a href="#">3.</a>	IANA considerations . . . . .	<a href="#">9</a>
<a href="#">4.</a>	Security Considerations . . . . .	<a href="#">10</a>
<a href="#">Appendix A.</a>	References . . . . .	<a href="#">10</a>
<a href="#">A.1.</a>	Normative References . . . . .	<a href="#">10</a>
<a href="#">A.2.</a>	Informative References . . . . .	<a href="#">10</a>
	Author's Address . . . . .	<a href="#">11</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">12</a>







## **2. Design Consideration**

There are several issues to design a protocol for Correspondent Router.

### **2.1. Triggering Route Optimization**

In the NEMO Basic Support protocol [[RFC-3963](#)], a mobile router takes care of all the mobility signaling. The mobile router first needs to detect the flow in or out the mobile network to initiate the route optimization. The detection can be done by receiving packets of mobile network nodes at either ingress or egress interfaces. In Mobile IPv6, the mobile host can decide whether the route optimization is initiated or not. However, It is hard for the mobile router to optimize only specific flows. The mobile router is an intermediate node between end nodes and cannot judge the route optimization per flow without some policy.

The information of the policy might be a flow classification (5 tuples), a route optimization capability (BOOLEAN: ON/OFF), etc. The packets snooping does not help much to distinguish the flow characteristics such as short/long-term, delay-sensitive, etc. It is also hard to distinguish a flow if there are the ESP protected flows. There are several ways to set such policy to the mobile router. If a mobile network node dynamically installs such policy to a mobile router, we need a new policy exchange protocol between a mobile network node and the mobile router. Alternatively, the operator of the mobile router can statically set the policy.

The home agent distribution such as the global HAHA [[ID-HAHAINTEROP](#)] [[ID-HAHA](#)] is much simpler. The mobile router or the mobile node are not involving the route optimization trigger. The trigger is given by the home agent.

### **2.2. Discovering Correspondent Router**

Since a correspondent router is also intermediate node on the path between end-nodes, it is harder to discover the address of the correspondent router. We have to consider two different scenarios for the discovery.

1. Correspondent Router is located on the path of end-nodes
2. Correspondent Router is NOT located on the path of end-nodes

If a correspondent router is located on the path, the mobile router might send control packets (ICMP, etc) and discovers the Correspondent Router. This is dynamic discovery based on routing



mechanism. On the other hand, if a Correspondent Router is NOT located on the path of end nodes, it can be discovered by some lookup system such as DNS. A mobile router lookup DNS server for the correspondent router address of the target flow. The anycast address can be also used to find the best correspondent router [[ID-ORC](#)], but the anycast address must be defined at any networks where correspondent nodes locate. How to look up the anycast address is another issue.

The global HAHA [[ID-HAHAINTEROP](#)] [[ID-HAHA](#)] does not require the dynamic discovering any entity, because the home agents are operated by the same operator and are controlled in their network.

### **2.3. Registering Binding to Correspondent Router**

The Correspondent Router and the mobile router are not belong to the same administrative domain, there are several security concerns. After detecting the correspondent Router, a mobile router needs to send a secured binding update to the correspondent router. However, since both a mobile router and a Correspondent Router are intermediate nodes of the end-nodes, a mechanism to secure the signaling between two routers is required. The establishment cost of the security association might be negligible.

Next concern is whether a mobile router sends a binding update for either an address of the mobile network node or prefix(es) of the mobile router. If the binding is for the mobile network prefix(es), careful operations must be taken. Otherwise, all the flows initiated from the the mobile network prefix(es) are going to be optimized with the correspondent router. This might be unexpected behavior in some scenarios. After the mobile router registers the prefix binding to the correspondent router, it is uncontrollable to optimize only specific flow destined to correspondent nodes behind the correspondent router.

Another security concern is the address/prefix ownership verification of the binding. Since the mobile router does not configure with the address, how can the correspondent router believe the the address in the binding update which is not sent from the address owner (mobile network node). The prefix ownership verification is more challenging issue. An address/prefix ownership verification mechanism between a mobile router and a correspondent router is required. Note that the reachability test like Return Routability cannot be used because the mobile router cannot respond to the correspondent router with the address of the mobile network node or the mobile network prefix(es).

In the global HAHA, all the home agents are belong to the same administrative group. Therefore, we might expect the secured link





between home agents or might utilize strong security mechanism for signaling between home agents. The prefix or address verification is easily operated, since the home agent delegates that address and prefix(es) to the mobile router.

#### **2.4. Routing Packets via Correspondent Router**

Even after the successful binding registration to the Correspondent Router, the path between two nodes should be via both the mobile router and the Correspondent Router (HA-MR-CR-CN). However, some considerations are required to keep the ideal path by the operators of the Mobile Router and the Correspondent Router. The routing managements are another challenging issue of the Correspondent Router. The issues are classified into two parts: MR-CR routing path management and CN-CR routing path management.

MR-CR Route Management:

In Figure 1, the path between a correspondent node and a mobile network node is drawn as the symmetric path. However, in the current Internet, the path is often asymmetric. Many autonomous systems has multiple peering points and injects the own routes from them. Therefore, even if one direction is optimized, there is no guarantee that the reverse path is also optimized (Figure 2). Therefore, for the deployment of correspondent routers, the operator must be carefully managed their network in terms of routing, the location of correspondent routers, and the number of correspondent routers, etc. Note that this management is relatively difficult because the mobile router changes its attachment point. The path between the mobile router and the correspondent router is changed by the mobile router's movements.

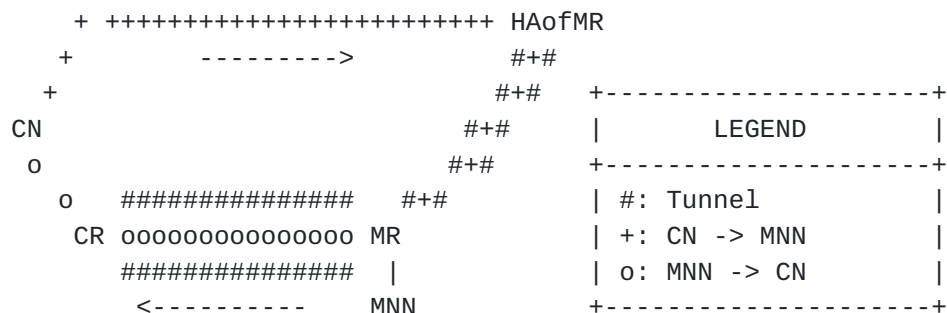


Figure 2: Asymmetric Path (MR-CN Route Management)



## CN-CR Route Management:

Another routing management issue is how the Correspondent Router handle the packets meant for the mobile router from correspondent nodes. In Figure 3, there are two exit routers toward the Internet in the site of correspondent node and place one or more correspondent routers at the exit router as an example configuration.

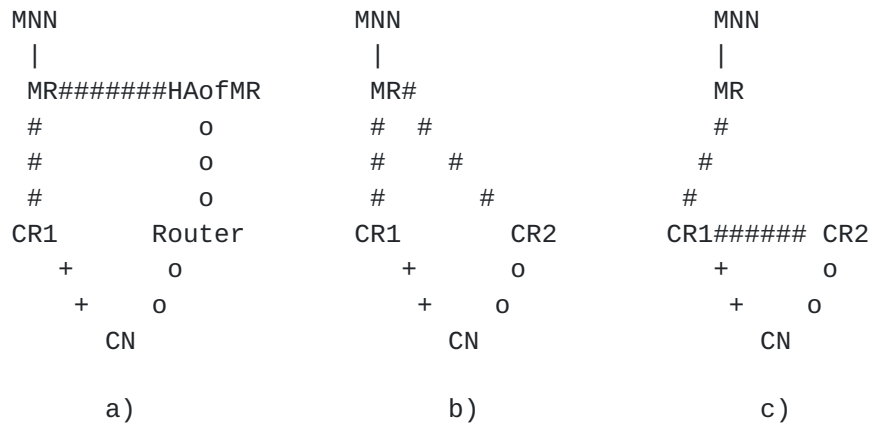


Figure 3: Multiple Exit Routers (CN-CR Route Management)

In Figure 3-a), if the packets from the correspondent node is routed to the Router, the packet is routed through the home agent (i.e. unoptimized path). In order to optimize the path, the operator MUST guarantee that the Correspondent Router (CR1) receives all packets meant for the mobile router from correspondent nodes. To do so, the CR1 dynamically injects the mobile network prefix of the mobile router to the site of the correspondent node. This injecting routes will be available while the CR1 manages the active binding of the mobile router. However, from the administrative and operational point of view, the route injection of the different prefixes from its autonomous system are often restricted.

Another approach is shown in Figure 3-b) and -c). Correspondent Routers are placed at all the exit routers of the site. We now investigate the multiple correspondent router managements. This configuration might brings other routing management issues inside the site of the correspondent router.

In Figure 3-b), the mobile router sends a binding update to both CR1 and CR2 to establish bi-directional tunnels. It causes additional overheads to the mobile router such as 1) discovering all the correspondent routers, 2) sending multiple binding updates, 3) managing multiple tunnels.



Alternatively, after receiving a binding update from the mobile router, the receiver of the binding update (let's say CR1 as an example) synchronizes the state with the other correspondent routers (CR2) in Figure 3-c). The CR2 establishes a tunnel to the CR1 for the packets destined to the mobile network prefix. Additional protocols such as inter-correspondent router protocol like the inter-HAHA protocol [[ID-HAHA](#)] might be required.

In the global HAHA, the differences might be 1) the aggregated route injection per the home prefix (sets of the mobile network prefixes), 2) the stable (controlled?!) route injection (no dynamic injection). Each home agent in the global HAHA injects its entire home prefix from different location and advertise that the aggregated home prefix route persistently. The routing management of the HAHA must be more controllable for operators than the one of Correspondent routers.



### **3. IANA considerations**

This document does not require any IANA action.



#### **4. Security Considerations**

Security vulnerability is not introduced in this specification.

#### **Appendix A. References**

##### **A.1. Normative References**

[RFC-3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.

[RFC-3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", [RFC 3963](#), January 2005.

##### **A.2. Informative References**

[RFC-3753] Manner, J. and M. Kojo, "Mobility Related Terminology", [RFC 3753](#), June 2004.

[RFC-4885] Ernst, T. and H. Lach, "Network Mobility Support Terminology", [RFC 4885](#), July 2007.

[RFC-4888] C. Ng, et. al, "Network Mobility Route Optimization Problem Statement", [RFC 4888](#), July 2007.

[RFC-4889] C. Ng, et. al, "Network Mobility Route Optimization Solution Space Analysis", [RFC 4889](#), July 2007.

[ID-HAHA] Thubert, P., Wakikawa, R., and V. Devarapalli, "Global HA to HA protocol", Work in Progress, September 2006.

[ID-HAHAINTEROP] R. Wakikawa, K. Shima and N. Shigechika, "The Global HAHA Operation at the Interop Tokyo 2008", [draft-wakikawa-mext-haha-interop2008-00.txt](#) (work in progress), July 2008.

[ID-AEROREQ] W. Eddy, et. al, "NEMO Route Optimization Requirements for Operational Use in Aeronautics and Space Exploration Mobile Networks", [draft-ietf-mext-aero-reqs-02.txt](#), May 2008.

[ID-AUTOREQ] R. Baldessari, et. al, "Automotive Industry Requirements for NEMO Route Optimization", [draft-ietf-mext-nemo-ro-automotive-req-00.txt](#), February 2008.

[PAPER-ORC] Wakikawa, R., Koshiba, S., Uehara, K., and J. Murai,



"ORC: Optimized Route Cache Management Protocol for Network Mobility", 10th International Conference on Telecommunications, vol 2, pp 1194-1200, February 2003.

[ID-ORC] Wakikawa, R. and M. Watari, "Optimized Route Cache Protocol (ORC)", Work in Progress, November 2004.

#### Author's Address

Ryuji Wakikawa  
Toyota ITC / Keio University  
6-6-20 Akasaka, Minato-ku  
Tokyo 107-0052  
Japan

Phone: +81-3-5561-8276  
Fax: +81-3-5561-8292  
Email: [ryuji@jp.toyota-itc.com](mailto:ryuji@jp.toyota-itc.com)



## Full Copyright Statement

Copyright (C) The IETF Trust (2008).

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](mailto:ietf-ipr@ietf.org).

## Acknowledgment

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

