Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 7, 2012

Zhengming. Ma
Ke. Wang
Fei. Zhang
SUN YAT-SEN UNIVERSITY
January 4, 2012

Network-based Inter-domain handover Support for Proxy Mobile IPv6
draft-ma-netext-pmip-handover-02.txt

Abstract

[RFC5213] prompts the Inner-domain handover of the MN in Proxy Mobile IPv6(PMIPv6).This document describes network-based Inter-domain handover functionality and corresponding mobility options for PMIPv6.This document strictly abides by the three principle describes in PMIPv6:

(a)The movement of MN is transparent to CN.

(b)MN doesn't participate in any mobility-related signaling.LMA and MAG are responsible for managing IP mobility on behalf of the host.

(c)This document is compatible with RFC5213.

The points of this document are as follows:

(1) Concepts: The MN's Home Agent(HA) ,Home Address (HoA) and Care-of address(CoA) is not only for user but also for the specific session.MN initiating a session uses the address assigned by the LMA which the MN is registered at the moment as the HoA for the session.The user initiating a session uses the address assigned by the LMA which the MN moves to as the CoA for the session.

(2) Binding Cache:Every local mobility anchor must maintain two Binding Cache entries for each currently registered mobile node. One is Inner-domain BCE,the other is Inter-domain BCE. Inner-domain BCE maintains the binding between MN's Proxy-CoA and MN's HoA. Inter-domain BCE maintains the bingding between CN's HoA and CN's CoA.

(3)Communication:For the user initiating a session or accepting a session,no matter how it moves,the HoA for the session is unchanged,the source address of the data packets is the user's own HoA,and the destination address of the the data packets is the HoA of CN.The local mobility anchor will check all the packets received from the mobile access gateway.If both the source address of the data packets is the MN's HoA recorded in Inner-domain BCE,and the CN's HoA and CoA recorded in Inter-domain BCE are the same,the LMA will route

the packets directly to CN as described in RFC5213.Otherwise, according to looking up the Inter-domain BCE,LMA gets the CoA of CN. Then ,LMA encapsulates the packets to route to CN.On receiving a packet from a correspondent node with the destination address matching a mobile node's home network prefix(es), the CN's LMA MUST first check the source address and the destination address of the data packets,if the source address of the data packets is MN's HoA recorded in Inter-domain BCE and the destination address is CN's HoA recorded in Inner-domain BCE ,the CN'LMA will forward the packets to the right MAG directly as described in RFC5213.Otherwise, CN'LMA will remove the outer header before forwarding the packet. Then,LMA looks up the Inner-domain BCE to forward the packets to the right MAG.

(4)Updates:When MN moves to visited LMA(MN-vLMA),MN-vLMA will do three things.

Firstly MN-vLMA will assign a MN-CoA for MN and build up the Inner-domain BCE for MN. Secondly,MN-vLMA will sends message to MN-hLMA to get the HoA of CN .Then,MN-vLMA builds up the binding between CN-HoA and CN-HoA in the Inter-domain BCE.Thirdly, MN-vLMA sends message to CN-LMA wiht the MN-CoA and MN-HoA included in the message to help CN-LMA updating the Inter-domain BCE for MN.

Compared with "draft-ma-netext-pmip-handover-00.txt", this document is compatible with RFC5213 and the LMA described in this document should decide if it is necessary to encapsulate the packets.In other word,if MN and CN are both in their home domain,they will communicate just as the way described in RFC5213 and otherwise they will communicate in the way described in this document.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on July 7, 2012.

Copyright Notice

Table of Contents

1. Introduction

Proxy Mobile IPv6 (PMIPv6) [RFC5213] is network based mobility management protocol which allows IP mobility session continuity for a Mobile Node (MN) without its involvement in mobility management signaling. In RFC5213 the inter-domain handover is not involved.This document describes the network-based Inter-domain handover options, and the corresponding functionality for Inter-domain handover for PMIPv6. The Inter-domain handover takes place during MN moves from home LMA(hLMA) to visited LMA(vLMA).

The network-based Inter-domain handover functionality described in this specification does not depend on information provisioned to external entities, such as the Domain Name System (DNS) or the Authentication,Authorization and Accounting (AAA) infrastructure. The trust relationship and coordination management between LMAs within a PMIPv6 domain is deployment specific and will be described in this specification.

2. Requirements and Terminology

2.1. Requirements

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].

2.2. Terminology

In addition to the terminology defined in [RFC5213], the following terminology is also used:

hLMA

Home Local Mobility Anchor is the first LMA the MN registered and is the home agent for the mobile node in a Proxy Mobile IPv6 domain. It is the topological anchor point for the mobile node's home network prefix(es) and is the entity that manages the mobile node's binding state. The local mobility anchor has the functional capabilities of a home agent as defined in Mobile IPv6 base specification [RFC3775] with the additional capabilities required for supporting Proxy Mobile IPv6 protocol as defined in this specification.

vLMA

The vLMA is the LMA the MN visited.

rPBU

A request message sent by a mobile access gateway to a mobile node's local mobility anchor for establishing a binding between the mobile node's home network prefix(es) assigned to a given interface of a mobile node and its current care-of address (Proxy-CoA).

rPBA

A reply message sent by a local mobility anchor in response to a Proxy Binding Update message that it received from a mobile access gateway.

pPBU

A request message sent from a LMA to another LMA. There are two kinds of message formats:a message sent from vLMA to hLMA and a message sent from vLMA to CN's LMA.

pPBA

A reply message sent from a LMA to another LMA. There are two kinds

of message formats:a message sent from hLMA to vLMA and a message sent from CN's LMA to vLMA.

Home AAA (hAAA):

An Authentication, Authorization, and Accounting (AAA) server located in MN's home network. In scope of this document the hAAA corresponds to a RADIUS server that includes the role of the PMIPv6 Policy Store.

Visited AAA (vAAA):

An Authentication, Authorization, and Accounting (AAA) server located in MN's visited network. In this document the vAAA is the AAA server that acts as a RADIUS Proxy when the MN moves or attaches through the Visited network. The VAAA receives an authentication (or accounting) request from an AAA client such as a NAS, forwards the request to the hAAA server, receives the reply from the hAAA, and sends that reply back to the AAA client potentially adding changes to reflect local administrative policy.

3. The assumptions on the PMIPv6 domain

They are discussed here as they have an impact on PMIPv6 deployment.

Home AAA server records the user's static and dynamic information,and

the dynamic information includes the information of LMA which the MN is registered right now.

The MN's Home Address (HoA) and Care-of address(CoA) is not only for user but also for the specific session.

MN initiating a session uses the address assigned by the LMA which the MN is registered as the HoA for the session.The user initiating a session uses the address assigned by the LMA which the MN moves to as the CoA for the session.

CN accepting a session uses the address assigned by the LMA which the CN is registered as the HoA for the session.CN accepting a session uses the address assigned by the LMA which the CN moves to as the CoA for the session.

For the user initiating a session or accepting a session,no matter how it moves,the HoA for the session is unchanged,while the CoA for the session is changing.Then, the source address of the data packets sent by a user initiating a session or accepting a session is the user's own HoA,and the destination address of the the data packets is the HoA of the other end of the session.

The network-based Inter-domain handover Management not only ensures the continuity in the session but also ensures that the MN will not detect any change with respect to CN.

This specification diverses the PBU/PBA message into two kinds of message formate: pPBU/pPBA message between LMAs ,rPBU/rPBA message between LMA and MAG.

4. Local Mobility Anchor Operation

The local mobility anchor MUST support the home agent function as defined in [RFC3775] and the extensions defined in this specification. A home agent with these modifications and enhanced capabilities for supporting the Proxy Mobile IPv6 protocol is referred to as a local mobility anchor.This section describes the operational details of the local mobility anchor.

4.1. Home address configuration

LMA not only assignes the network prefix of the home address for the new users , but also configures the home address for the new users.So that LMA can performs mobility management on behalf of a mobile node.

4.2. Binding Cache Entry Data in LMA

Every local mobility anchor MUST maintain two Binding Cache entries for each currently registered mobile node. One is Inner-domain BCE,the other is Inter-domain BCE. Inner-domain BCE maintains the binding between MN's Proxy-CoA and MN's HoA. Inter-domain BCE maintains the bingding between CN's HoA and CN's CoA.

4.3. Forwarding Considerations

LMA should intercepts the packets sent to the Mobile Node's Home Network:When the local mobility anchor is serving a mobile node, it MUST be able to receive packets that are sent to the mobile node's home network. In order for it to receive those packets, it MUST advertise a connected route in to the Routing Infrastructure for the mobile node's home network prefix(es) or for an aggregated prefix with a larger scope. This essentially enables IPv6 routers in that network to detect the local mobility anchor as the last-hop router for the mobile node's home network prefix(es).

4.3.1. Forwarding Packets Sent by the Mobile Node

The local mobility anchor will check all the packets received from the mobile access gateway.If both the source address of the data packets is the MN's HoA recorded in Inner-domain BCE,and the CN's HoA and CoA recorded in Inter-domain BCE are the same,the LMA will route the packets directly to CN as described in RFC5213.Otherwise, according to looking up the Inter-domain BCE,LMA gets the CoA of CN. Then ,LMA encapsulates the packets to route to CN. The format of the tunneled packet is shown below:

IPv6 header (src= LMAA, dst= CN's CoA) /* Tunnel Header */

IPv6 header (src= MN's HoA, dst= CN's HoA) /* Packet Header */

Upper layer protocols /* Packet Content*/

4.3.2. Forwarding Packets to the Mobile Node:

On receiving a packet from a correspondent node with the destination address matching a mobile node's home network prefix(es), the LMA MUST first check the source address and the destination address of the data packets,if the source address of the data packets is CN's HoA recorded in Inter-domain BCE and the destination address is MN's HoA recorded in Inner-domain BCE ,the LMA will forward the packets to the right MAG directly as described in RFC5213.Otherwise, LMA will remove the outer header before forwarding the packet. Then,LMA looks up the Inner-domain BCE to forward the packets to the right MAG. The

format of the tunneled packet is shown below:

IPv6 header (src= LMAA, dst= MN's Proxy CoA) /* Tunnel Header */

IPv6 header (src= CN's HoA, dst= MN's HoA) /* Packet Header */

Upper layer protocols /* Packet Content*/

5. Mobile Access Gateway Operation

RFC5213 introduces a new functional entity, the mobile access gateway (MAG).The mobile access gateway is the entity that is responsible for detecting the mobile node's movements to and from the access link and sending the Proxy Binding Update messages to the local mobility anchor. In essence, the mobile access gateway performs mobility management on behalf of a mobile node.

Every mobile access gateway MUST maintain a Binding Update List.Each entry in the Binding Update List represents a mobile node's mobility binding with its local mobility anchor. The Binding Update List is a conceptual data structure.

For supporting this specification, the conceptual Binding Update List entry data structure needs be extended as follows:

(a)After detecting a new mobile node on its access link, the mobile access gateway MUST identify the mobile node and acquire its MN-Identifier. If it determines that the network-based mobility management service needs to be offered to the mobile node, it MUST send a Proxy Binding Update message to the local mobility anchor.

(b)If the MAG detectes the MN's registration is initial binding registration , the MAG will maintain a binding between MN's HoA and hLMA when it recieves the rPBA message.

(c)If the MAG detectes the MN is performing a inter-domain handover , the MAG will maintain a binding between MN's HoA ,vLMA and CoA when it recieves the rPBA message from vLMA. The CoA which is included in rPBA message is the address vLMA assigns for MN.

6. Protocol Operation

In order to improve the performance during inter-handover (when operations such as attachment to a new LMA and signaling between LMAs are involved), the PFMIPv6 protocol in this document specifies new message forms between the MN's hLMA and MN's vLMA and new message

forms between the MN's vLMA and CN's LMA. In this specification take the communication between MN and CN as a example. Both MN and CN are in PMIPv6 domain.

6.1. Initial Binding Registration and Forwarding Considerations

Both MN and CN are in PMIPv6 domain.The related signaling of Initial Binding Registration is described in RFC5213. Both MN and CN has registered in its hLMA ,and both gets its home address (MN-HoA and CN-HoA).The reference network is illustrated in Figure 1.

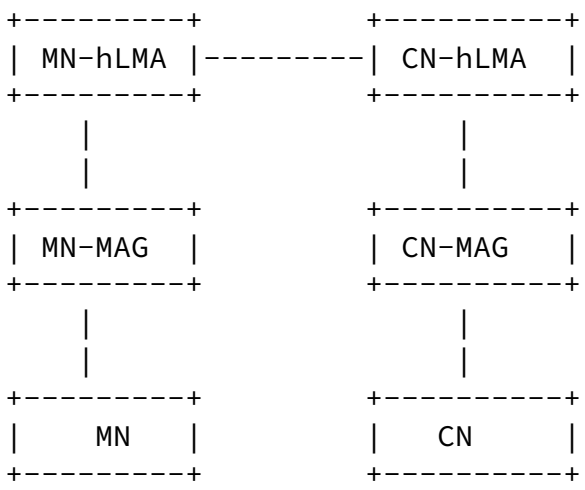


Figure 1:Reference network for Initial Binding Registration and Forwarding Considerations

Forwarding Considerations:

(a) Packets from MN to CN:

(1).The source address is MN-HoA, and the destination address is CN-HoA.

(2).The packets are forwarded from MN to MN-MAG through Link-layer.

(3).The packets are forwarded form MN-MAG to MN-hLMA through tunnel, the source address of the tunnel is MN-MAG's IP address (MN-Proxy-CoA), and the destination address of the tunnel is MN-hLMA's address (MN-hLMAA).

(4).MN-hLMA decapsulates the packets and check both the source address and the destination address of the data packets.If both the

source address of the data packets is the MN's HoA recorded in Inner-domain BCE,and the CN's HoA and CoA recorded in Inter-domain BCE are

the same,the LMA will route the packets directly to CN as described in RFC5213.

(5)The packets are intercepted by CN-hLMA.CN-hLMA MUST first check the source address and the destination address of the data packets,if the source address of the data packets is MN's HoA recorded in Inter-domain BCE and the destination address is CN's HoA recorded in Inner-domain BCE ,the CN-hLMA forwards the packets to the right MAG directly as described in RFC5213.CN-hLMA forwards them to CN-MAG through tunnel, the source address of the tunnel is CN-hLMA's address (CN-hLMAA), and the destination address of the tunnel is CN-MAG's address (CN-Proxy-CoA).

(6)CN-MAG decapsulates the packets and forwards them to CN through Link-layer.

(b) Packets from CN to MN:

(1).The source address is CN-HoA , and the destination address is MN-HoA .

(2).The packets are forwarded from CN to CN-MAG through Link-layer.

(3).The packets are forwarded form CN-MAG to CN-hLMA through tunnel, the source address of the tunnel is CN-Proxy-CoA and the destination address of the tunnel is CN-hLMAA.

(4).CN-hLMA decapsulates the packets and check both the source address and the destination address of the data packets.If both the source address of the data packets is the CN's HoA recorded in Inner-domain BCE,and the MN's HoA and CoA recorded in Inter-domain BCE are the same,the LMA will route the packets directly to CN as described in RFC5213.

(5). The packets are intercepted by MN-hLMA.The packets are intercepted by MN-hLMA.MN-hLMA MUST first check the source address and the destination address of the data packets,if the source address of the data packets is CN's HoA recorded in Inter-domain BCE and the destination address is MN's HoA recorded in Inner-domain BCE ,the MN-

hLMA forwards the packets to the right MAG directly as described in RFC5213.

(6).MN-MAG decapsulates the packets and forwards them to MN through Link-layer.

6.2. MN Performs Inter-domain handover

On the basis of situation described in 6.1,MN roams to MN-vLMA domain and CN is still in its home domain.The reference network is illustrated in Figure 2.

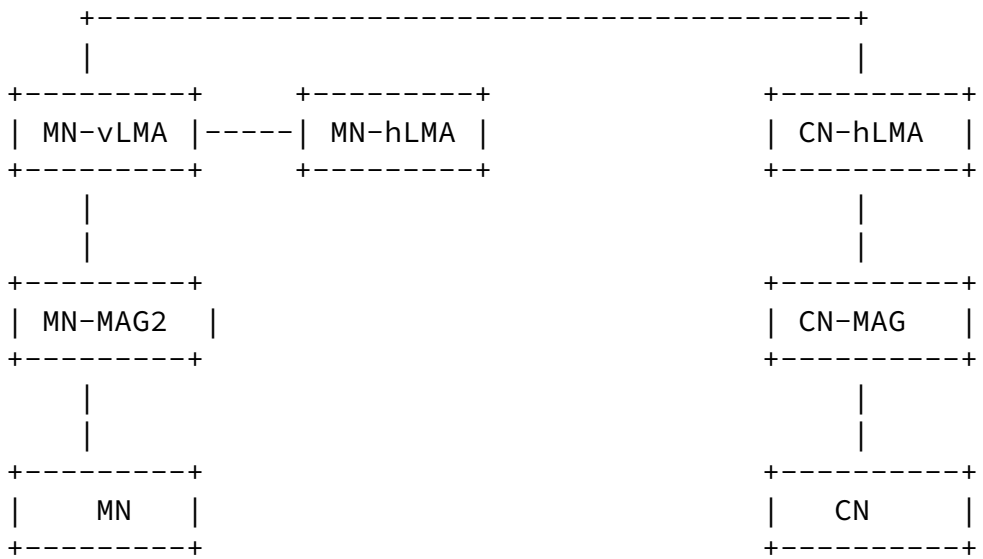
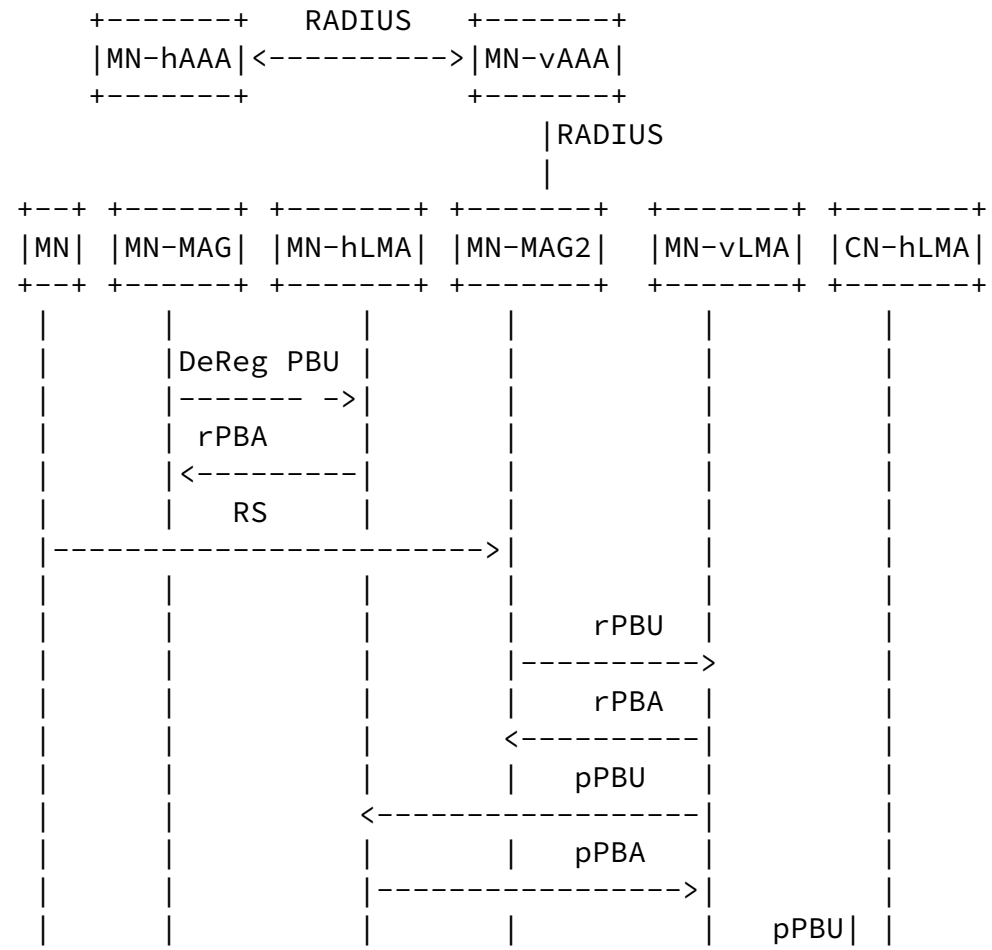


Figure 2:MN roams to MN- vLMA domain

6.2.1. Inter-domain handover operation

In RFC5213 the inter-domain handover is not involved.This document describes the network-based Inter-domain handover options, and the corresponding functionality for Inter-domain handover for PMIPv6.Since the MN is not involved in IP mobility signaling in

PMIPv6, the sequence of events illustrating the MN inter-domain handover are shown in Figure 3.



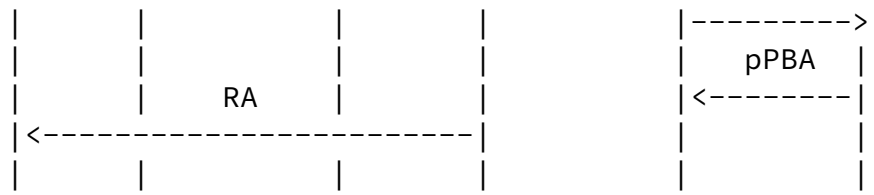


Figure 3:signaling of MN inter-handover

(a)MN-MAG detects that a handover is imminent and sends the DeReg PBU message to the MN-hLMA asking MN-hLMA to remove the binding between MN-MAG and MN.

(b)The MN-hLMA sends back the rPBA message to MN-MAG.

(c) MN roams to MN-vLMA, and sends Router Solicit(RS) message to MN-MAG2. The MN-HoA and CN-HoA are included in RS message.

(d) Upon receiving RS message ,MN-MAG2 sends request to download the per MN Policy Profile from the MN-vAAA.

(e)MN-vAAA assigns a MN-vLMA to MN -MAG2 ,and sends request to MN-hAAA to download the per MN Policy Profile . MN-vLMA's address is included in the request message.

(f)MN-hAAA receives the request message and sends the MN Policy Profile to MN-vAAA ,then MN-hAAA uses MN-vLMAA to take place of MN-hLMAA.

(g)MN-vAAA sends the Accept Message which includes both MN-hLMAA and MN-vLMAA to MN-MAG2.

(h) MN-MAG2 sends the rPBU message to MN-vLMA. MN-HoA,CN-HoA and MN-hLMAA are included in rPBU message .

(i) Upon receiving rPBU message, MN-vLMA firstly assigns a MN-CoA for MN ,builds up the inner-domain BCE for MN and sends rPBA message back to MN-MAG2 .The MN-CoA is included in rPBA message.In the Inner-domain BCE there is a binding between MN's Proxy-CoA2 and MN's CoA.

Secondly,MN-vLMA sends pPBU message to MN-hLMA,the source address of the pPBU message is MN-vLMAA and the destination address of the pPBU message is MN-hLMAA. CN-HoA is included in pPBU message. Upon receiving the pPBU message,MN-hLMA sends back pPBA message to MN-vLMA with CN-HoA included .MN-vLMA builds up the binding between CN-HoA and CN-HoA in the Inter-domain BCE.

Thirdly,MN-vLMA sends pPBU message to CN-hLMA, the source address of the pPBU message is MN-CoA and the destination address of the pPBU message is CN-HoA.The pPBU message includes the MN-CoA and MN-HoA. This pPBU message is packaged in UDP format,and by judging the format of the message CN-hLMA intercepts the pPBU message ,encapsulates the message and updates the Inter-domain BCE for MN. That means in the Inter-domain BCE there is a binding between MN-CoA and MN-HoA.

(j) After receiving rPBA message from MN-vLMA, MN-MAG2 builds up the binding among MN-HoA ,MN-CoA and MN-vLMA. Then MN-MAG2 sends Router Advertise (RA) message to MN. The inter-domain handover operation is over.

6.2.2. Forwarding Consideratons

Forwarding Considerations:

(a) Packets from MN to CN:

(1).The source address is MN-HoA, and the destination address is CN-HoA.

(2).The packets are forwarded from MN to MN-MAG2 through Link-layer.

(3).The packets are forwarded form MN-MAG2 to MN-hLMA through tunnel, the source address of the tunnel is MN-MAG2's IP address, and the destination address of the tunnel is MN-vLMAA.

(4).According to check both the source address and the destination address of the data packets.MN-vLMA detects the MN and CN are not both in their home domain,so MN-vLMA encapsulates the packets to route to CN. The format of the tunneled packet is shown below:

IPv6 header (src= MN-vLMAA, dst= CN's HoA) /* Tunnel Header */

IPv6 header (src= MN's HoA, dst= CN's HoA) /* Packet Header */

Upper layer protocols /* Packet Content*/

(5).The packets are intercepted by CN-hLMA.According to check both the source address and the destination address of the data packets.CN-hLMA detects the MN and CN are not both in their home domain,CN-hLMA decapsulates the packets and forwards them to CN-MAG through tunnel, the source address of the tunnel is CN-hLMAA, and the destination address of the tunnel is CN-Proxy-CoA .

(6).CN-MAG decapsulates the packets and forwards them to CN through Link-layer.

(b) Packets from CN to MN:

(1).The source address is CN-HoA , and the destination address is MN-HoA .

(2).The packets are forwarded from CN to CN-MAG through Link-layer.

(3).The packets are forwarded form CN-MAG to CN-hLMA through tunnel, the source address of the tunnel is CN-Proxy-CoA and the destination address of the tunnel is CN-hLMAA.

(4).According to check both the source address and the destination address of the data packets.CN-hLMA detects the MN and CN are not both in their home domain,so CN-hLMA encapsulates the packets to route to MN..The format of the tunneled packet is shown below:

IPv6 header (src= CN-hLMAA, dst= MN's CoA) /* Tunnel Header */

IPv6 header (src= CN's HoA, dst= MN's HoA) /* Packet Header */

Upper layer protocols /* Packet Content*/

(5). The packets are intercepted by MN-vLMA.MN-vLMA decapsulates the packets and forwards them to MN-MAG2 through tunnel, the source address of the tunnel is MN-vLMAA, and the destination address of the tunnel is MN-Proxy-CoA2.

(6).MN-MAG2 decapsulates the packets and forwards them to MN through Link-layer.

6.3. CN Performs Inter-domain handover

On the basis of situation described in 6.2,CN roams to CN-vLMA domain and MN is still in MN-vLMA domain.The reference network is illustrated in Figure 4.

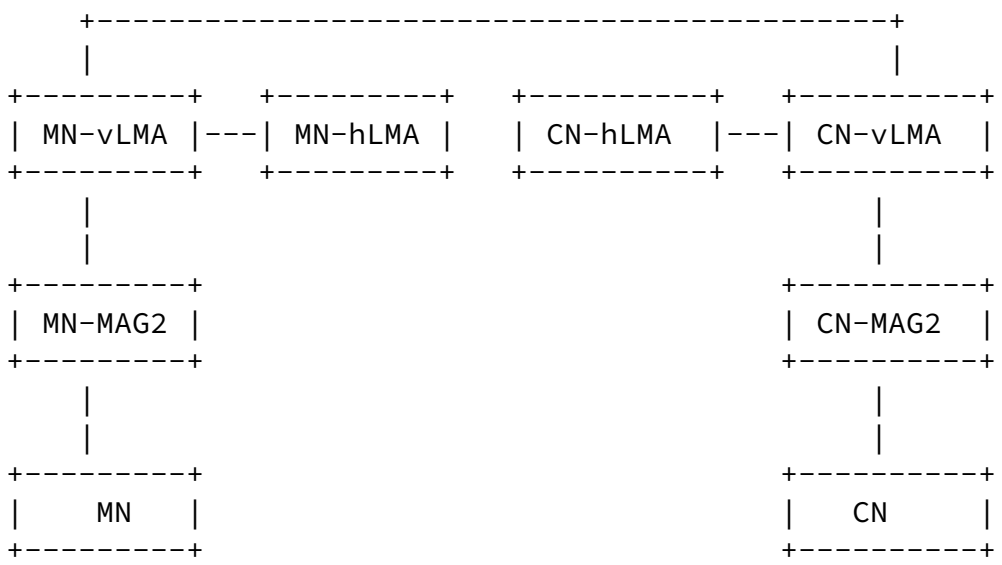


Figure 4:CN roams to CN- vLMA domain

6.3.1. Inter-domain handover operation

The sequence of events illustrating the CN inter-domain handover are shown in Figure 5.

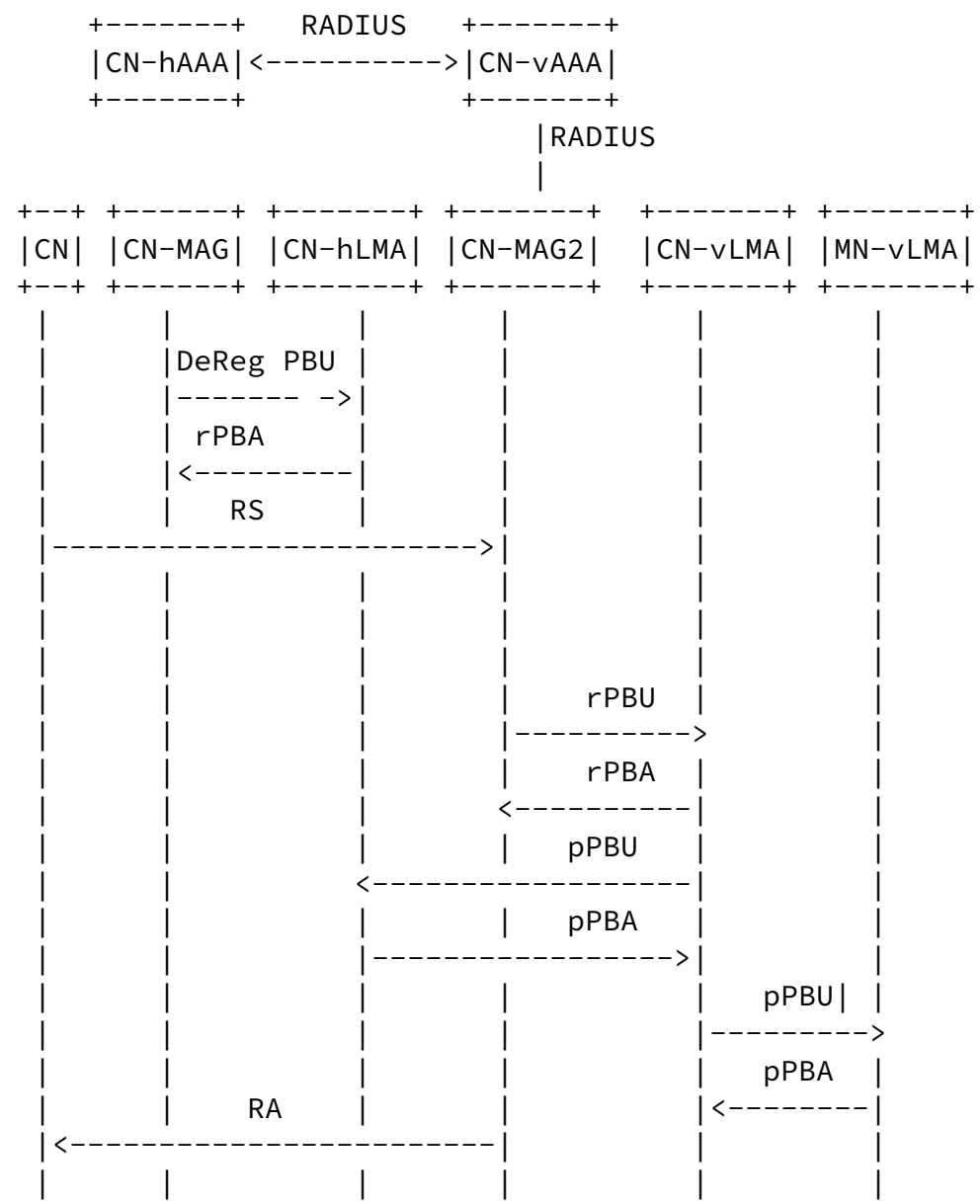


Figure 5:signaling of CN inter-handover

(a)CN-MAG detects that a handover is imminent and sends the DeReg PBU message to the CN-hLMA asking CN-hLMA to remove the binding between CN-MAG and CN.

(b)The CN-hLMA sends back the rPBA message to CN-MAG.

(c) CN roams to CN-vLMA, and sends RS message to CN-MAG2. The CN-HoA and MN-HoA are included in RS message.

(d) Upon receiving RS message ,CN-MAG2 sends request to download the per CN Policy Profile from the CN-vAAA.

(e)CN-vAAA assigns a CN-vLMA to CN -MAG2 ,and sends request to CN-hAAA to download the per CN Policy Profile . CN-vLMA's address is included in the request message.

(f)CN-hAAA receives the request message and sends the CN Policy Profile to CN-vAAA ,then CN-hAAA uses CN-vLMAA to take place of CN-hLMAA.

(g)CN-vAAA sends the Accept Message which includes both CN-hLMAA and CN-vLMAA to CN-MAG2.

(h) CN-MAG2 sends the rPBU message to CN-vLMA. MN-HoA,CN-HoA and CN-hLMAA are included in rPBU message .

(i) Upon receiving rPBU message, CN-vLMA firstly assigns a CN-CoA for CN ,builds up the inner-domain BCE for CN and sends rPBA message back to CN-MAG2 .The CN-CoA is included in rPBA message.In the Inner-domain BCE there is a binding between CN's Proxy-CoA2 and CN's CoA.

Secondly,CN-vLMA sends pPBU message to CN-hLMA,the source address of the pPBU message is CN-vLMAA and the destination address of the pPBU message is CN-hLMAA. MN-HoA is included in pPBU message. Upon receiving the pPBU message,CN-hLMA sends back pPBA message to CN-vLMA with MN-HoA and MN-CoA included .CN-vLMA updates the inter-domain BCE with the binding between MN-HoA and MN-CoA.

Thirdly,CN-vLMA sends pPBU message to MN-hLMA, the source address of the pPBU message is CN-CoA and the destination address of the pPBU message is MN-CoA.The pPBU message includes the CN-CoA and CN-HoA. This pPBU message is packaged in UDP format,and by judging the format of the message MN-hLMA intercepts the pPBU message ,encapsulates the message and updates the Inter-domain BCE for CN. That means in the Inter-domain BCE there is a binding between CN-CoA and CN-HoA.

(j) After receiving rPBA message from CN-vLMA, CN-MAG2 builds up the binding among CN-HoA ,CN-CoA and CN-vLMA. Then CN-MAG2 sends RA message to CN. The inter-domain handover operation is over.

6.3.2. Forwarding Consideratons

Forwarding Considerations:

(a) Packets from MN to CN:

(1).The source address is MN-HoA, and the destination address is CN-HoA.

(2).The packets are forwarded from MN to MN-MAG2 through Link-layer.

(3).The packets are forwarded form MN-MAG2 to MN-hLMA through tunnel, the source address of the tunnel is MN-MAG2's IP address, and the destination address of the tunnel is MN-vLMAA.

(4). According to check both the source address and the destination address of the data packets.CN-hLMA detects the MN and CN are not both in their home domain,so MN-vLMA encapsulates the packets to route to CN. The format of the tunneled packet is shown below:

IPv6 header (src= MN-vLMAA, dst= CN's CoA) /* Tunnel Header */

IPv6 header (src= MN's HoA, dst= CN's HoA) /* Packet Header */

Upper layer protocols /* Packet Content*/

(5).The packets are intercepted by CN-vLMA. According to check both the source address and the destination address of the data packets.CN-hLMA detects the MN and CN are not both in their home domain,so CN-vLMA decapsulates the packets and forwards them to CN-MAG2 through tunnel, the source address of the tunnel is CN-vLMAA, and the destination address of the tunnel is CN-Proxy-CoA2 .

(6).CN-MAG2 decapsulates the packets and forwards them to CN through Link-layer.

(b) Packets from CN to MN:

(1).The source address is CN-HoA , and the destination address is MN-HoA .

(2).The packets are forwarded from CN to CN-MAG2 through Link-layer.

(3).The packets are forwarded form CN-MAG2 to CN-vLMA through tunnel, the source address of the tunnel is CN-Proxy-CoA2 and the destination address of the tunnel is CN-vLMAA.

(4). According to check both the source address and the destination address of the data packets.CN-hLMA detects the MN and CN are not both in their home domain,so CN-vLMA encapsulates the packets to route to MN. The format of the tunneled packet is shown below:

IPv6 header (src= CN-vLMAA, dst= MN's CoA) /* Tunnel Header */

IPv6 header (src= CN's HoA, dst= MN's HoA) /* Packet Header */

Upper layer protocols /* Packet Content*/

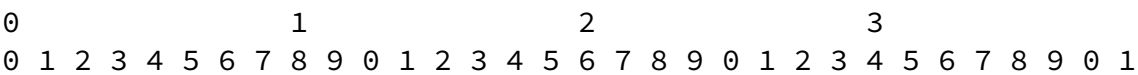
(5). The packets are intercepted by MN-vLMA. According to check both the source address and the destination address of the data packets.CN-hLMA detects the MN and CN are not both in their home domain,so MN-vLMA decapsulates the packets and forwards them to MN-MAG2 through tunnel, the source address of the tunnel is MN-vLMAA, and the destination address of the tunnel is MN-Proxy-CoA2.

(6).MN-MAG2 decapsulates the packets and forwards them to MN through Link-layer.

7. Message Formats

This section defines extensions to the Proxy Mobile IPv6 [RFC5213] protocol messages.

7.1. rPBU



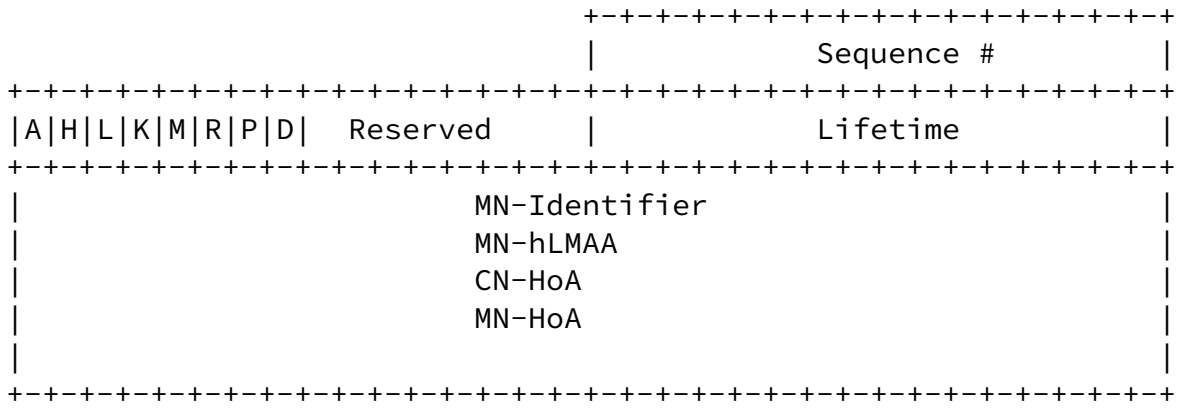


Figure 6:rPBU

A Binding Update message that is sent by a mobile access gateway to a local mobility anchor is referred to as the "rPBU" message.A new flag (D) is included in the rPBU message. The rest of the Binding Update message format remains the same as defined in [RFC5213] and with the additional (R) and (M) flags, as specified in [RFC3963] and

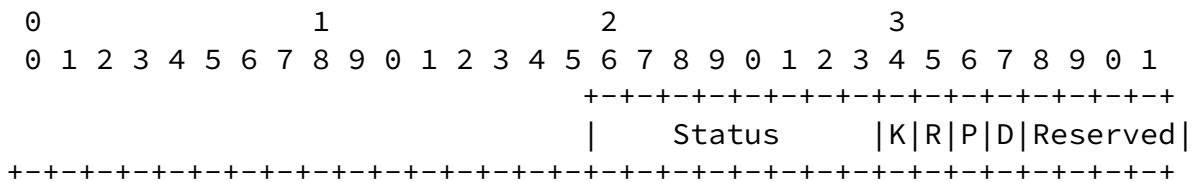
[RFC4140], respectively.

Distinguish Flag (D)

A new flag (D) is included in the Binding Update message to indicate to the local mobility anchor that the Binding Update message is a proxy registration sent by a mobile access gateway to a local mobility anchor. The flag MUST be set to the value of 1 .

The rPBU message sent by a mobile access gateway to a local mobility anchorcontains MN-Identifer , MN-hLMAA, MN-HoA and CN-HoA.

7.2. rPBA



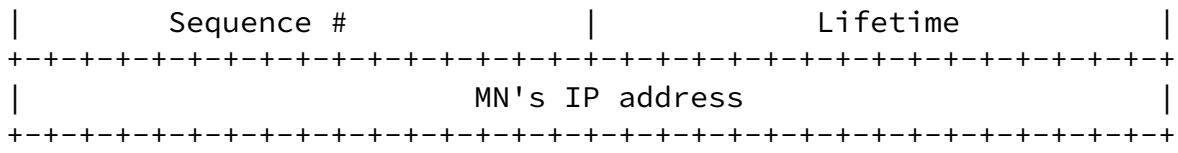


Figure 7:rPBA

A Binding Acknowledgement message that is sent by a local mobility anchor to a mobile access gateway is referred to as the "rPBA" message. A new flag (D) is included in the Binding Acknowledgement message. The rest of the Binding Acknowledgement message format remains the same as defined in [RFC5213] and with the additional (R) flag as specified in [RFC3963].

Distinguish Registration Flag (D)

A new flag (D) is included in the Binding Acknowledgement message to indicate that the local mobility anchor processed the corresponding Proxy Binding Update message as rPBU message. The flag is set to a value of 1 . The rPBA message sent by a local mobility anchor to a mobile access gateway contains MN's IP address assigned by the local mobility anchor .

7.3. pPBU

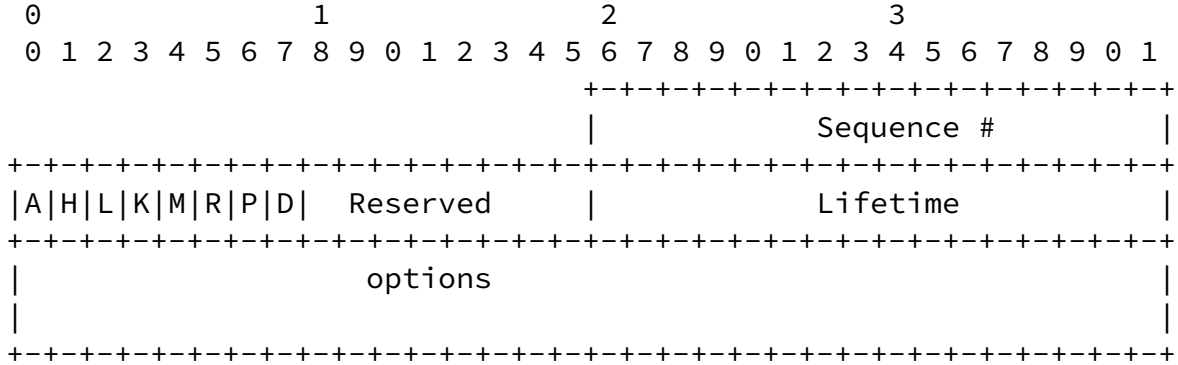


Figure 8:pPBU

A Binding Update message that is sent by a local mobility anchor to a local mobility anchor is referred to as the "pPBU" message.A new flag (D) and a new flag (M) are included in the pPBU message. The rest of the Binding Update message format remains the same as defined in [RFC5213] and with the additional (R) and (M) flags, as specified in [RFC3963] and [RFC4140], respectively.

Distinguish Flag (D)

A new flag (D) is included in the Binding Update message to indicate to the local mobility anchor that the Binding Update message is a proxy registration sent by a local mobility anchor to a local mobility anchor. The flag MUST be set to the value of 2 or 3.

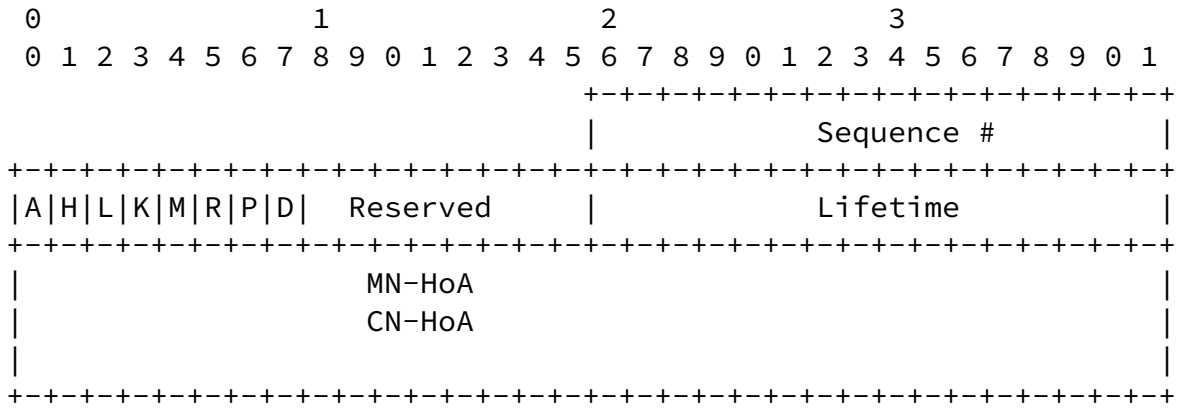


Figure 9:pPBU sent by a visit LMA to the home LMA

A new flag (D) is included in the Binding Update message to indicate to the local mobility anchor that the Binding Update message is a PBU

message sent by a visit local mobility anchor to the home local mobility anchor. The flag MUST be set to the value of 2. This pPBU message sent by a visit local mobility anchor to the home local mobility anchor contains MN-HoA and CN-HoA.

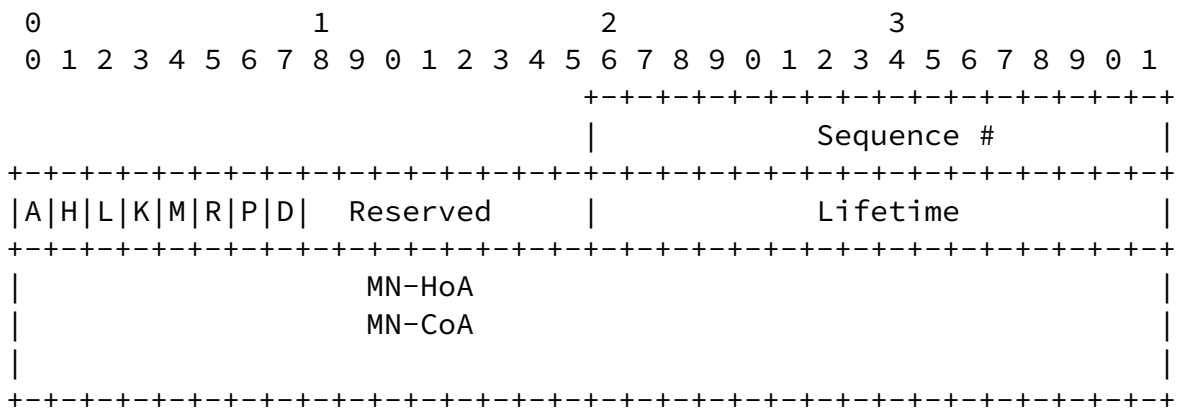


Figure 10:pPBU sent by MN's LMA to CN's LMA

A new flag (D) is included in the Binding Update message to indicate to the local mobility anchor that the Binding Update message is a PBU message sent by MN's local mobility anchor to CN's local mobility anchor . The flag MUST be set to the value of 3.This pPBU message sent by MN's local mobility anchor to CN's local mobility anchor contains MN-HoA and MN-HoA.

7.4. pPBA

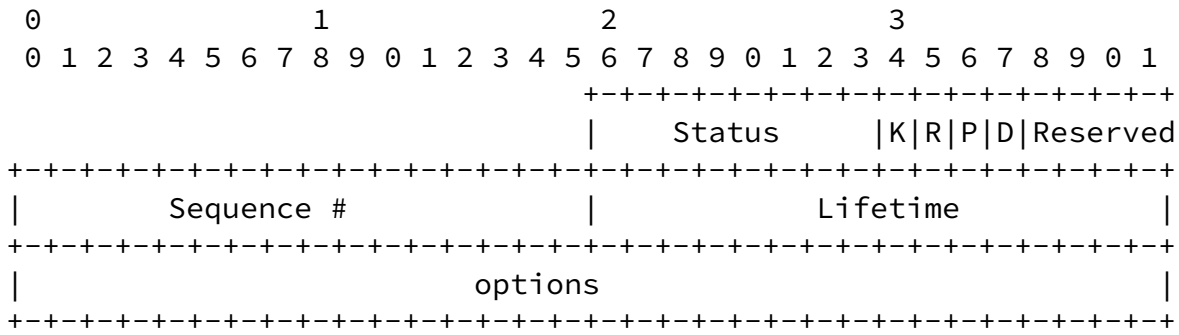


Figure 11:pPBA

A Binding Acknowledgement message that is sent by a local mobility anchor to a local mobility anchor is referred to as the "pPBA"

message. A new flag (D) and a new flag (M) are included in the Binding Acknowledgement message. The rest of the Binding Acknowledgement message format remains the same as defined in [RFC5213] and with the additional (R) flag as specified in [RFC3963].

Distinguish Registration Flag (D)

A new flag (D) is included in the Binding Acknowledgement message to indicate that the local mobility anchor processed the corresponding Proxy Binding Update message as pPBU message. The flag is set to a value of 2 or 3.

A new flag (D) is included in the Binding Acknowledgement message to indicate that the local mobility anchor processed the corresponding Proxy Binding Update message as pPBU message sent by a visit local mobility anchor to the home local mobility anchor. The flag is set to a value of 2 .The options of the message contains the CN-CoA.

A new flag (D) is included in the Binding Acknowledgement message to indicate that the local mobility anchor processed the corresponding Proxy Binding Update message as pPBU message sent by MN's local mobility anchor to CN's local mobility anchor. The flag is set to a value of 3 .

8. Security Considerations

The potential security threats against any network-based mobility management protocol are described in [RFC4832]. This section explains how Proxy Mobile IPv6 protocol defends itself against those threats.

Proxy Mobile IPv6 protocol recommends the signaling messages, Proxy Binding Update and Proxy Binding Acknowledgement, exchanged between the mobile access gateway and the local mobility anchor or between a local mobility anchor and a local mobility anchorto be protected using IPsec using the established security associationbetween them. This essentially eliminates the threats related to the impersonation of the mobile access gateway or the local mobility anchor.

This specification allows a mobile access gateway to send binding registration messages on behalf of a mobile node. If proper authorization checks are not in place, a malicious node may be able to hijack a mobile node's mobility session or may carry out a denial-of-service attack. To prevent this attack, this specification requires the local mobility anchor to allow only authorized mobile access gateways that are part of that Proxy Mobile IPv6 domain to send Proxy Binding Update messages on behalf of a mobile node.

To eliminate the threats on the interface between the mobile access gateway and the mobile node, this specification requires an established trust between the mobile access gateway and the mobile node and to authenticate and authorize the mobile node before it is allowed to access the network. Further, the established authentication mechanisms enabled on that access link will ensure that there is a secure binding between the mobile node's identity and its link-layer address. The mobile access gateway will definitively identify the mobile node from the packets that it receives on that access link.

To address the threat related to a compromised mobile access gateway, the local mobility anchor, before accepting a Proxy Binding Update message for a given mobile node, may ensure that the mobile node is attached to the mobile access gateway that sent the Proxy Binding Update message. This may be accomplished by contacting a trusted entity, which is able to track the mobile node!_s current point of attachment. However, the specific details of the actual mechanisms for achieving this is outside the scope of this document.

9. IANA Considerations

This document defines six new Mobility Header options, the HomeNetwork Prefix Option, Handoff Indicator Option, Access Technology Type Option, Mobile Node Link-layer Identifier Option, Link-local Address Option, and Timestamp Option. The Type value for these options has been assigned from the same numbering space as allocated for the other mobility options,as defined in [RFC3775].

The Handoff Indicator Option introduces a new Handoff Indicator (HI) numbering space, where the values from 0 to 5 have been reserved by this document. Approval of new Handoff Indicator type values are to be made through IANA Expert Review.

The Access Technology Type Option introduces a new Access Technology type (ATT) numbering space, where the values from 0 to 5 have been reserved by this document. Approval of new Access Technology type values are to be made through IANA Expert Review.

This document also defines new Binding Acknowledgement status values. The status values MUST be assigned from the same number space used

for Binding Acknowledgement status values,as defined in [RFC3775]. The allocated values for each of thesestatus values must be greater than 128.

This document creates a new registry for the flags in the Binding

Update message called the "Distinguish Flag".

The following flags are reserved:

(A) 0x8000 [RFC3775]

(H)0x4000 [RFC3775]

(L)0x2000 [RFC3775]

(K) 0x1000 [RFC3775]

(M) 0x0800 [RFC4140]

(R) 0x0400 [RFC3963]

(P) 0x0200[RFC5213]

This document reserves a new flag (D) as follows:

(D) 0x0100

The rest of the values in the 16-bit field are reserved. New values can be assigned by Standards Action or IESG approval.

This document also creates a new registry for the flags in the Binding Acknowledgment message called the "Distinguish Flag". The following values are reserved.

(K) 0x80 [RFC3775]

(R) 0x40 [RFC3963]

(P) 0x20 [RFC5213]

This document reserves a new flag (D) as follows:

(D) 0x10

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.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

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

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[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.

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

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

10.2. Informative References

[RFC1981] McCann, J., Deering, S., and J. Mogul, "Path MTU Discovery for IP version 6", RFC 1981, August 1996.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC4140] Soliman, H., Castelluccia, C., El Malki, K., and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC 4140, August 2005.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4330] Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", RFC 4330, January 2006.

[RFC4372] Adrangi, F., Lior, A., Korhonen, J., and J. Loughney, "Chargeable User Identity", RFC 4372, January 2006.

[RFC4821] Mathis, M. and J. Heffner, "Packetization Layer Path MTU

Discovery", RFC 4821, March 2007.

[RFC4830] Kempf, J., "Problem Statement for Network-Based Localized Mobility Management (NETLMM)", RFC 4830, April 2007.

[RFC4831] Kempf, J., "Goals for Network-Based Localized Mobility Management (NETLMM)", RFC 4831, April 2007.

Authors' Addresses

Zhengming Ma
SUN YAT-SEN UNIVERSITY
Department of Electronics and Engineering,daxuecheng,313
Zhongshan University,Guangzhou, 510006
P.R. China

Email: issmzm@mail.sysu.edu.cn

Ke Wang
SUN YAT-SEN UNIVERSITY
Department of Electronics and Engineering,daxuecheng,313
Zhongshan University,Guangzhou, 510006
P.R. China

Email: wang923zheng@sina.com

Fei Zhang
SUN YAT-SEN UNIVERSITY
Department of Electronics and Engineering,daxuecheng,313
Zhongshan University,Guangzhou, 510006
P.R. China

Email: zsu05zhangfei@163.com