Internet Engineering Task Force (IETF)
Request for Comments: 5949
Category: Standards Track
ISSN: 2070-1721

H. Yokota
KDDI Lab
K. Chowdhury
R. Koodli
Cisco Systems
B. Patil
Nokia
F. Xia
Huawei USA

September 2010

Fast Handovers for Proxy Mobile IPv6

Abstract

Mobile IPv6 (MIPv6; RFC 3775) provides a mobile node with IP mobility when it performs a handover from one access router to another, and fast handovers for Mobile IPv6 (FMIPv6) are specified to enhance the handover performance in terms of latency and packet loss. While MIPv6 (and FMIPv6 as well) requires the participation of the mobile node in the mobility-related signaling, Proxy Mobile IPv6 (PMIPv6; RFC 5213) provides IP mobility to nodes that either have or do not have MIPv6 functionality without such involvement. Nevertheless, the basic performance of PMIPv6 in terms of handover latency and packet loss is considered no different from that of MIPv6.

When the fast handover is considered in such an environment, several modifications are needed to FMIPv6 to adapt to the network-based mobility management. This document specifies the usage of fast handovers for Mobile IPv6 (FMIPv6; RFC 5568) when Proxy Mobile IPv6 is used as the mobility management protocol. Necessary extensions are specified for FMIPv6 to support the scenario when the mobile node does not have IP mobility functionality and hence is not involved with either MIPv6 or FMIPv6 operations.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5949.

Copyright Notice

Table of Contents

1. Introduction

Proxy Mobile IPv6 (PMIPv6) [RFC5213] provides IP mobility to a mobile node that does not support Mobile IPv6 (MIPv6) [RFC3775] mobile node functionality. A proxy agent in the network performs the mobility management signaling on behalf of the mobile node. This model transparently provides mobility for nodes within a PMIPv6 domain. Nevertheless, the basic performance of PMIPv6 in terms of handover latency and packet loss is considered no different from that of Mobile IPv6.

Fast handovers for Mobile IPv6 (FMIPv6) [RFC5568] describes the protocol to reduce the handover latency for Mobile IPv6 by allowing a mobile node to send packets as soon as it detects a new subnet link and by delivering packets to the mobile node as soon as its attachment is detected by the new access router. This document extends FMIPv6 for Proxy MIPv6 operation to minimize handover delay and packet loss as well as to transfer network-resident context for a PMIPv6 handover. [RFC5568] is normative for this document, except where this document specifies new or revised functions and messages.

2. Requirements Notation

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].

3. Terminology

This document reuses terminology from [RFC5213], [RFC5568], and [RFC3775]. The following terms and abbreviations are additionally used in this document.

Access Network (AN):
: A network composed of link-layer access devices such as access points or base stations providing access to a Mobile Access Gateway (MAG) connected to it.

Previous Access Network (P-AN):
: The access network to which the Mobile Node (MN) is attached before handover.

New Access Network (N-AN):
: The access network to which the Mobile Node (MN) is attached after handover.

Previous Mobile Access Gateway (PMAG):
: The MAG that manages mobility-related signaling for the mobile node before handover. In this document, the MAG and the Access Router are co-located.

New Mobile Access Gateway (NMAG):
: The MAG that manages mobility-related signaling for the mobile node after handover. In this document, the MAG and the Access Router (AR) are co-located.

Local Mobility Anchor (LMA):
The topological anchor point for the mobile node's home network prefix(es) and the entity that manages the mobile node's binding state. This specification does not alter any capability or functionality defined in [RFC5213].

Handover indication:
A generic signaling message, sent from the P-AN to the PMAG, that indicates a mobile node's handover. While this signaling is dependent on the access technology, it is assumed that Handover indication can carry the information to identify the mobile node and to assist the PMAG in resolving the NMAG (and the new access point or base station) to which the mobile node is moving. The details of this message are outside the scope of this document.

4. Proxy-Based FMIPv6 Protocol Overview

This specification describes fast handover protocols for the network-based mobility management protocol called Proxy Mobile IPv6 (PMIPv6) [RFC5213]. The core functional entities defined in PMIPv6 are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). The LMA is the topological anchor point for the mobile node's home network prefix(es). The MAG acts as an access router (AR) for the mobile node and performs the mobility management procedures on its behalf. The MAG is responsible for detecting the mobile node's movements to and from the access link and for initiating binding registrations to the mobile node's local mobility anchor. If the MAGs can be informed of the detachment and/or attachment of the mobile node in a timely manner via, e.g., lower-layer signaling, it will become possible to optimize the handover procedure, which involves establishing a connection on the new link and signaling between mobility agents, compared to the baseline specification of PMIPv6.

In order to further improve the performance during the handover, this document specifies a bidirectional tunnel between the Previous MAG (PMAG) and the New MAG (NMAG) to tunnel packets meant for the mobile node. In order to enable the NMAG to send the Proxy Binding Update (PBU), the Handover Initiate (HI) and Handover Acknowledge (HAck) messages in [RFC5568] are extended for context transfer, in which parameters such as the mobile node's Network Access Identifier (NAI), Home Network Prefix (HNP), and IPv4 Home Address are transferred from the PMAG. New flags, 'P' and 'F', are defined for the HI and HAck messages to distinguish from those in [RFC5568] and to request packet forwarding, respectively.

In this document, the Previous Access Router (PAR) and New Access Router (NAR) are interchangeable with the PMAG and NMAG, respectively. The reference network is illustrated in Figure 1. The access networks in the figure (i.e., P-AN and N-AN) are composed of Access Points (APs) defined in [RFC5568], which are often referred to as base stations in cellular networks.

Since a mobile node is not directly involved with IP mobility protocol operations, it follows that the mobile node is not directly involved with fast handover procedures either. Hence, the messages involving the mobile node in [RFC5568] are not used when PMIPv6 is in use. More specifically, the Router Solicitation for Proxy Advertisement (RtSolPr), the Proxy Router Advertisement (PrRtAdv), Fast Binding Update (FBU), Fast Binding Acknowledgment (FBack), and the Unsolicited Neighbor Advertisement (UNA) messages are not applicable in the PMIPv6 context. A MAG that receives a RtSolPr or FBU message from a mobile node SHOULD behave as if they do not implement FMIPv6 as defined in [RFC5568] at all -- continuing to operate according to this specification within the network -- or alternatively, start serving that particular mobile node as specified in [RFC5568].

```
                  +----------+
                  |   LMA    |
                  |          |
                  +----------+
                    /      \
                   /        \
                  /          \
      +........../..+      +..\..........+
      . +-------+-+ .______. +-+-------+ .
      . |  PMAG   |()_______)|  NMAG   | .
      . |  (PAR)  | .      . |  (NAR)  | .
      . +----+----+ .      . +----+----+ .
      .      |      .      .      |      .
      .   ___|___   .      .   ___|___   .
      .  /       \  .      .  /       \  .
      . (  P-AN   ) .      . (  N-AN   ) .
      .  \_______/  .      .  \_______/  .
      .      |      .      .      |      .
      .   +----+    .      .   +----+    .
      .   | MN |  ---------->  | MN |    .
      .   +----+    .      .   +----+    .
      +.............+      +.............+
```

Figure 1: Reference Network for Fast Handover

4.1. Protocol Operation

There are two modes of operation in FMIPv6 [RFC5568]. In the predictive mode of fast handover, a bidirectional tunnel between the PMAG (PAR) and NMAG (NAR) is established prior to the mobile node's attachment to the NMAG. In the reactive mode, this tunnel establishment takes place after the mobile node attaches to the NMAG. In order to alleviate the packet loss during a mobile node's handover (especially when the mobile node is detached from both links), the downlink packets for the mobile node need to be buffered either at the PMAG or NMAG, depending on when the packet forwarding is performed. It is hence REQUIRED that all MAGs have the capability and enough resources to buffer packets for the mobile nodes accommodated by them. The buffer size to be prepared and the rate at which buffered packets are drained are addressed in Section 5.4 of [RFC5568]. Note that the protocol operation specified in the document is transparent to the local mobility anchor (LMA); hence there is no new functional requirement or change on the LMA.

Unlike MIPv6, the mobile node in the PMIPv6 domain is not involved with IP mobility signaling; therefore, in order for the predictive fast handover to work effectively, it is REQUIRED that the mobile node is capable of reporting lower-layer information to the AN at a short enough interval, and that the AN is capable of sending the Handover indication to the PMAG at an appropriate timing. The sequence of events for the predictive fast handover is illustrated in Figure 2.

```
                                            PMAG        NMAG
          MN         P-AN       N-AN        (PAR)       (NAR)     LMA
          |           |          |            |           |        |
     (a)  |--Report-->|          |            |           |        |
          |           |          |            |           |        |
          |           |       Handover        |           |        |
     (b)  |           |------indication------>|           |        |
          |           |          |            |           |        |
          |           |          |            |           |        |
     (c)  |           |          |            |----HI---->|        |
          |           |          |            |           |        |
          |           |          |            |           |        |
     (d)  |           |          |            |<---HAck---|        |
          |           |          |            |           |        |
          |           |          |            |           |        |
          |           |          |            |HI/HAck(optional)   |
     (e)  |           |          |            |<- - - - ->|        |
          |           |          |          #=|<===================|
     (f)  |           |          |          #====DL data=>|        |
          |  Handover |       Handover        |           |        |
     (g)  |<-command--|<------command---------|           |        |
         ~~~          |          |            |           |        |
         ~~~          |          |            |           |        |
          |   MN-AN connection   |    AN-MAG connection   |        |
     (h)  |<---establishment---->|<----establishment----->|        |
          |           |          |  (substitute for UNA)  |        |
          |           |          |            |           |        |
     (i)  |<==================DL data=====================|        |
          |           |          |            |           |        |
     (j)  |===================UL data====================>|=#      |
          |           |          |          #=|<============#      |
          |           |          |          #=====================>|
     /    |           |          |            |           |        | \
     |(k) |           |          |            |           |--PBU-->| |
     |    |           |          |            |           |        | |
     |(l) |           |          |            |           |<--PBA--| |
     |    |<==================DL data=====================|<=======| |
     |    |           |          |            |           |        | |
     \    |===================UL data====================>|=======>| /

          UL        Uplink
          DL        Downlink
          PBA       Proxy Binding Acknowledgment
```

Figure 2: Predictive Fast Handover for PMIPv6 (Initiated by PMAG)

The detailed descriptions are as follows:

(a) The mobile node detects that a handover is imminent and reports its identifier (MN ID) and the New Access Point Identifier (New AP ID) [RFC5568] to which the mobile node is most likely to move. The MN ID could be the NAI, link-layer address, or any other suitable identifier, but the MAG SHOULD be able to map any access-specific identifier to the NAI as the MN ID. In some cases, the previous access network (P-AN) will determine the New AP ID for the mobile node. This step is access technology specific, and details are outside the scope of this document.

(b) The previous access network, to which the mobile node is currently attached, indicates the handover of the mobile node to the previous mobile access gateway (PMAG), with the MN ID and New AP ID. Detailed definition and specification of this message are outside the scope of this document.

(c) The previous MAG derives the new mobile access gateway (NMAG) from the New AP ID, which is a similar process to that of constructing an [AP ID, AR-Info] tuple in [RFC5568]. The previous MAG then sends the Handover Initiate (HI) message to the new MAG. The HI message MUST have the 'P' flag set and include the MN ID, the HNP(s), and the address of the local mobility anchor that is currently serving the mobile node. If there is a valid (non-zero) MN Link-layer Identifier (MN LL-ID), that information MUST also be included. With some link layers, the MN Link-local Address Interface Identifier (MN LLA-IID) can also be included (see Section 6.2.3).

(d) The new MAG sends the Handover Acknowledge (HAck) message back to the previous MAG with the 'P' flag set.

(e) If it is preferred that the timing of buffering or forwarding should be later than step (c), the new MAG MAY optionally request that the previous MAG buffer or forward packets at a later and appropriate time, by setting the 'U' flag [RFC5568] or the 'F' flag in the HI message, respectively.

(f) If the 'F' flag is set in the previous step, a bidirectional tunnel is established between the previous MAG and new MAG, and packets destined for the mobile node are forwarded from the previous MAG to the new MAG over this tunnel. After decapsulation, those packets MAY be buffered at the new MAG. If the connection between the new access network and new MAG has already been established, those packets MAY be forwarded towards the new access network, which then becomes responsible for them (e.g., buffering or delivering, depending on the condition of the mobile node’s attachment); this is access technology specific.

(g) When handover is ready on the network side, the mobile node is triggered to perform handover to the new access network. This step is access technology specific, and details are outside the scope of this document.

(h) The mobile node establishes a physical-layer connection with the new access network (e.g., radio channel assignment), which in turn triggers the establishment of a link-layer connection between the new access network and new MAG if not yet established. An IP-layer connection setup may be performed at this time (e.g., PPP IPv6 Control Protocol) or at a later time (e.g., stateful or stateless address autoconfiguration). This step can be a substitute for the Unsolicited Neighbor Advertisement (UNA) in [RFC5568]. If the new MAG acquires a valid new MN LL-ID via the new access network and a valid old MN LL-ID from the previous MAG at step (c), these IDs SHOULD be compared to determine whether the same interface is used before and after handover. When the connection between the mobile node and new MAG is PPP and the same interface is used for the handover, the new MAG SHOULD confirm that the same interface identifier is used for the mobile node’s link-local address (this is transferred from the previous MAG using the MN LLA-IID option at step (c), and sent to the mobile node during the Configure-Request/Ack exchange).

(i) The new MAG starts to forward packets destined for the mobile node via the new access network.

(j) The uplink packets from the mobile node are sent to the new MAG via the new access network, and the new MAG forwards them to the previous MAG. The previous MAG then sends the packets to the local mobility anchor that is currently serving the mobile node.

(k) The new MAG sends the Proxy Binding Update (PBU) to the local mobility anchor, whose address is provided in step (c). Steps (k) and (l) are not part of the fast handover procedure but are shown for reference.

(l) The local mobility anchor sends back the Proxy Binding Acknowledgment (PBA) to the new MAG. From this time on, the packets to/from the mobile node go through the new MAG instead of the previous MAG.

According to Section 4 of [RFC5568], the previous MAG establishes a binding between the Previous Care-of Address (PCoA) and New Care-of Address (NCoA) to forward packets for the mobile node to the new MAG, and the new MAG creates a proxy neighbor cache entry to receive those packets for the NCoA before the mobile node arrives. In the case of PMIPv6, however, the only address that is used by the mobile node is the Mobile Node's Home Address (MN-HoA), so the PMAG forwards the mobile node's packets to the NMAG instead of the NCoA. The NMAG then simply decapsulates those packets and delivers them to the mobile node. FMIPv4 [RFC4988] specifies forwarding when the mobile node uses the home address as its on-link address rather than the care-of address. The usage in PMIPv6 is similar to that in FMIPv4, where the address(es) used by the mobile node is/are based on its HNP(s). Since the NMAG can obtain the link-layer address (MN LL-ID) and HNP(s) via the HI message (also the interface identifier of the mobile node's link-local address (MN LLA-ID), if available), it can create a neighbor cache entry for the link-local address and the routes for the whole HNP(s), even before the mobile node performs Neighbor Discovery. For the uplink packets from the mobile node after handover in step (j), the NMAG forwards the packets to the PMAG through the tunnel established in step (f). The PMAG then decapsulates and sends them to the local mobility anchor.

The timing of the context transfer and that of packet forwarding may be different. Thus, a new flag 'F' and Option Code values for it in the HI and HAck messages are defined to request forwarding. To request buffering, the 'U' flag has already been defined in [RFC5568]. If the PMAG receives the HI message with the 'F' flag set, it starts forwarding packets for the mobile node. The HI message with the 'U' flag set MAY be sent earlier if the timing of buffering is different from that of forwarding. If packet forwarding is completed, the PMAG MAY send the HI message with the 'F' flag set and the Option Code value set to 2. Via this message, the ARs on both ends can tear down the forwarding tunnel synchronously.

The IP addresses in the headers of those user packets are summarized below:

In step (f),

Inner source address: IP address of the correspondent node

Inner destination address: HNP or Mobile Node's IPv4 Home Address (IPv4-MN-HoA)

Outer source address: IP address of the PMAG

Outer destination address: IP address of the NMAG

In step (i),

Source address: IP address of the correspondent node

Destination address: HNP or IPv4-MN-HoA

In step (j),

- from the mobile node to the NMAG,

  Source address: HNP or IPv4-MN-HoA

  Destination address: IP address of the correspondent node

- from the NMAG to the PMAG,

  Inner source address: HNP or IPv4-MN-HoA

  Inner destination address: IP address of the correspondent node

  Outer source address: IP address of the NMAG

  Outer destination address: IP address of the PMAG

- from the PMAG to the LMA,

  Inner source address: HNP or IPv4-MN-HoA

  Inner destination address: IP address of the correspondent node

  Outer source address: IP address of the PMAG

  Outer destination address: IP address of the LMA

In the case of the reactive handover for PMIPv6, since the mobile node does not send either the FBU or UNA, it would be more natural that the NMAG send the HI message to the PMAG after the mobile node has moved to the new link. The NMAG then needs to obtain the information of the PMAG beforehand. Such information could be provided, for example, by the mobile node sending the AP-ID on the old link and/or by the lower-layer procedures between the P-AN and N-AN. The exact method is not specified in this document. Figure 3 illustrates the reactive fast handover procedures for PMIPv6, where the bidirectional tunnel establishment is initiated by the NMAG.

```
                                         PMAG            NMAG
          MN       P-AN      N-AN        (PAR)           (NAR)     LMA
          |         |         |            |               |        |
     (a) ~~~        |         |            |               |        |
         ~~~        |         |            |               |        |
          |  MN-AN connection |       AN-MAG connection    |        |
     (b)  |<--establishment-->|<-------establishment------>|        |
          |         |         |(substitute for UNA and FBU)|        |
          |         |         |            |               |        |
          |         |         |            |               |        |
     (c)  |         |         |            |<-----HI-------|        |
          |         |         |            |               |        |
          |         |         |            |               |        |
     (d)  |         |         |            |-----HAck----->|        |
          |         |         |            |               |        |
          |         |         |            |               |        |
     (e)  |         |         |          #=|<=======================|
          |         |         |          #================>|=#      |
          |<====================DL data======================#      |
          |         |         |            |               |        |
     (f)  |=====================UL data===================>|=#      |
          |         |         |          #=|<================#      |
          |         |         |          #=========================>|
          |         |         |            |               |        |
     /    |         |         |            |               |        | \
     |(g) |         |         |            |               |--PBU-->| |
     |    |         |         |            |               |        | |
     |(h) |         |         |            |               |<--PBA--| |
     |    |<====================DL data====================|<=======| |
     |    |         |         |            |               |        | |
     \    |=====================UL data===================>|=======>| /
```

Figure 3: Reactive Fast Handover for PMIPv6 (Initiated by NMAG)

The detailed descriptions are as follows:

(a) The mobile node undergoes handover from the previous access network to the new access network.

(b) The mobile node establishes a connection (e.g., radio channel) with the new access network, which triggers the establishment of the connection between the new access network and new MAG. The MN ID is transferred to the new MAG at this step for the subsequent procedures. The AP-ID on the old link (Old AP ID), which will be provided by either the mobile node or the new access network, is also transferred to the new MAG to help identify the previous MAG on the new link. This can be regarded as a substitute for the UNA and FBU.

(c) The new MAG sends the HI message to the previous MAG. The HI message MUST have the 'P' flag set and include the MN ID. The Context Request option MAY be included to request additional context information on the mobile node to the previous MAG.

(d) The previous MAG sends the HAck message back to the new MAG with the 'P' flag set. The HAck message MUST include the HNP(s) and/or IPv4-MN-HoA that corresponds to the MN ID in the HI message and SHOULD include the MN LL-ID, only if it is valid (non-zero), and the local mobility anchor address that is currently serving the mobile node. The context information requested by the new MAG MUST be included. If the requested context is not available for some reason, the previous MAG MUST return the HAck message with the Code value 131. If the 'F' flag is set in the HI message at step (c) and forwarding is nevertheless not executable for some reason, the previous MAG MUST return the HAck message with the Code value 132.

(e) If the 'F' flag in the HI message is set at step (c), a bidirectional tunnel is established between the previous MAG and new MAG, and packets destined for the mobile node are forwarded from the previous MAG to the new MAG over this tunnel. After decapsulation, those packets are delivered to the mobile node via the new access network.

(f) The uplink packets from the mobile node are sent to the new MAG via the new access network, and the new MAG forwards them to the previous MAG. The previous MAG then sends the packets to the local mobility anchor that is currently serving the mobile node.

Steps (g)-(h) are the same as steps (k)-(l) in the predictive fast handover procedures.

In step (c), the IP address of the PMAG needs to be resolved by the NMAG to send the HI message to the PMAG. This information may come from the N-AN or some database that the NMAG can access.

4.2. Inter-AR Tunneling Operation

When the PMAG (PAR) or NMAG (NAR), depending on the fast handover mode, receives the HI message with the 'F' flag set, it prepares to send/receive the mobile node's packets to/from the other MAG and returns the HAck message with the same sequence number. Both MAGs SHOULD support the following encapsulation modes for the user packets, which are also defined for the tunnel between the local mobility anchor and MAG:

- o IPv4-or-IPv6-over-IPv6 [RFC5844]
- o IPv4-or-IPv6-over-IPv4 [RFC5844]
- o IPv4-or-IPv6-over-IPv4-UDP [RFC5844]
- o TLV-header UDP tunneling [RFC5845]
- o Generic Routing Encapsulation (GRE) tunneling with or without GRE key(s) [RFC5845]

The PMAG and the NMAG MUST use the same tunneling mechanism for the data traffic tunneled between them. The encapsulation mode to be employed SHOULD be configurable. It is RECOMMENDED that:

1. As the default behavior, the inter-MAG tunnel uses the same encapsulation mechanism as that for the PMIPv6 tunnel between the local mobility anchor and the MAGs. The PMAG and NMAG automatically start using the same encapsulation mechanism without a need for a special configuration on the MAGs or a dynamic tunneling mechanism negotiation between them.

2. Configuration on the MAGs can override the default mechanism specified in scenario #1 above. The PMAG and NMAG MUST be configured with the same mechanism, and this configuration is most likely to be uniform throughout the PMIPv6 domain. If the packets on the PMIPv6 tunnel cannot be uniquely mapped on to the configured inter-MAG tunnel, this scenario is not applicable, and scenario #3 below SHOULD directly be applied.

3. An implicit or explicit tunnel negotiation mechanism between the MAGs can override the default mechanism specified in scenario #1 above. The employed tunnel negotiation mechanism is outside the scope of this document.

The necessary information MUST be transferred in the HI/HAck messages to determine whether a mobile node's packets should be forwarded immediately or at a later time. Such information includes the HNP(s) (or IPv4-MN-HoA) and/or GRE key(s). In the case of GRE tunneling with GRE keys being used, for each mobility session, the NMAG selects the GRE key for the downlink packets, and the PMAG selects the GRE key for the uplink packets. These GRE keys are exchanged between the PMAG and the NMAG using the GRE Key option as described in [RFC5845]; e.g., in the case of the reactive mode as shown in Figure 3, the DL GRE key is communicated in the HI message while the UL GRE key is sent in the HAck message. In the case of downlink packets, the PMAG redirects the mobile node's packets from the local mobility anchor towards the NMAG, and if the mobile node is ready to receive those packets or the N-AN can handle them regardless of the state of the mobile node, the NMAG SHOULD immediately send them towards the N-AN; otherwise, it SHOULD buffer them until the mobile node is ready. In the case of uplink packets, the NMAG SHOULD reverse-tunnel them from the mobile node towards the PMAG, and the PMAG will then send them to the local mobility anchor.

When the PMAG or NMAG receives the HI message with the 'U' flag set, it prepares to buffer the mobile node's packets and returns the HAck message with the same sequence number. It MUST be followed by another HI message with the 'F' flag set at an appropriate time to forward the buffered packets.

If the MAG that received the HI message encounters an erroneous situation (e.g., insufficient buffer space), it SHOULD immediately send the HAck message with the cause of the error and cancel all tunneling operations.

4.3. IPv4 Support Considerations

The motivation and usage scenarios of IPv4 protocol support by PMIPv6 are described in [RFC5844]. The scope of IPv4 support covers the following two features:

- o IPv4 Home Address Mobility Support, and
- o IPv4 Transport Support.

As for IPv4 Home Address Mobility Support, the mobile node acquires the IPv4 Home Address (IPv4-MN-HoA), and in the case of handover, the PMAG needs to transfer IPv4-MN-HoA to the NMAG, which is the inner destination address of the packets forwarded on the downlink. For this purpose, the IPv4 Address option described in Section 6.2.7 is used. In order to provide IPv4 Transport Support, the NMAG needs to know the IPv4 address of the local mobility anchor (IPv4-LMAA) to send PMIPv6 signaling messages to the local mobility anchor in the IPv4 transport network. For this purpose, a new option called the LMA Address (LMAA) option is defined in Section 6.2.2 so as to convey IPv4-LMAA from the PMAG to the NMAG.

5. PMIPv6-Related Fast Handover Issues

5.1. Manageability Considerations

This specification does not require any additional IP-level functionality on the local mobility anchor and the mobile node running in the PMIPv6 domain. A typical network interface that the mobile node could be assumed to have is one with the cellular network, where the network controls the movement of the mobile node. Different types of interfaces could be involved, such as different generations (3G and 3.9G) or different radio access systems. This specification supports a mobile node with the single radio mode, where only one interface is active at any given time. The assigned IP address is preserved whether the physical interface changes or not, and the mobile node can identify which interface should be used if there are multiple ones.

5.2. Expedited Packet Transmission

The protocol specified in this document enables the NMAG to obtain parameters that would otherwise be available only by communicating with the local mobility anchor. For instance, the HNP(s) and/or IPv4-MN-HoA of a mobile node are made available to the NMAG through context transfer. This allows the NMAG to perform some procedures that may be beneficial. The NMAG, for example, SHOULD send a Router Advertisement (RA) with prefix information to the mobile node as soon as its link attachment is detected (e.g., via receipt of a Router Solicitation message). Such an RA is recommended, for example, in scenarios where the mobile node uses a new radio interface while attaching to the NMAG; since the mobile node does not have information regarding the new interface, it will not be able to immediately send packets without first receiving an RA with HNP(s). Especially in the reactive fast handover, the NMAG gets to know the HNP(s) assigned to the mobile node on the previous link at step (d) in Figure 3. In order to reduce the communication disruption time, the NMAG SHOULD expect the mobile node to keep using the same HNP and to send uplink packets before that step upon the mobile node's request. However, if the HAck message from the PMAG returns a different HNP or the subsequent PMIPv6 binding registration for the HNP fails for some reason, then the NMAG MUST withdraw the advertised HNP by sending another RA with zero prefix lifetime for the HNP in question. This operation is the same as that described in Section 6.12 of [RFC5213].

The protocol specified in this document is applicable regardless of whether link-layer addresses are used between a mobile node and its MAG. A mobile node should be able to continue sending packets on the uplink even when it changes link. When link-layer addresses are used, the mobile node performs Neighbor Unreachability Detection (NUD) [RFC4861], after attaching to a new link, probing the reachability of its default router. The new router should respond to the NUD probe, providing its link-layer address in the solicited Neighbor Advertisement, which is common in the PMIPv6 domain. Implementations should allow the mobile node to continue to send uplink packets while it is performing NUD.

6. Message Formats

This document defines new Mobility Header messages for the extended HI and HAck, and new mobility options for conveying context information.

6.1. Mobility Header

6.1.1. Handover Initiate (HI)

This section defines extensions to the HI message in [RFC5568]. The format of the Message Data field in the Mobility Header is as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                +-------------------------------+
                                |          Sequence #           |
+-+-+-+-+-------+---------------+-------------------------------+
|S|U|P|F|Resv'd |      Code     |                               |
+-+-+-+-+-------+---------------+                               |
|                                                               |
.                                                               .
.                       Mobility options                        .
.                                                               .
|                                                               |
+---------------------------------------------------------------+
(Note: P=1)
```

IP Fields:

Source Address

The IP address of the PMAG or NMAG

Destination Address

The IP address of the peer MAG

Message Data:

Sequence # Same as [RFC5568].

'S' flag Defined in [RFC5568], and MUST be set to zero in this specification.

'U' flag Buffer flag. Same as [RFC5568].

'P' flag   Proxy flag. Used to distinguish the message from that defined in [RFC5568], and MUST be set in all new message formats defined in this document when using this protocol extension.

'F' flag   Forwarding flag. Used to request to forward the packets for the mobile node.

Reserved   Same as [RFC5568].

Code   [RFC5568] defines this field and its values, 0 and 1. In this specification, with the 'P' flag set, this field can be set to zero by default, or to the following values:

2: Indicate the completion of forwarding

3: All available context transferred

Code value 3 is set when the transfer of all necessary context information is completed with this message. This Code value is used both in cases where the context information is fragmented into several pieces and the last fragment is contained in this message, and where the whole information is transferred in one piece.

Mobility options:

This field contains one or more mobility options, whose encoding and formats are defined in [RFC3775].

Required option

In order to uniquely identify the target mobile node, the mobile node identifier MUST be contained in the Mobile Node Identifier option.

The transferred context MUST be for one mobile node per message. In addition, the NMAG can request necessary mobility options via the Context Request option defined in this document.

Context Request Option

This option MAY be present to request context information, typically by the NMAG to the PMAG in the NMAG-initiated fast handover.

6.1.2. Handover Acknowledge (HAck)

This section defines extensions to the HAck message in [RFC5568]. The format of the Message Data field in the Mobility Header is as follows:

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                 +-------------------------------+
                                 |          Sequence #           |
 +-+-+-+-+---------+---------------+-------------------------------+
 |U|P|F|Reserved |      Code     |                               |
 +-+-+-+-+---------+---------------+                               |
 |                                                               |
 .                                                               .
 .                       Mobility options                        .
 .                                                               .
 |                                                               |
 +---------------------------------------------------------------+
 (Note: P=1)
```

IP Fields:

Source Address

Copied from the destination address of the Handover Initiate message to which this message is a response.

Destination Address

Copied from the source address of the Handover Initiate message to which this message is a response.

Message Data:

The usages of Sequence # and Reserved fields are exactly the same as those in [RFC5568].

'U' flag   Same as defined in Section 6.1.1.

'P' flag   Same as defined in Section 6.1.1. Used to distinguish the message from that defined in [RFC5568], and MUST be set in all new message formats defined in this document when using this protocol extension.

'F' flag   Same as defined in Section 6.1.1.

Code Code values 0 through 4 and 128 through 130 are defined in [RFC5568]. When the 'P' flag is set, the meaning of Code value 0 is as defined in this specification; 128 through 130 are reused; and 5, 6, 131, and 132 are newly defined.

0: Handover Accepted or Successful

5: Context Transfer Accepted or Successful

6: All available Context Transferred

128: Handover Not Accepted, reason unspecified

129: Administratively prohibited

130: Insufficient resources

131: Requested Context Not Available

132: Forwarding Not Available

Mobility options:

This field contains one or more mobility options, whose encoding and formats are defined in [RFC3775]. The mobility option that uniquely identifies the target mobile node MUST be copied from the corresponding HI message, and the transferred context MUST be for one mobile node per message.

Required option(s)

All the context information requested by the Context Request option in the HI message SHOULD be present in the HAck message. The other cases are described below.

In the case of the PMAG-initiated fast handover, when the PMAG sends the HI message to the NMAG with the context information and the NMAG successfully receives it, the NMAG returns the HAck message with Code value 5. In the case of the NMAG-initiated fast handover, when the NMAG sends the HI message to the PMAG with or without the Context Request option, the PMAG returns the HAck message with the requested or default context information (if any). If all available context information is transferred, the PMAG sets the Code value in the HAck message to 6. If more context information is available, the PMAG sets the Code value in the HAck message to 5, and the NMAG MAY send new HI message(s) to retrieve the rest of the available context information. If none of the requested context information is available, the PMAG returns the HAck message with Code value 131 without any context information.

6.2. Mobility Options

6.2.1. Context Request Option

This option is sent in the HI message to request context information on the mobile node. If a default set of context information is defined and always sufficient, this option is not used. This option is more useful to retrieve additional or dynamically selected context information.

The Context Request option is typically used for the reactive (NMAG-initiated) fast handover mode to retrieve the context information from the PMAG. When this option is included in the HI message, all the requested context information SHOULD be included in the HAck message in the corresponding mobility option(s) (e.g., HNP, LMAA, or MN LL-ID mobility options).

The default context information to request is the Home Network Prefix option. If the Mobile Node link layer is available and used, the Mobile Node Link-layer Identifier option MUST also be requested.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+---------------+---------------+---------------+---------------+
|  Option-Type  | Option-Length |           Reserved            |
+---------------+---------------+-------------------------------+
|  Req-type-1   | Req-length-1  |  Req-type-2   | Req-length-2  |
+---------------------------------------------------------------+
|  Req-type-3   | Req-length-3  |         Req-option-3          |
+---------------------------------------------------------------+
|                              ...                              |
```

Option-Type 40

Option-Length The length in octets of this option, not including the Option Type and Option Length fields.

Reserved This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Req-type-n The type value for the nth requested option.

Req-length-n The length of the nth requested option, excluding the Req-type-n and Req-length-n fields.

Req-option-n The optional data to uniquely identify the requested context for the nth requested option.

In the case where there are only Req-type-n and Req-length-n fields, the value of Req-length-n is set to zero. If additional information besides Req-type-n is necessary to uniquely specify the requested context, such information follows after Req-length-n. For example, when the requested contexts start with the HNP option (type=22), the MN Link-layer ID option (type=25), and the Vendor-Specific option (type=19), the required option format looks as follows:

```
|                              ...                              |
+---------------+---------------+---------------+---------------+
|Option-Type=CRO| Option-Length |           Reserved            |
+---------------+---------------+---------------+---------------+
| Req-type-n=22 | Req-length-n=0| Req-type-n=25 | Req-length-n=0|
+---------------+---------------+-------------------------------+
| Req-type-n=19 | Req-length-n=5|           Vendor-ID           |
+-------------------------------+---------------+---------------+
|           Vendor-ID           |   Sub-Type    |               |
+-----------------------------------------------+               |
|                              ...                              |
```

Note: CRO = Context Request Option

The first two options can uniquely identify the requested contexts (i.e., the HNP and MN Link-layer ID) by the Req-type, so the Req-length is set to zero; however, the subsequent Vendor-Specific option further needs the Vendor-ID and Sub-Type to identify the requested context, so these parameters follow, and the Req-length is set to 5. Note that the exact values in the Vendor-ID and Sub-Type follow [RFC5094].

6.2.2. Local Mobility Anchor Address (LMAA) Option

This option is used to transfer the Local Mobility Anchor IPv6 Address (LMAA) or its IPv4 Address (IPv4-LMAA) with which the mobile node is currently registered. The detailed definition of the LMAA is described in [RFC5213].

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |  Option-Type  | Option-Length |  Option-Code  |   Reserved    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |              Local Mobility Anchor Address ...                |
```

Option-Type 41

Option-Length 18 or 6

Option-Code 0 Reserved

1 IPv6 address of the local mobility anchor (LMAA)

2 IPv4 address of the local mobility anchor (IPv4-LMAA)

Reserved This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Local Mobility Anchor Address

If the Option-Code is 1, the LMA IPv6 address (LMAA) is inserted. If the Option-Code is 2, the LMA IPv4 address (IPv4-LMA) is inserted.

6.2.3. Mobile Node Link-Local Address Interface Identifier (MN LLA-IID) Option

This option is used to transfer the interface identifier of the mobile node’s IPv6 Link-local Address that is used in the P-AN. In deployments where the interface identifier is assigned by the network or is known to the network, this option is used to transfer this identifier from the PMAG to the NMAG.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | Option-Type   | Option-Length |            Reserved           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    +                     Interface Identifier                      +
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Option-Type 42

Option-Length 10

Reserved This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Interface Identifier

The Interface Identifier value used for the mobile node's IPv6 Link-local address in the P-AN.

6.2.4. Home Network Prefix Option

This option, as defined in [RFC5213], is used to transfer the home network prefix that is assigned to the mobile node in the P-AN.

6.2.5. Link-Local Address Option

This option, as defined in [RFC5213], is used to transfer the link-local address of the PMAG.

6.2.6. GRE Key Option

This option is used to transfer the GRE Key for the mobile node's data flow over the bidirectional tunnel between the PMAG and NMAG. The message format of this option follows that of the GRE Key option defined in [RFC5845]. The GRE Key value uniquely identifies each flow, and the sender of this option expects to receive packets of the flow from the peer AR with this value.

6.2.7. IPv4 Address Option

As described in Section 4.3, if the mobile node runs in IPv4-only mode or dual-stack mode, it requires the IPv4 home address (IPv4-MN-HoA). This option is used to transfer the IPv4 home address if assigned on the previous link. The format of this option follows that of the IPv4 Home Address Request option defined in [RFC5844].

6.2.8. Vendor-Specific Mobility Option

This option is used to transfer any other information defined in this document. The format and used values of this option follow those of the Vendor-Specific Mobility option defined in [RFC5094].

7. Security Considerations

Security issues for this document follow those for PMIPv6 [RFC5213] and FMIPv6 [RFC5568]. In PMIPv6, the MAG and local mobility anchor are assumed to share security associations. In FMIPv6, the access routers (i.e., the PMAG and NMAG in this document) are assumed to share security associations.

The Handover Initiate (HI) and Handover Acknowledge (HAck) messages exchanged between the PMAG and NMAG MUST be protected using end-to-end security association(s) offering integrity and data origin authentication. The PMAG and the NMAG MUST implement IPsec [RFC4301] for protecting the HI and HAck messages. IPsec Encapsulating Security Payload (ESP) [RFC4303] in transport mode with mandatory integrity protection SHOULD be used for protecting the signaling messages. Confidentiality protection SHOULD be used if sensitive context related to the mobile node is transferred.

IPsec ESP [RFC4303] in tunnel mode SHOULD be used to protect the mobile node’s packets at the time of forwarding if the link between the PMAG and NMAG exposes the mobile node’s packets to more threats than if they had followed their normal routed path.

8. IANA Considerations

This document defines new flags and status codes in the HI and HAck messages, as well as three new mobility options. The Type values for these mobility options are assigned from the same numbering space as that allocated for the other mobility options defined in [RFC3775]. Those for the flags and status codes are assigned from the corresponding numbering space defined in [RFC5568], and have been created as new tables in the IANA registry (marked with asterisks). New values for these registries can be allocated by Standards Action or IESG approval [RFC5226].

Mobility Options

Value	Description	Reference
40	Context Request Option	Section 6.2.1
41	Local Mobility Anchor Address Option	Section 6.2.2
42	Mobile Node Link-local Address Interface Identifier Option	Section 6.2.3

Handover Initiate Flags (*)
Registration Procedures: Standards Action or IESG Approval

Flag	Value	Description	Reference
S	0x80	Assigned Address Configuration flag	[RFC5568]
U	0x40	Buffer flag	[RFC5568]
P	0x20	Proxy flag	Section 6.1.1
F	0x10	Forwarding flag	Section 6.1.1

Handover Acknowledge Flags (*)
Registration Procedures: Standards Action or IESG Approval

Flag	Value	Description	Reference
U	0x80	Buffer flag	Section 6.1.2
P	0x40	Proxy flag	Section 6.1.2
F	0x20	Forwarding flag	Section 6.1.2

Handover Initiate Status Codes (*)
Registration Procedures: Standards Action or IESG Approval

Code	Description	Reference
0	FBU with the PCoA as source IP address	[RFC5568]
1	FBU whose source IP address is not PCoA	[RFC5568]
2	Indicate the completion of forwarding	Section 6.1.1
3	All available context transferred	Section 6.1.1
4-255	Unassigned	

Handover Acknowledge Status Codes (*)
Registration Procedures: Standards Action or IESG Approval

Code	Description	Reference
0	Handover Accepted or Successful (when 'P' flag is set)	Section 6.1.2
	Handover Accepted with NCoA valid	[RFC5568]
1	Handover Accepted, NCoA not valid	[RFC5568]
2	Handover Accepted, NCoA assigned	[RFC5568]
3	Handover Accepted, use PCoA	[RFC5568]
4	Message sent unsolicited	[RFC5568]
5	Context Transfer Accepted or Successful	Section 6.1.2
6	All available Context Transferred	Section 6.1.2
7-127	Unassigned	
128	Handover Not Accepted, reason unspecified	[RFC5568]
129	Administratively prohibited	[RFC5568]
130	Insufficient resources	[RFC5568]
131	Requested Context Not Available	Section 6.1.2
132	Forwarding Not Available	Section 6.1.2
133-255	Unassigned	

9. Acknowledgments

The authors would like to specially thank Vijay Devarapalli and Sri Gundavelli for their thorough reviews of this document.

The authors would also like to thank Charlie Perkins, Desire Oulai, Ahmad Muhanna, Giaretta Gerardo, Domagoj Premec, Marco Liebsch, Fan Zhao, Julien Laganier, and Pierrick Seite for their passionate discussions in the MIPSHOP working group mailing list.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC5094] Devarapalli, V., Patel, A., and K. Leung, "Mobile IPv6 Vendor Specific Option", RFC 5094, December 2007.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5568] Koodli, R., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

[RFC5845] Muhanna, A., Khalil, M., Gundavelli, S., and K. Leung, "Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6", RFC 5845, June 2010.

10.2. Informative References

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4988] Koodli, R. and C. Perkins, "Mobile IPv4 Fast Handovers", RFC 4988, October 2007.

Appendix A. Applicable Use Cases

A.1. PMIPv6 Handoff Indication

PMIPv6 [RFC5213] defines the Handoff Indicator option and also describes the type of handoff and values that can be set for this option. This document proposes one approach to determining the handoff type by the NMAG when the handoff of the mobile node is executed.

According to [RFC5213], the following handoff types are defined:

0) Reserved

1) Attachment over a new interface

2) Handoff between two different interfaces of the mobile node

3) Handoff between mobile access gateways for the same interface

4) Handoff state unknown

5) Handoff state not changed (Re-registration)

Assuming that there is a valid MN Link-layer Identifier (MN LL-ID), the following solution can be considered. When the NMAG receives the MN LL-ID from the PMAG in the MN LL-ID option via the HI or HAck message, the NMAG compares it with the new MN LL-ID that is obtained from the mobile node in the N-AN. If these two MN LL-IDs are the same, the handoff type falls into type 3 (defined above) and the Handoff Indicator value is set to 3. If these two MN LL-IDs are different, the handoff is likely to be type 2 (defined above) since the HI/HAck message exchange implies that this is a handoff rather than a multihoming, and therefore the Handoff Indicator value can be set to 2. If there is no HI/HAck exchange performed prior to the network attachment of the mobile node in the N-AN, the NMAG may infer that this is a multi-homing case and set the Handoff Indicator value to 1. In the case of re-registration, the MAG, to which the mobile node is attached, can determine if the handoff state is not changed, so the MAG can set the HI value to 5 without any additional information. If no handoff type can be assumed or if there is no valid MN LL-ID available, the NMAG may set the value to 4.

A.2. Local Routing

As described in Section 6.10.3 of [RFC5213], if the EnableMAGLocalRouting flag is set, when two mobile nodes are attached to one MAG, the traffic between them may be locally routed. If one mobile node moves from this MAG (PMAG) to another MAG (NMAG) and if the PMAG does not detect the mobile node's detachment, it will continue to forward packets locally forever. This situation is more likely to happen in the reactive fast handover with Wireless Local Area Network (WLAN) access, which does not have the capability to detect the detachment of the mobile node in a timely manner. This specification can be applied to handle this case. When the mobile node attaches to the NMAG, the NMAG sends the HI message to the PMAG with the 'F' flag set, which makes the PMAG realize the detachment of the mobile node and establish the inter-MAG tunnel. The PMAG immediately stops the local routing and sends the packets for the mobile node to the NMAG via that tunnel; the packets are then delivered to the mobile node on the new link.

Authors' Addresses

Hidetoshi Yokota
KDDI Lab
2-1-15 Ohara, Fujimino
Saitama 356-8502
Japan

EMail: yokota@kddilabs.jp

Kuntal Chowdhury
Cisco Systems
30 International Place
Tewksbury, MA 01876
USA

EMail: kchowdhu@cisco.com

Rajeev Koodli
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
USA

EMail: rkoodli@cisco.com

Basavaraj Patil
Nokia
6000 Connection Drive
Irving, TX 75039
USA

EMail: basavaraj.patil@nokia.com

Frank Xia
Huawei USA
1700 Alma Dr. Suite 500
Plano, TX 75075
USA

EMail: xiayangsong@huawei.com