

Mobile IP Working Group
INTERNET DRAFT
5 October 2000

Rajeev Koodli
Charles E. Perkins
Communication Systems Laboratory
Nokia Research Center

Fast Handovers in Mobile IPv6
[draft-koodli-mobileip-fastv6-00.txt](#)

Status of This Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

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 document is an individual submission for the mobile-ip Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the MOBILE-IP@STANDARDS.NORTELNETWORKS.COM mailing list.

Distribution of this memo is unlimited.

Internet Draft

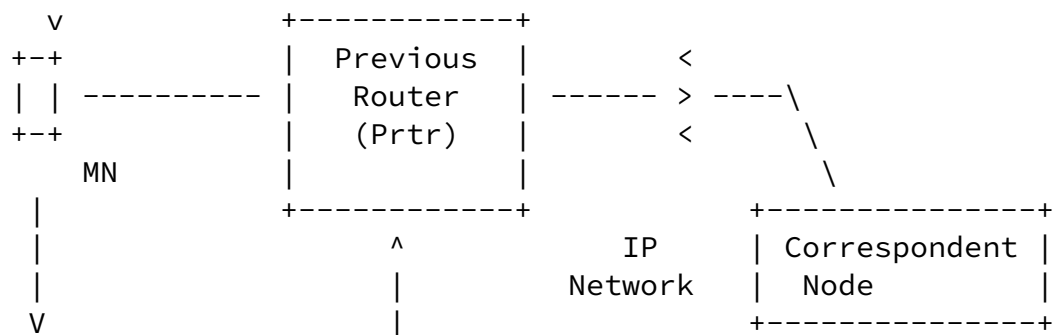
Fast Handovers in Mobile IPv6

5 October 2000

Contents

Status of This Memo	i
1. Fast Handover Definition	2
2. Proposal	3
3. Relation to Link Switching Failures	6
4. Security Considerations	6
Addresses	6

When a Mobile Node (MN) undergoes handover from a link to another, it needs to obtain a new IP address at the New Router as soon as possible in order to be able to send and receive IP packets. See Figure 1 for a reference diagram of handover assumed in the rest of this document. The latency involved in forming a new CoA in IPv6 comes mainly from Neighbor Discovery, which includes Router Advertisement and possibly Router Solicitation, and Duplicate Address Detection (DAD) when stateless auto-configuration is used. After the MN forms a new CoA, it can send packets using the new CoA, but not receive packets at that address until its mobility agent(s) and correspondent nodes are notified through Binding Updates. This is illustrated in Figure 2. Thus, the delay involved in forming a new CoA must be reduced so that the MN can resume IP packet transmission quickly, and, the latency involved in getting the BU to its recipients must be optimized. In this proposal, we outline means to optimize these two design points when handovers are network-controlled, i.e., some network entity instructs the MN to undergo handover from an access router to another, and hence is assumed to know the IP addresses and network prefixes of those routers.



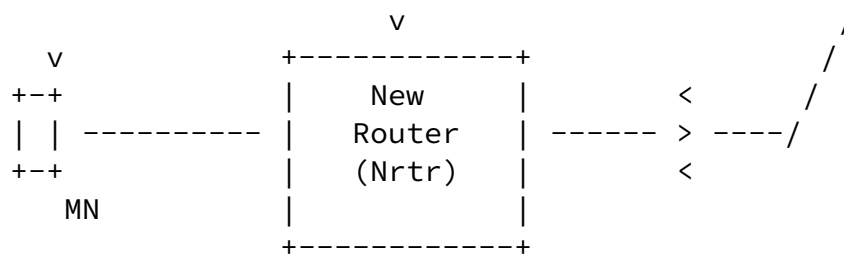


Figure 1: Reference Scenario for Handover

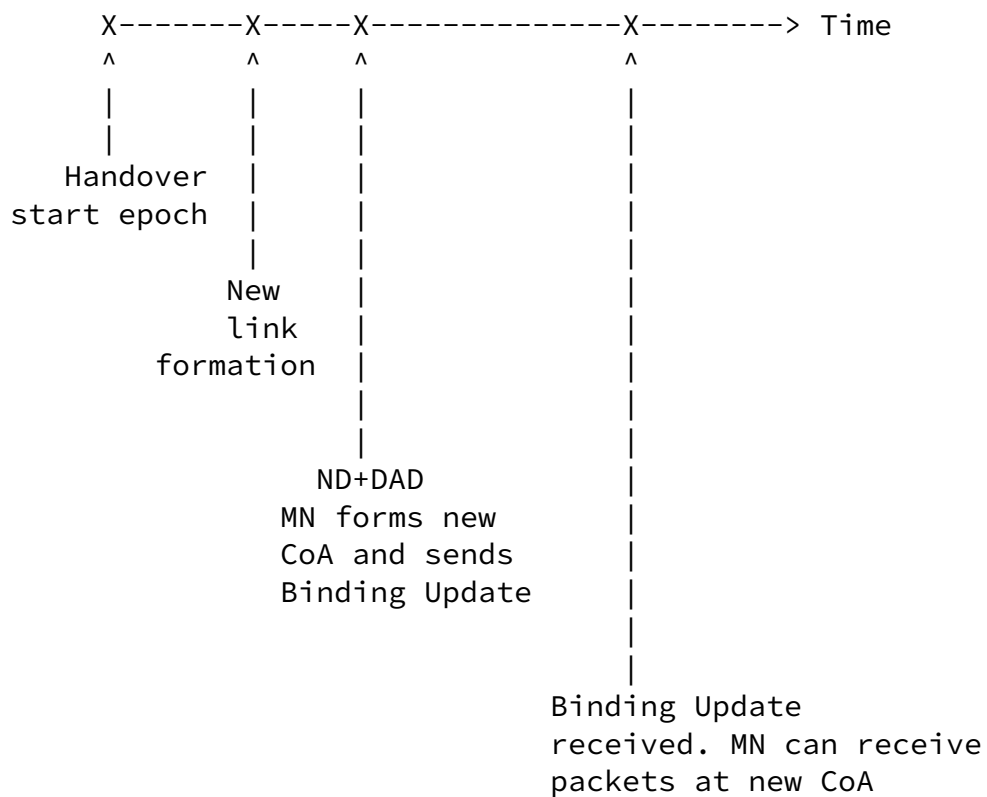


Figure 2: Handover Delays

2. Proposal

When the handovers are triggered by the network, with possible assistance from the MN regarding the decision to undergo handover, the Previous Router determines the network prefix of the New Router to which the MN will get attached to next. The Previous Router can obtain network prefix(s), e.g., from a network entity that controls the handover. Subsequently, Previous Router sends a modified Neighbor Discovery Redirect message to the MN in which it provides one or more network prefixes of the New Router as well as the New Router's link-local IP address. The MN then forms a new CoA using address auto-configuration, includes it as an alternate CoA and sends a Proactive Previous Router Notification message to the Previous Router. In this message, the MN supplies its new CoA and possibly its security credentials. The effect of this message is to set up forwarding from Previous Router to the MN's new CoA at the New Router. Note that the Previous Router may set up this forwarding subsequent to issuing the Redirect message without waiting for, or expecting a Notification

message from the MN when it is desirable not to send this control message over the air interface.

After this process, the MN undergoes Layer 2 handover to establish a new link to the New Router. The MN then directly sends a Neighbor Solicitation message to determine the New Router's link-layer address. When the New Router responds back with a Neighbor Advertisement message, it indirectly verifies if the IP address of the MN as derived from the Source Address field in Neighbor Solicitation message is already in use when it updates its Neighbor Cache. In this way, (partial) Duplicate Address Detection can also be performed. After the Neighbor Solicitation and Neighbor Advertisement messages, the MN is ready to send and receive IP packets at its new CoA. With these optimizations, the handover delays are as shown in Figure 3.

Subsequent to Neighbor Discovery, the MN sends a Binding Update towards its mobility agent. Note that since the Previous Router already

has an association from the previous CoA to the new CoA, the packets could be arriving at the New Router almost as soon as a new link is established for the MN. Some of these packets that arrive earlier than the MN's establishment of IP connectivity at the New Router could be lost without appropriate support for buffering. The number of such packets lost can also be reduced by instrumenting the forwarding epoch at the Previous Router appropriately (e.g, by sending the Proactive Previous Router Notification message just ahead of the impending link disruption in L2 handover process or by other means).

Figure 3: Optimized Handover Delays

nothing. If an entry does not exist, the New Router begins to act as a Proxy so that it can respond to any potential DAD conflicts on its link for the new CoA. This provides means for avoiding potential DAD conflicts due to selecting an address while not on-link.

Second, subsequent to attaching to the new link, the MN performs Neighbor Solicitation to determine the New Router's link-layer address. When it does this, it sets an ``O'ptimistic flag in the Reserved field of the Neighbor Solicitation message indicating to the Target (New Router) that the address in the Source IP address is optimistic, and if the New Router already has an entry for that address in its ND cache, it must not overwrite that entry, and that the New Router must respond back with a Neighbor Advertisement message indicating that the address is in use. The MN should then proceed to form a new link-local address according to the rules specified in [3]. This provides an optimized way of reducing latency due to DAD after the MN attaches to the new link.

The modifications to the ND Redirect message are as follows. The Destination Address field is set to zero to indicate that the MN should use the address specified in the Target Address field as the New Router subsequent to handover. The Redirected Header option is also set to zero to minimize space. In addition, a new option type is defined that allows inclusion of one or more network prefixes. This option type follows the format specification in [2]. Note that the Redirect message implicitly assumes that the Router parameters remain the same for the target (New Router). Thus, the MN should continue to use its existing Router parameters until it hears a new Router Advertisement by the New Router and take actions according to [2].

The Previous Router MAY send a message to the New Router providing security keys to validate the neighbor cache at the New Router. The New Router MAY NOT respond back to the MN's Neighbor Solicitation message until its credentials are validated, e.g., through the receipt of a suitable message from the Previous Router. The Previous Router MAY use an unsolicited SHREP message [1], in response to the Proactive Previous Router notification message, to supply this security information (as well as an indication to buffer packets) and it MAY also include any other useful context information in the same message.

In some radio networks, it is possible that the MN is not able to establish the link with the New Router after deciding to undergo new link establishment. In such a case, the MN may revert back to the Previous Router resulting in a ``link reversal''. When this happens, the MN has to send a Previous Router Notification message requesting to disable forwarding to the new CoA that is no longer valid. Note that since a Binding Update has not been delivered yet, packets will still be arriving at the Previous Router, and by disabling forwarding to the new CoA, those packets can be delivered again at the MN's current location.

When link reversals are not a concern, the MN MAY send a binding update prior to leaving the Previous Router itself.

[4](#). Security Considerations

To be added.

References

- [1] R. Koodli and C. Perkins. A Framework for Smooth Handovers with Mobile IPv6 (work in progress). Internet Draft, Internet Engineering Task Force.
[draft-ietf-koodli-smoothv6-00.txt](#), July 2000.
- [2] T. Narten, E. Nordmark, and W. Simpson. Neighbor Discovery for IP Version 6 (IPv6). Request for Comments (Draft Standard) [2461](#), Internet Engineering Task Force, December 1998.
- [3] S. Thomson and T. Narten. IPv6 Stateless Address Autoconfiguration. Request for Comments (Draft Standard) [2462](#), Internet Engineering Task Force, December 1998.

Addresses

The working group can be contacted via the current chairs:

Basavaraj Patil
Nokia Corporation
6000 Connection Drive
M/S M8-540
Irving, Texas 75039
USA
Phone: +1 972-894-6709
Fax : +1 972-894-5349
EMail: Basavaraj.Patil@nokia.com

Phil Roberts
Motorola
1501 West Shure Drive
Arlington Heights, IL 60004
USA
Phone: +1 847-632-3148
EMail: QA3445@email.mot.com

Internet Draft

Fast Handovers in Mobile IPv6

5 October 2000

Questions about this memo can also be directed to the authors:

Rajeev Koodli
Communications Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
Phone: +1-650 625-2359
EMail: rajeev.koodli@nokia.com
Fax: +1 650 625-2502

Charles E. Perkins
Communications Systems Lab
Nokia Research Center
313 Fairchild Drive
Mountain View, California 94043
USA
Phone: +1-650 625-2986
EMail: charliep@iprg.nokia.com
Fax: +1 650 625-2502

