NETLMM Working Group   R. Wakikawa
Internet-Draft   Toyota ITC
Intended status: Standards Track   S. Gundavelli
Expires: August 16, 2010   Cisco
                                                  February 12, 2010

                  IPv4 Support for Proxy Mobile IPv6
                  draft-ietf-netlmm-pmip6-ipv4-support-18.txt

Abstract

   This document specifies extensions to Proxy Mobile IPv6 protocol for
   adding IPv4 protocol support. The scope of IPv4 protocol support is
   two-fold: 1) enable IPv4 home address mobility support to the mobile
   node. 2) allow the mobility entities in the Proxy Mobile IPv6 domain
   to exchange signaling messages over an IPv4 transport network.

Table of Contents

[1](#). **Overview**

   The transition from IPv4 to IPv6 is a long process and during this
   period of transition, both the protocols will be enabled over the
   same network infrastructure. Thus, it is reasonable to assume that a
   mobile node in a Proxy Mobile IPv6 domain may operate in an IPv4-only
   IPv6-only or in dual-stack mode and additionally the network between
   the mobile access gateway and a local mobility anchor may be an IPv4
   or an IPv6 network. It is also reasonable to expect the same
   mobility infrastructure in the Proxy Mobile IPv6 domain to provide
   mobility to the mobile nodes operating in IPv4, IPv6 or in dual mode
   and whether the transport network is IPv4 or IPv6 network. The
   motivation and scope of IPv4 support in Mobile IPv6 is summarized in
   [RFC4977] and all those requirements apply to Proxy Mobile IPv6
   protocol as well.

   The Proxy Mobile IPv6 protocol [RFC5213] specifies a mechanism for
   providing IPv6 home address mobility support to a mobile node in a
   Proxy Mobile IPv6 domain. The protocol requires IPv6 transport
   network between the mobility entities. The extensions defined in
   this document extends IPv4 support to the Proxy Mobile IPv6 protocol
   [RFC5213].

   The scope of IPv4 support in Proxy Mobile IPv6 includes the support
   for the following two features:

   o IPv4 Home Address Mobility Support: A mobile node which is dual-
      stack or IPv4-only enabled will be able to obtain an IPv4 address
      and be able to use that address from any of the access networks in
      that Proxy Mobile IPv6 domain. The mobile node is not required to
      be allocated or assigned an IPv6 address to enable IPv4 home
      address support.

   o IPv4 Transport Network Support: The mobility entities in the Proxy
      Mobile IPv6 domain will be able to exchange Proxy Mobile IPv6
      signaling messages over an IPv4 transport.

   These two features, the IPv4 Home Address Mobility support and the
   IPv4 transport support features, are independent of each other and
   deployments may choose to enable any one or both of these features as
   required.

   Figure 1 shows a typical Proxy Mobile IPv6 domain with IPv4 transport
   network and with IPv4 enabled mobile nodes. The terms used in this
   illustration are explained in the Terminology section.

```
               +----+                    +----+
               |LMA1|                    |LMA2|
               +----+                    +----+
   IPv4-LMAA  -> |          IPv4-LMAA-> | <-- LMAA
               |                     |
               \\                   //\\
                \\                 //  \\
                 \\               //    \\
             +---\\------------- //------\\----+
             (     \\  IPv4/IPv6 //        \\    )
             (      \\  Network //          \\   )
             +------\\--------//-----------\\-+
                 \\      //                 \\
                  \\    //                   \\
                   \\  //                     \\
       IPv4-Proxy-CoA --> |                    | <-- Proxy-CoA
                   +----+                    +----+
                   |MAG1|-----{MN2}        |MAG2|
                   +----+     |            +----+
     (MN-HoA)          |        |            | <-- (MN-HoA)
     (IPv4-MN-HoA) --> |   (IPv4-MN-HoA)     | <-- (IPv4-MN-HoA)
                   {MN1}                    {MN3}
```
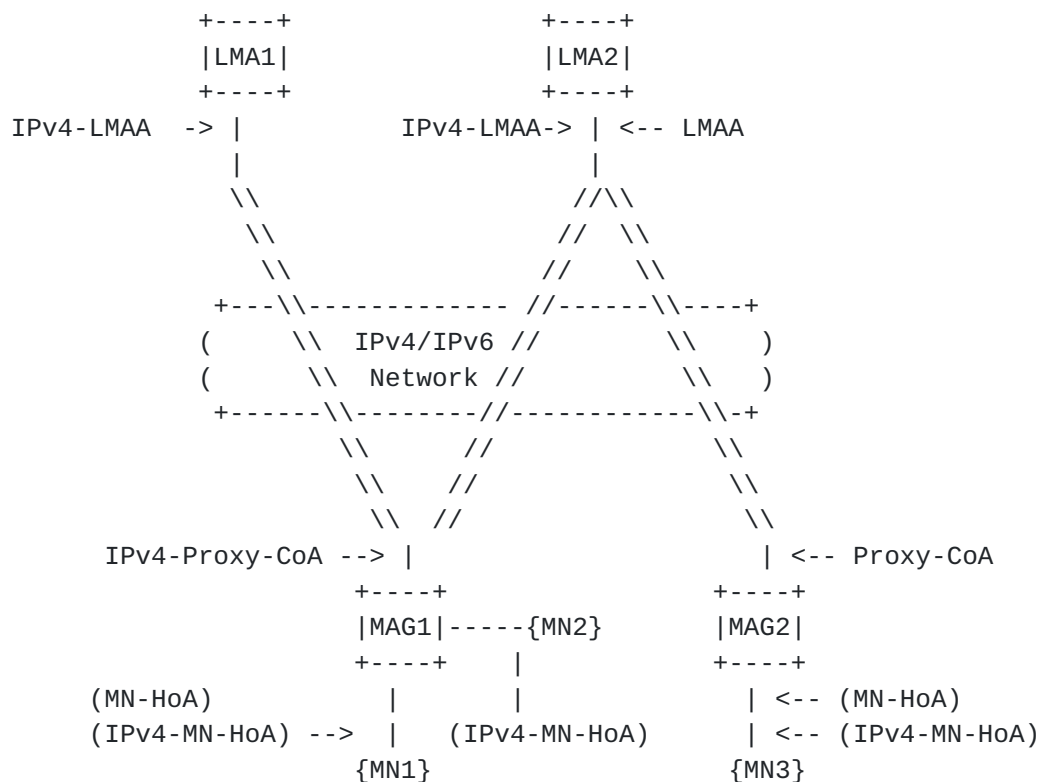
Figure 1: IPv4 support for Proxy Mobile IPv6

1.1. Stated Assumptions

The following are the system and configuration requirements from the
mobility entities in the Proxy Mobile IPv6 domain for supporting the
extensions defined in this document.

o Both the mobility entities, the local mobility anchor and the
   mobile access gateway are dual stack (IPv4/IPv6) enabled.
   Irrespective of the type of transport network (IPv4 or IPv6)
   separating these two entities, the mobility signaling is always
   based on Proxy Mobile IPv6 [RFC5213].

o A deployment where a mobile access gateway uses an IPv4 private
   address with NAT [RFC3022] translation devices in path to a local
   mobility anchor is not supported by this specification.

o The mobile node can be operating in IPv4-only, IPv6-only or in
   dual mode. Based on what is enabled for a mobile node, it should
   be able to obtain IPv4-only, IPv6-only or both IPv4 and IPv6
   address(es) for its interface and furthermore achieve mobility
   support for those addresses.

o For enabling IPv4 home address mobility support to a mobile node,
   it is not required that the IPv6 home address mobility support
   needs to enabled. However, the respective protocol(s) support,
   such as IPv4 or IPv6 packet forwarding, must be enabled on the
   access link between the mobile node and the mobile access gateway.

o The mobile node can obtain an IPv4 address for its attached
   interface. Based on the type of link, it may be able to acquire
   its IPv4 address configuration using standard IPv4 address
   configuration mechanisms such as DHCP [RFC2131], IPCP [RFC1332],
   IKEv2 [RFC4306] or static address configuration. However, the
   details on how IPCP or IKEv2 can be used for address delivery is
   outside the scope of this document.

o The mobile node's IPv4 home subnet is typically a shared address
   space. It is not for the exclusive use of any one mobile node.
   There can be multiple mobile nodes that are assigned IPv4
   addresses from the same subnet.

o The mobile access gateway is the IPv4 default router for the
   mobile node on its access link. It will be in the forwarding path
   for the mobile node's data traffic. Additionally, as specified in
   section 6.9.3 of [RFC5213], all the mobile access gateways in the
   Proxy Mobile IPv6 domain MUST use the same link-layer address on
   any of the access links wherever the mobile node attaches.

1.2. Relevance to Dual-Stack Mobile IPv6

   IPv4 support for Mobile IPv6 is specified in Dual-Stack Mobile IPv6
   specification [RFC5555]. This document leverages some of the
   approaches, messaging options and processing logic defined in that
   document for extending IPv4 support to Proxy Mobile IPv6, except with
   deviation in some aspects for obvious reasons of supporting a
   network-based mobility model. Following are some of the related
   considerations.

o The Binding Update flag 'F' and the NAT Detection Option defined
   in Sections 3.1.3 and 3.2.2 of [RFC5555] are used by this
   specification in Proxy Binding Update and Proxy Binding
   Acknowledgement messages. Their sole purpose is to allow forcing
   of UDP encapsulation between a mobile access gateway and a local
   mobility anchor in situations similar to those discussed in
   Sections 4.1 and 4.4.1 of [RFC5555].

o The extensions needed to the conceptual data structures, Binding
   Cache entry and Binding Update List entry, for storing the state
   related to the IPv4 support defined in [RFC5555], will all be
   needed and relevant for this document.

o In Mobile IPv6 [RFC3775] and in Dual-Stack Mobile IPv6 [RFC5555],
   IPsec security associations (SAs) are specific to a single mobile
   node; they use the identifier visible to upper-layer protocols
   (HoA/IPv4-HoA) as traffic selector; and the IKE/IPsec SAs need to
   be updated when the mobile node moves.

   In Proxy Mobile IPv6 (both [RFC5213] and this document), the IPsec
   SAs are specific to mobile access gateway (and used for
   potentially large number of mobile nodes); they use the locators
   used for routing (Proxy-CoA/IPv4-Proxy-CoA) as traffic selector;
   and they are not updated when the mobile node moves.

   This means the IPsec processing for Mobile IPv6 and Proxy Mobile
   IPv6 (whether IPv6 only or dual-stack) is very different.

o The tunneling considerations specified in [RFC5555] for supporting
   IPv4 transport is relevant for this document as well.

[2](#). Conventions & Terminology

[2.1](#). Conventions

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 [RFC 2119](#) [[RFC2119](#)].

[2.2](#). Terminology

All the mobility related terms used in this document are to be interpreted as defined in the Mobile IPv6 specification [[RFC3775](#)] and Proxy Mobile IPv6 specification [[RFC5213](#)]. In addition this document introduces the following terms.

IPv4 Proxy Care-of Address (IPv4-Proxy-CoA)

   The IPv4 address that is configured on the egress-interface of the mobile access gateway. When using IPv4 transport, this address will be the registered care-of address in the mobile node's Binding Cache entry and will also be the transport-endpoint of the tunnel between the local mobility anchor and a mobile access gateway.

IPv4 Local Mobility Anchor Address (IPv4-LMAA)

   The IPv4 address that is configured on the egress-interface of the local mobility anchor. When using IPv4 transport, the mobile access gateway sends the Proxy Binding Update messages to this address and will be the transport-endpoint of the tunnel between the local mobility anchor and the mobile access gateway.

Mobile Node's IPv4 Home Address (IPv4-MN-HoA)

   The IPv4 home address assigned to the mobile node's attached interface. This address is topologically anchored at the mobile node's local mobility anchor. The mobile node configures this address on its attached interface. If the mobile node connects to the Proxy Mobile IPv6 domain via multiple interfaces each of the interfaces are assigned a unique IPv4 address. All the IPv6 home network prefixes and the IPv4 home address assigned to a given interface of a mobile node will be managed under one mobility session.

Selective De-registration

A procedure for partial de-registration of all the addresses that
belong to one address family, i.e. de-registration of either the
IPv4 home address, or one or more of the assigned IPv6 home
network prefixes.

Encapsulation Modes

This document uses the following terms when referring to the
different encapsulation modes.

IPv4-or-IPv6-over-IPv6

   IPv4 or IPv6 packet carried as a payload of an IPv6 packet

IPv4-or-IPv6-over-IPv4

   IPv4 or IPv6 packet carried as a payload of an IPv4 packet

IPv4-or-IPv6-over-IPv4-UDP

   IPv4 or IPv6 packet carried as a payload in an IPv4 packet with
   a UDP header

IPv4-or-IPv6-over-IPv4-UDP-TLV

   IPv4 packet carried as a payload in an IPv4 packet with UDP and
   TLV headers

IPv4-or-IPv6-over-IPv4-GRE

   IPv4 packet carried as a payload in an IPv4 packet with GRE
   header (but no UDP or TLV header)

3.   **IPv4 Home Address Mobility Support**

   The IPv4 home address mobility support essentially enables a mobile
   node in a Proxy Mobile IPv6 domain to obtain IPv4 home address
   configuration for its attached interfaces and be able to retain that
   address configuration even after performing an handoff anywhere
   within that Proxy Mobile IPv6 domain. This section describes the
   protocol operation and the required extensions to Proxy Mobile IPv6
   protocol for extending IPv4 home address mobility support.

   When an IPv4-enabled or a dual-stack enabled mobile node attaches to
   the Proxy Mobile IPv6 domain, the mobile access gateway on the access
   link where the mobile node is attached will identify the mobile node
   and will initiate the Proxy Mobile IPv6 signaling with the mobile
   node's local mobility anchor. The mobile access gateway will follow
   the signaling considerations specified in Section 3.2 for requesting
   IPv4 home address mobility support. Upon the completion of the
   signaling, the local mobility anchor and the mobile access gateway
   will establish the required routing states for allowing the mobile
   node to use its IPv4 home address from its current point of
   attachment.

   The mobile node on the access link using any of the standard IPv4
   address configuration mechanisms supported on that access link, such
   as IPCP [RFC1332], IKEv2 [RFC4306] or DHCP [RFC2131], will be able to
   obtain an IPv4 home address (IPv4-MN-HoA) for its attached interface.
   Although the address configuration mechanisms for delivering the
   address configuration to the mobile node is independent of the Proxy
   Mobile IPv6 protocol operation, however there needs to be some
   interactions between these two protocol flows. Section 3.4
   identifies these interactions for supporting DHCP based address
   configuration.

   The support for IPv4 home address mobility is not dependent on the
   IPv6 home address mobility support. It is not required that the IPv6
   home address mobility support needs to be enabled for providing IPv4
   home address mobility support. A mobile node will be able to obtain
   IPv4-only, IPv6-only or dual IPv4/IPv6 address configuration for its
   attached interface. The mobile node's policy profile will determine
   if the mobile node is entitled for both the protocol versions or a
   single protocol version. Based on the policy, only those protocols
   will be enabled on the access link. Furthermore, if the mobile node
   after obtaining the address configuration on its interface performs
   an handoff, either by changing its point of attachment over the same
   interface or to a different interface, the network will ensure the
   mobile node will be able to use the same IPv4 address configuration
   after the handoff.

Additionally, If the mobile node connects to the Proxy Mobile IPv6
domain, through multiple interfaces and simultaneously through
different access networks, each of the connected interfaces will
obtain an IPv4 home address from different subnets. In such
scenario, there will be multiple Binding Cache entries for the mobile
node on the local mobility anchor. All the address (IPv4/IPv6)
assigned to a given interface will be managed as part of one mobility
session, as specified in Section 5.4 of [RFC5213].

3.1. Local Mobility Anchor Considerations

3.1.1. Extensions to Binding Cache Entry

To support this feature, the conceptual Binding Cache entry data
structure maintained by the local mobility anchor needs to include
the following parameters.

o The IPv4 home address assigned to the mobile node's interface and
   registered by the mobile access gateway. The IPv4 home address
   entry also includes the corresponding subnet mask. It is to be
   noted that this parameter is defined in the [RFC5555] and is
   presented here for completeness.

o The IPv4 default router address assigned to the mobile node.

3.1.2. Signaling Considerations

3.1.2.1. Processing Proxy Binding Updates

The processing rules specified in Section 5.3 of [RFC5213] are
applied for processing the received Proxy Binding Update message.
However, if the received Proxy Binding Update message has an IPv4
Home Address Request option, the following considerations MUST be
applied additionally.

o If there is an IPv4 Home Address Request option present in the
   received Proxy Binding Update message, but no Home Network Prefix
   option [RFC5213] present in the received Proxy Binding Update
   message, the local mobility anchor MUST NOT reject the request as
   specified in Section 5.3.1 of [RFC5213]. At least one instance of
   any of these two options, either the IPv4 Home Address Request
   option or the Home Network Prefix option, MUST be present. If
   there is not a single instance of any of these two options present
   in the request, the local mobility anchor MUST reject the request
   and send a Proxy Binding Acknowledgement message with Status field
   set to MISSING_HOME_NETWORK_PREFIX_OPTION (Missing mobile node's
   home network prefix option) [RFC5213].

o If there is at least one instance of Home Network Prefix option
   [RFC5213] present in the received Proxy Binding Update message,
   but it is known from the mobile node's policy profile that the
   mobile node is not authorized for IPv6 service, or IPv6 routing in
   not enabled in the home network, the local mobility anchor MUST
   reject the request and send a Proxy Binding Acknowledgement
   message with the Status field set to
   NOT_AUTHORIZED_FOR_IPV6_MOBILITY_SERVICE (mobile node not
   authorized for IPv6 mobility service).

o If there is an IPv4 Home Address Request option present in the
   received Proxy Binding Update message, but it is known from the
   mobile node's policy profile that the mobile node is not
   authorized for IPv4 service, or if IPv4 routing not enabled in the
   home network, the local mobility anchor MUST reject the request
   and send a Proxy Binding Acknowledgement message with the Status
   field set to NOT_AUTHORIZED_FOR_IPV4_MOBILITY_SERVICE (mobile node
   not authorized for IPv4 mobility service).

o If there are more than one instance of the IPv4 Home Address
   Request option present in the request, then the local mobility
   anchor MUST reject the request and send a Proxy Binding
   Acknowledgement message with the Status field set to
   MULTIPLE_IPV4_HOME_ADDRESS_ASSIGNMENT_NOT_SUPPORTED (multiple IPv4
   home address assignment not supported).

o For associating the received Proxy Binding Update message to an
   existing mobility session, the local mobility anchor MUST perform
   the Binding Cache entry existence test by applying the following
   considerations.

   * If there is at least one instance of the Home Network Prefix
      option [RFC5213] with a NON_ZERO prefix value, or, if there is
      an IPv4 Home Address Request option with the IPv4 address in
      the option set to ALL_ZERO, considerations from Section 5.4.1
      of [RFC5213] MUST be applied.

   * If there is an IPv4 Home Address Request option present in the
      request with the IPv4 address value in the option set to a
      NON_ZERO value, considerations from Section 3.1.2.7 MUST be
      applied.

o If there is no existing Binding Cache entry that can be associated
   with the request, the local mobility anchor MUST consider this
   request as an initial binding registration request and
   considerations from Section 3.1.2.2 MUST be applied.
   Additionally, if there are one or more Home Network Prefix options
   [RFC5213] present in the request, considerations from Section

     5.3.2 of [RFC5213] MUST also be applied.

  o If there exists a Binding Cache entry that can be associated with
     the request, the local mobility anchor MUST apply considerations
     from Section 5.3.1 of [RFC5213], (point 13), to determine if the
     request is re-registration or a de-registration request. If the
     request is a re-registration request, considerations from Section
     3.1.2.3 MUST be applied and if it is a de-registration request,
     considerations from Section 3.1.2.5 MUST be applied.

  o If there exists a Binding Cache entry that can be associated with
     the request and if it is determined that the request is a re-
     registration request for extending IPv4 home address mobility
     support to the existing IPv6-only mobility session, considerations
     from Section 3.1.2.2 MUST be applied with respect to IPv4 support.

3.1.2.2. Initial Binding Registration (New Mobility Session)

  o If there is an IPv4 Home Address Request option present in the
     Proxy Binding Update message with the IPv4 address value in the
     option set to ALL_ZERO, the local mobility anchor MUST allocate an
     IPv4 home address to the mobile node and associate it with the new
     mobility session created for that mobile node.

  o If there is an IPv4 Home Address Request option with the IPv4
     address in the option set to a NON_ZERO value, the local mobility
     anchor before accepting the request MUST ensure the address is
     topologically anchored on the local mobility anchor and
     furthermore the mobile node is authorized to use that address. If
     the mobile node is not authorized for that specific address, the
     local mobility anchor MUST reject the request and send a Proxy
     Binding Acknowledgement message with the Status field set to
     NOT_AUTHORIZED_FOR_IPV4_HOME_ADDRESS (mobile node not authorized
     for the requesting IPv4 address). It MUST also include the IPv4
     Home Address Reply option in the reply with the status field value
     in the option set to 129 (Administratively prohibited).

  o If the local mobility anchor is unable to allocate an IPv4 address
     due to lack of resources, it MUST reject the request and send a
     Proxy Binding Acknowledgement message with Status field set to 130
     (Insufficient resources). It MUST also include the IPv4 Home
     Address Reply option in the reply with the status field value in
     the option set to 128 (Failure, reason unspecified).

  o Upon accepting the request, the local mobility anchor MUST create
     a Binding Cache entry for this mobility session. However, if the
     request also contains one or more Home Network Prefix options
     [RFC5213], there should still be only one Binding Cache entry that

should be created for this mobility session. The created Binding
Cache entry MUST be used for managing both IPv4 and IPv6 home
address bindings. The fields in the Binding Cache entry MUST be
updated with the accepted values for that session.

o   The local mobility anchor MUST establish a bi-directional tunnel
    to the mobile access gateway with the encapsulation mode set to
    the negotiated mode for carrying the IPv4 payload traffic. When
    using IPv6 transport, the encapsulation mode is IPv4-or-IPv6-over-
    IPv6 (IPv4 or IPv6 packet carried as a payload of an IPv6 packet).
    When using IPv4 transport, the encapsulation mode is as specified
    in Section 4.

o   The local mobility anchor MUST create an IPv4 host route (or a
    platform specific equivalent function that sets up the forwarding)
    for tunneling the packets received for the mobile node's home
    address associated with this mobility session.

o   The local mobility anchor MUST send the Proxy Binding
    Acknowledgement message with the Status field set to 0 (Proxy
    Binding Update Accepted). The message MUST be constructed as
    specified in Section 3.1.2.6.

3.1.2.3. Binding Lifetime Extension (No handoff)

All the considerations from Section 5.3.3 of [RFC5213] MUST be
applied.

3.1.2.4. Binding Lifetime Extension (After handoff)

o   If there is no Home Network Prefix option(s) [RFC5213] present in
    the request, but if the Binding Cache entry associated with this
    request has IPv6 home network prefix(es), the local mobility
    anchor MUST consider this as a request to extend lifetime only for
    the IPv4 home address and not for the IPv6 home network
    prefix(es). Hence, the local mobility anchor SHOULD release all
    the IPv6 home network prefix(es) assigned to that mobile node and
    for that specific attached interface. Similar considerations
    apply for the case where there is no IPv4 Home Address Request
    option present in the request, but if the Binding Cache entry
    associated with that request has both IPv4 home address and IPv6
    home network prefix(es).

o   The local mobility anchor MUST remove the previously created IPv4
    host route (or the forwarding state) and the dynamically created
    bi-directional tunnel for carrying the IPv4 payload traffic (if
    there are no other mobile nodes for which the tunnel is being
    used). This will remove the routing state towards the mobile

access gateway where the mobile node was anchored prior to the
handoff.

o   The local mobility anchor MUST create a bi-directional tunnel to
    the mobile access gateway that sent the request (if there is no
    existing bi-directional tunnel) and with the encapsulation mode
    set to the negotiated mode for carrying the IPv4 payload traffic.
    An IPv4 host route for tunneling the packets received for the
    mobile node's IPv4 home address MUST also be added.

o   The required forwarding state identified in Section 5.3.6 of
    [RFC5213] is for IPv6 payload traffic. Those considerations apply
    for IPv4 payload traffic as well. However, if IPv4 transport is
    in use, considerations from Section 4 MUST be applied.

3.1.2.5. Binding De-Registration

All the considerations from Section 5.3.5 of [RFC5213] MUST be
applied. Additionally, for removing the IPv4 state as part of the
Binding Cache entry deletion, the IPv4 host route and the dynamically
created bi-directional tunnel for carrying the IPv4 payload traffic
(if there are no other mobile nodes for which the tunnel is being
used) MUST be removed. However, if the request is for a selective
de-registration (IPv4 home address only, or all the IPv6 home network
prefixes), the Binding Cache entry MUST NOT be deleted, only the
respective states with respect to those addresses MUST be deleted.

3.1.2.6. Constructing the Proxy Binding Acknowledgement Message

The local mobility anchor when sending the Proxy Binding
Acknowledgement message to the mobile access gateway MUST construct
the message as specified in Section 5.3.6 of [RFC5213].
Additionally, the following considerations MUST be applied.

o   Section 5.3.6 of [RFC5213] requires the local mobility anchor to
    include at least one instance of Home Network Prefix option
    [RFC5213] in the Proxy Binding Acknowledgement message that it
    sends to the mobile access gateway. However, if the received
    Proxy Binding Update message has only the IPv4 Home Address
    Request option and did not contain the Home Network Prefix
    option(s), then the local mobility anchor MUST NOT include any
    Home Network Prefix option(s) in the reply. However, there MUST
    be at least one instance of either the Home Network Prefix option
    [RFC5213] or the IPv4 Home Address Reply option present in the
    Proxy Binding Acknowledgement message.

o   The IPv4 Home Address Reply option MUST be present in the Proxy
    Binding Acknowledgement message.

   1. If the Status field is set to a value greater than or equal to
       (128), i.e., if the Proxy Binding Update is rejected, then
       there MUST be an IPv4 Home Address Reply option corresponding
       to the IPv4 Home Address Request option present in the request
       and with the IPv4 address value and the prefix length fields
       in the option set to the corresponding values in the request.
       The status field value in the option must be set to the
       specific error code.

   2. For all other cases, there MUST be an IPv4 Home Address Reply
       option for carrying the IPv4 home address assigned for that
       mobility session and with the value in the option set to the
       allocated IPv4 address. The prefix length in the option MUST
       be set to the prefix length of the allocated address. The
       status field value in the option must be set to 0 (Success).

   o The IPv4 Default-Router Address option MUST be present, if the
      Status field value in the Proxy Binding Acknowledgement message is
      set to 0 (Proxy Binding Update Accepted). Otherwise, the option
      MUST NOT be present. If the option is present, the default router
      address in the option MUST be set to the mobile node's default
      router address.

3.1.2.7. Binding Cache Entry Lookup Considerations

   The Binding Cache entry lookup considerations specified in section
   5.4.1.1 of [RFC5213] uses the Home Network Prefix option [RFC5213] as
   the key parameter for identifying the Binding Cache entry. However,
   when there is not a single Home Network Prefix option with a NON_ZERO
   value present in the request, but if there is an IPv4 Home Address
   option with a NON_ZERO value present in the request, then the
   following considerations MUST be applied.

   o The search rules specified in section 5.4.1.1 of [RFC5213], which
      primarily uses IPv6 home network prefix set as the search key, are
      equally valid when using a single IPv4 home address as the key.
      When applying those considerations, instead of the IPv6 home
      network prefix(es), the IPv4 home address from the IPv4 Home
      Address option present in the request MUST be used as the search
      key.

   o The rules specified in section 5.4.1.1 of [RFC5213], assume the
      presence of one or more IPv6 home network prefixes in the received
      request and also in the Binding Cache entry. But, when using the
      IPv4 home address as the search key, these considerations MUST
      always assume just one single IPv4 home address, both in the
      request and also in the Binding Cache entry.

3.1.3. Routing Considerations for the Local Mobility Anchor

Intercepting Packets Sent to the Mobile Node's IPv4 home address:

o When the local mobility anchor is serving a mobile node, it MUST
   advertise a connected route into the Routing Infrastructure for
   the mobile node's IPv4 home address or for its home subnet, in
   order to receive packets that are sent to the mobile node's IPv4
   home address. This essentially enables IPv4 routers in that
   network to detect the local mobility anchor as the last-hop router
   for that subnet.

Forwarding Packets to the Mobile Node:

o On receiving a packet from a correspondent node with the
   destination address matching the mobile node's IPv4 home address,
   the local mobility anchor MUST forward the packet through the bi-
   directional tunnel setup for that mobile node.

o The format of the tunneled packet when payload protection is not
   enabled:


```
   IPv6 header (src= LMAA, dst= Proxy-CoA        /* Tunnel Header */
      IPv4 header (src= CN, dst= IPv4-MN-HOA )  /* Packet Header */
          Upper layer protocols                 /* Packet Content*/
```


                 Figure 2: Tunneled Packets from LMA to MAG

Forwarding Packets Sent by the Mobile Node:

o All the reverse tunneled packets that the local mobility anchor
   receives from the mobile access gateway, after removing the tunnel
   header MUST be routed to the destination specified in the inner
   IPv4 packet header. These routed packets will have the source
   address field set to the mobile node's IPv4 home address.

3.1.4. ECN & Payload Fragmentation Considerations

The ECN considerations specified in Section 5.6.3 of [RFC5213] apply
for the IPv4 payload packets as well. The mobility agents at the
tunnel entry and exit points MUST handle ECN information as specified
in that document.

The mobility agents at the tunnel entry and exit points MUST apply

the IP packet fragmentation considerations as specified in section 7 of [RFC2473] and additionally they MUST apply the considerations related to tunnel error processing and reporting as specified in section 8 of [RFC2473].

3.2. Mobile Access Gateway Considerations

3.2.1. Extensions to Binding Update List Entry

To support the IPv4 home address mobility feature, the conceptual Binding Update List entry data structure needs to be extended with the following additional fields.

o The IPv4 home address assigned to the mobile node's attached interface. This IPv4 home address may have been statically configured in the mobile node's policy profile, or, may have been dynamically allocated by the local mobility anchor. The IPv4 home address entry also includes the corresponding subnet mask.

o The IPv4 default router address of the mobile node. This is acquired from the mobile node's local mobility anchor through the received Proxy Binding Acknowledgment message.

3.2.2. Extensions to Mobile Node's Policy Profile

To support the IPv4 Home Address Mobility Support feature the mobile node's policy profile, specified in Section 6.2 of [RFC5213] MUST be extended with the following additional fields.

Extensions to the mandatory section of the policy profile:

o This field identifies all the IP protocol versions for which the home address mobility support needs to be extended to the mobile node. The supported modes are IPv4-only, IPv6-only and dual IPv4/ IPv6.

Extensions to the optional section of the policy profile:

o The IPv4 home address assigned to the mobile node's attached interface. The specific details on how the network maintains the association between the address and the attached interface is outside the scope of this document. This address field also includes the corresponding subnet mask.

3.2.3. **Signaling Considerations**

3.2.3.1. **Mobile Node Attachment and Initial Binding Registration**

   After detecting a new mobile node on its access link, the mobile
   access gateway on the access link MUST determine if IPv4 home address
   mobility support needs to be enabled for that mobile node. The
   mobile node's policy profile identifies the supported modes (IPv4-
   only, IPv6-only or dual IPv4/IPv6) for that mobile node for which the
   mobile service needs to be enabled. Based on those policy
   considerations and from other triggers such as from the network, if
   it is determined that IPv4 home address mobility support needs to be
   enabled for the mobile node, considerations from section 6.9.1.1 of
   [RFC5213] MUST be applied with the following exceptions.

   o The IPv4 Home Address Request option MUST be present in the Proxy
      Binding Update message.

      * If the mobile access gateway learns the mobile node's IPv4 home
         address either from its policy profile, or from other means,
         the mobile access gateway MAY ask the local mobility anchor to
         allocate that specific address by including exactly one
         instance of the IPv4 Home Address Request option with the IPv4
         home address and the prefix length fields in the option set to
         that specific address and its prefix length.

      * The mobile access gateway MAY also ask the local mobility
         anchor for dynamic IPv4 home address allocation. It can
         include exactly one instance of the IPv4 Home Address option
         with the IPv4 home address and the prefix length fields in the
         option set to ALL_ZERO value. Furthermore, the (P) flag in the
         option MUST be set to 0. This serves as a request to the local
         mobility anchor for the IPv4 home address allocation.

   o The Proxy Binding Update message MUST be constructed as specified
      in Section 6.9.1.5 of [RFC5213]. However, the Home Network Prefix
      option(s) [RFC5213] MUST be present in the Proxy Binding Update
      only if IPv6 home address mobility support also needs to be
      enabled for the mobile node. Otherwise, the Home Network Prefix
      option(s) MUST NOT be present.

   o When using IPv4 transport for carrying the signaling messages, the
      related considerations from section 4 MUST be applied
      additionally.

3.2.3.2. **Receiving Proxy Binding Acknowledgement**

   All the considerations from section 6.9.1.2 of [RFC5213] MUST be
   applied with the following exceptions.

   o If the received Proxy Binding Acknowledgement message has the
      Status field value set to NOT_AUTHORIZED_FOR_IPV4_MOBILITY_SERVICE
      (The mobile node is not authorized for IPv4 mobility service), the
      mobile access gateway SHOULD NOT send a Proxy Binding Update
      message including a IPv4 Home Address Request option till an
      administrative action is taken.

   o If the received Proxy Binding Acknowledgement message has the
      Status field value set to NOT_AUTHORIZED_FOR_IPV4_HOME_ADDRESS(The
      mobile node is not authorized for the requesting IPv4 home
      address), the mobile access gateway SHOULD NOT request for the
      same IPv4 address again, but MAY request the local mobility anchor
      to perform the address assignment by including exactly one
      instance of IPv4 Home Address Request option with the IPv4 home
      address and the prefix length fields in the option set to ALL_ZERO
      value.

   o If the received Proxy Binding Acknowledgement message has the
      Status field value set to NOT_AUTHORIZED_FOR_IPV6_MOBILITY_SERVICE
      (The mobile node is not authorized for IPv6 mobility service), the
      mobile access gateway SHOULD NOT send a Proxy Binding Update
      message including any Home Network Prefix option(s) till an
      administrative action is taken.

   o If there is no IPv4 Home Address Reply option present in the
      received Proxy Binding Acknowledgement message, the mobile access
      gateway MUST NOT enable IPv4 support for the mobile node and the
      rest of the considerations from this section can be skipped.

   o If the received Proxy Binding Acknowledgement message has the
      Status field value in the IPv4 Home Address Reply option set to a
      value that indicates that the request was rejected by the local
      mobility anchor, the mobile access gateway MUST NOT enable
      forwarding for that specific IPv4 home address.

   o If the received Proxy Binding Acknowledgement message has the
      Status field value set to 0 (Proxy Binding Update accepted), the
      mobile access gateway MUST update a Binding Update List entry for
      that mobile node. The entry MUST be updated with the assigned
      IPv4 home address and other accepted registration values.

   o If the received Proxy Binding Acknowledgement message has the
      Status field value set to 0 (Proxy Binding Update accepted) and

has the IPv4 Home Address Reply option set to a value that
indicates that the request was accepted by the local mobility
anchor, the mobile access gateway MUST establish a bi-directional
tunnel to the local mobility anchor (if there is no existing bi-
directional tunnel to that local mobility anchor) and with the
encapsulation mode set to IPv4-or-IPv6-over-IPv6 (IPv4 or IPv6
packet carried as a payload of an IPv6 packet). Considerations
from Section 5.6.1 of [RFC5213] MUST be applied for managing the
dynamically created bi-directional tunnel. However, when using
IPv4 transport, the encapsulation mode MUST be set to the
negotiated encapsulation mode, as specified in Section 4 of this
specification.

o The mobile access gateway MUST set up the route for forwarding the
   IPv4 packets received from the mobile node (using its IPv4 home
   address) through the bi-directional tunnel set up for that mobile
   node.

o The default router address MUST be obtained from the IPv4 Default-
   Router Address option present in the received Proxy Binding
   Acknowledgement message. The mobile access gateway SHOULD
   configure this address on its interface and respond to any ARP
   requests sent by the mobile node for resolving the hardware
   address of the default router. However, since the link between
   the mobile access gateway and the mobile node is a point-to-point
   link, implementations will be able receive any packets sent to the
   default router address without having to explicitly configure the
   default router address on its interface. The mobile access
   gateway MAY also use the default router address as the source
   address for any datagrams sent to the mobile node and originated
   by the mobile access gateway itself. It MUST also use this
   address in the DHCP Router option [RFC2132] in the DHCP messages.

o If there is an IPv4 DHCP Support Mode option present in the
   received Proxy Binding Acknowledgement message and if the (S) flag
   in the option is set to a value of (1), then the mobile access
   gateway MUST function as a DHCP server for the mobile node. If
   either the (S) flag in the option is set to a value of (0), or if
   the option is not present in the request, then the mobile access
   gateway MUST function as a DHCP Relay for the mobile node.

3.2.3.3. Binding Re-Registration and De-Registrations

When sending a Proxy Binding Update either for extending the lifetime
of a mobility session or for de-registering the mobility session, the
respective considerations from [RFC5213] MUST be applied.
Furthermore, the following additional considerations MUST also be
applied.

o If there is an IPv4 home address assigned to the mobility session,
   then there MUST be exactly one instance of the IPv4 Home Address
   Request option present in the Proxy Binding Update message. The
   IPv4 home address and the prefix length fields in the option MUST
   be set to that specific address and its corresponding subnet-mask
   length.

o If there was no IPv4 home address requested in the initial Proxy
   Binding Update message, but if it is determined that the IPv4 home
   address MUST be requested subsequently, then there MUST be exactly
   one instance of the IPv4 Home Address Request option present in
   the Proxy Binding Update message. The IPv4 home address in the
   option MUST be set to either ALL_ZERO or to a specific address
   that is being requested.

o For performing selective de-registration of IPv4 home address but
   still retaining the mobility session with all the IPv6 home
   network prefixes, the Proxy Binding Update message with the
   lifetime value of (0) MUST NOT include any IPv6 Home Network
   Prefix options(s) [RFC5213]. It MUST include exactly one instance
   of the IPv4 Home Address Request option with the IPv4 home address
   and the prefix length fields in the option set to the IPv4 home
   address that is being de-registered. Similarly for selective de-
   registration of all the IPv6 home network prefixes, the Proxy
   Binding Update message MUST NOT include the IPv4 Home address
   option, it MUST include a Home Network Prefix option for each of
   the assigned home network prefixes assigned for that mobility
   session and with the prefix value in the option set to that
   respective prefix value.

o The Home Network Prefix option(s) [RFC5213] MUST NOT be present if
   the same option(s) was not present in the initial Proxy Binding
   Update message. Otherwise considerations from [RFC5213] with
   respect to this option MUST be applied.

o If at any point the mobile access gateway fails to extend the
   binding lifetime with the local mobility anchor for the mobile
   node's IPv4 address, it MUST remove any forwarding state set up
   for the mobile node's IPv4 home address.

3.2.4. Routing Considerations for the Mobile Access Gateway

o On receiving a packet from the bi-directional tunnel established
   with the mobile node's local mobility anchor, the mobile access
   gateway MUST remove the outer header before forwarding the packet
   to the mobile node.

o On receiving a packet from a mobile node connected to its access
   link, the packet MUST be forwarded to the local mobility anchor
   through the bi-directional tunnel established with the local
   mobility anchor. However, when EnableMAGLocalRouting flag is set,
   considerations from Section 6.10.3 of [RFC5213] MUST be applied
   with respect to local routing.

o When forwarding the packet through the bi-directional tunnel, the
   encapsulation considerations specified in section 3.1.3 MUST be
   applied. However, before forwarding the packet, the mobile access
   gateway MUST ensure the source address in the received packet is
   the address allocated for that mobile node and that there is an
   active binding on the local mobility anchor for that mobile node.

o The mobile access gateway SHOULD use Proxy ARP [RFC0925] to reply
   to ARP Requests that it receives from the mobile node seeking
   address resolutions for the destinations on the mobile node's home
   subnet. When receiving an ARP Request, the mobile access gateway
   SHOULD examine the target IP address of the Request, and if this
   IP address matches the mobile node's IPv4 home subnet, it SHOULD
   transmit a Proxy ARP Reply. However, on certain types of links,
   the mobile node does not use ARP for address resolutions, instead
   it forwards all the packets to the mobile access gateway. On such
   types of links, the mobile access gateway is not required to
   support Proxy ARP function. At the same time, implementations not
   supporting the Proxy ARP function on links where the mobile node
   uses ARP for seeking address resolutions for the destinations on
   the mobile node's home subnet will result in communication
   failure.

3.3. Mobility Options and Status Codes

To support the IPv4 home address mobility feature, this specification
defines the following new options and Status Codes.

3.3.1. IPv4 Home Address Request Option

A new option, IPv4 Home Address Request Option is defined for use
with the Proxy Binding Update message sent by the mobile access
gateway to the local mobility anchor. This option is used for
requesting IPv4 home address assignment for the mobile node.

The IPv4 Home Address Request option has an alignment requirement of
4n. Its format 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |    Length     |Prefix-len |     Reserved     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       IPv4 home address                      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

                Figure 3: IPv4 Home Address Request Option

     Type

        IANA

     Length

        8-bit unsigned integer indicating the length of the option in
        octets, excluding the type and length fields. This field MUST
        be set to (6).

     Prefix-len

        This 6-bit unsigned integer indicating the prefix length of the
        IPv4 home address contained in the option.

     Reserved

        This 10-bit field is unused for now. The value MUST be
        initialized to (0) by the sender and MUST be ignored by the
        receiver.

     IPv4 home address

        This four-byte field containing the IPv4 home address that is
        being requested. The value of 0.0.0.0 is used for requesting
        the local mobility anchor to perform the address allocation.

3.3.2. IPv4 Home Address Reply Option

   A new option, IPv4 Home Address Reply Option is defined for using it
   in the Proxy Binding Acknowledgment message sent by the local
   mobility anchor to the mobile access gateway. This option can be
   used for sending the assigned mobile node's IPv4 home address.

   The IPv4 Home Address Reply option has an alignment requirement of

4n. Its format 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |     Status    |Pref-len  |Res|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      IPv4 home address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: IPv4 Home Address Reply Option

Type

   IANA

Length

   8-bit unsigned integer indicating the length of the option in
   octets, excluding the type and length fields. This field MUST
   be set to (6).

Status

   Indicates success or failure for the IPv4 home address
   assignment. Values from 0 to 127 indicate success. Higher
   values (128 to 255) indicate failure. The following status
   values are currently allocated by this document:

      0 Success

      128 Failure, reason unspecified

      129 Administratively prohibited

      130 Incorrect IPv4 home address

      131 Invalid IPv4 address

132 Dynamic IPv4 home address assignment not available

Prefix-len

This 6-bit unsigned integer is used for carrying the prefix
length of the mobile node's IPv4 home network corresponding the
IPv4 home address contained in the option.

Reserved (Res)

This 2-bit field is unused for now. The value MUST be
initialized to (0) by the sender and MUST be ignored by the
receiver.

IPv4 home address

This four-byte field is used for carrying the IPv4 home address
assigned to the mobile node.

3.3.3. IPv4 Default-Router Address Option

A new option, IPv4 Default-Router Address Option is defined for using
it in the Proxy Binding Acknowledgment message sent by the local
mobility anchor to the mobile access gateway. This option can be
used for sending the mobile node's IPv4 default router address.

The IPv4 Default-Router Address option has an alignment requirement
of 4n. Its format 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |          Reserved (R)         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  IPv4 Default-Router Address                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
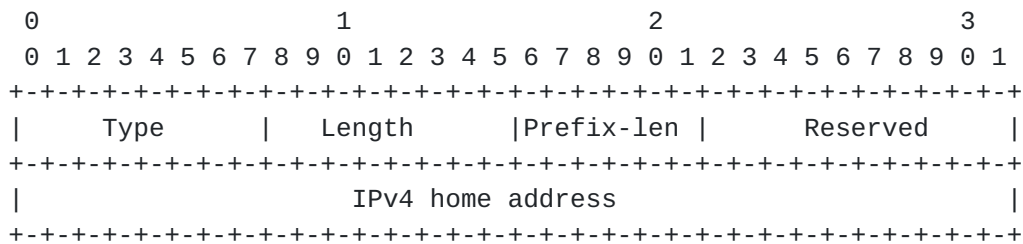
Figure 5: IPv4 Default-Router Address Option

Type

      IANA

   Length

      8-bit unsigned integer indicating the length of the option in
      octets, excluding the type and length fields. This field MUST
      be set to (6).

   Reserved (R)

      This 16-bit field is unused for now. The value MUST be
      initialized to (0) by the sender and MUST be ignored by the
      receiver.

   IPv4 Default-Router Address

      A four-byte field containing the mobile node's default router
      address.

3.3.4. IPv4 DHCP Support Mode

   A new option, IPv4 DHCP Support Mode Option is defined for using it
   in the Proxy Binding Acknowledgment message sent by the local
   mobility anchor to the mobile access gateway. This option can be
   used for notifying the mobile access gateway, if it should function
   as a DHCP Server or a DHCP Relay for the attached mobile node.

   The IPv4 DHCP Support Mode option has no alignment requirement. Its
   format 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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |    Length     |      Reserved (R)           |S|
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

                 Figure 6: IPv4 DHCP Support Mode Option

   Type

      IANA

Length

   8-bit unsigned integer indicating the length of the option in
   octets, excluding the type and length fields. This field MUST
   be set to 2.

Reserved (R)

   This 15-bit field is unused for now. The value MUST be
   initialized to (0) by the sender and MUST be ignored by the
   receiver.

DHCP Support Mode (S)

   A 1-bit field that specifies the DHCP support mode. This flag
   indicates if the mobile access gateway should function as a
   DHCP Server or a DHCP Relay for the attached mobile node. The
   flag value of (0) indicates the mobile access gateway should
   act as a DHCP Relay and the flag value of (1) indicates it
   should act as a DHCP Server.

3.3.5. Status Codes

This document defines the following new Status values for use in the
Proxy Binding Acknowledgement message. These values are to be
allocated from the same numbering space, as defined in Section 6.1.8
of [RFC3775].

NOT_AUTHORIZED_FOR_IPV4_MOBILITY_SERVICE: IANA

   Mobile node not authorized for IPv4 mobility service.

NOT_AUTHORIZED_FOR_IPV4_HOME_ADDRESS: IANA

   Mobile node not authorized for the requesting IPv4 home address

NOT_AUTHORIZED_FOR_IPV6_MOBILITY_SERVICE: IANA

   Mobile node not authorized for IPv6 mobility service.

MULTIPLE_IPV4_HOME_ADDRESS_ASSIGNMENT_NOT_SUPPORTED: IANA

   Multiple IPv4 home address assignment not supported

3.4. **Supporting DHCP-Based Address Configuration**

   This section explains how DHCP-based address configuration support
   can be enabled for a mobile node in a Proxy Mobile IPv6 domain. It
   explains the protocol operation, supported DHCP server deployment
   configurations and the protocol interactions between DHCP agents and
   mobility entities in each of the supported configurations.

   This specification supports the following two DHCP deployment
   configurations.

   o DHCP relay agent co-located with the mobile access gateway.

   o DHCP server co-located in the mobile access gateway.

   The following are the configuration requirements:

   o The DHCP server or the DHCP relay agent configured on the mobile
      access gateway is required to have an IPv4 address for exchanging
      the DHCP messages with the mobile node. This address is the
      mobile node's default router address provided by the local
      mobility anchor. Optionally, all the DHCP servers co-located with
      the mobile access gateways in the Proxy Mobile IPv6 domain can be
      configured with a fixed IPv4 address. This fixed address can be
      potentially an IPv4 private address [RFC1918] that can be used for
      the DHCP protocol communication on any of the access links. This
      address will be used as the server identifier in the DHCP
      messages.

   o A DHCP server identifies a DHCP interface from the contents of the
      DHCP "Client-identifier" option [RFC2132], if present, or from the
      client hardware address (chaddr), as specified in [RFC2131]. Note
      that the name "Client-identifier" is a misnomer as it actually
      identifies an interface and not the client. The DHCP server uses
      this identity to identify the interface for which the address is
      assigned. A mobile node in a Proxy Mobile IPv6 domain, can attach
      to the network through multiple interfaces and can obtain address
      configuration for each of its interfaces. Additionally, it may
      perform handoffs between its interfaces. Following are the
      related considerations with respect to the identification
      presented to the DHCP server.

      * If the mobile node attaches to the Proxy Mobile IPv6 domain
         through multiple physical interfaces, the DHCP server will
         uniquely identify each of those interfaces and will perform
         address assignment. The DHCP server will identify the
         interface as specified in RFC 2131. The mobile node SHOULD
         generate and use the "Client-identifier" for each physical

         interface according to [RFC4361]. Any time the mobile node
         performs an handoff of a physical interface to a different
         mobile access gateway, using the same interface, the DHCP
         server will always be able to identify the binding using the
         presented identifier. The presented identifier (either the
         "Client-identifier" or the hardware address) will remain as the
         primary key for each binding, just as how they are unique in a
         Binding Cache entry.

      * If the mobile node is capable of performing handoff between
         interfaces, as per [RFC5213], a "Client-identifier" value MUST
         be used for the attachment point that is not tied to any of the
         physical interfaces. The identifier MUST be generated
         according to [RFC4361], which guarantees that the identifier is
         stable and unique across all "Client-identifier" values in use
         in the Proxy Mobile IPv6 domain.

   o All the DHCP servers co-located with the mobile access gateways in
      a Proxy Mobile IPv6 domain can be configured with the same set of
      DHCP option values (Ex: DNS Server, SIP Server ..etc.) to ensure
      the mobile node receives the same configuration values on any of
      the access links in that Proxy Mobile IPv6 domain.

3.4.1. DHCP Server co-located with the Mobile Access Gateway

   This section explains the operational sequence of home address
   assignment operation when the DHCP server is co-located with the
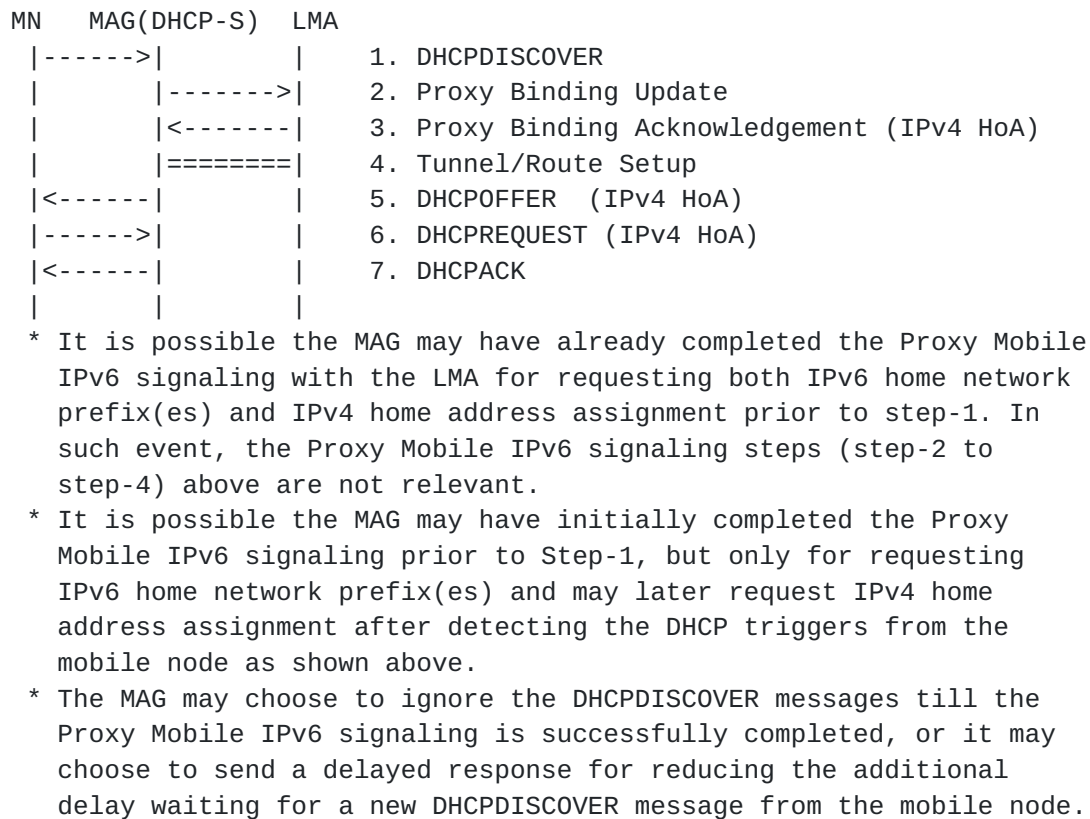   mobile access gateway.

```
    MN    MAG(DHCP-S)  LMA
     |------>|         |      1. DHCPDISCOVER
     |       |------->|      2. Proxy Binding Update
     |       |<-------|      3. Proxy Binding Acknowledgement (IPv4 HoA)
     |       |========|      4. Tunnel/Route Setup
     |<------|         |      5. DHCPOFFER  (IPv4 HoA)
     |------>|         |      6. DHCPREQUEST (IPv4 HoA)
     |<------|         |      7. DHCPACK
     |       |         |
```

   * It is possible the MAG may have already completed the Proxy Mobile
     IPv6 signaling with the LMA for requesting both IPv6 home network
     prefix(es) and IPv4 home address assignment prior to step-1. In
     such event, the Proxy Mobile IPv6 signaling steps (step-2 to
     step-4) above are not relevant.
   * It is possible the MAG may have initially completed the Proxy
     Mobile IPv6 signaling prior to Step-1, but only for requesting
     IPv6 home network prefix(es) and may later request IPv4 home
     address assignment after detecting the DHCP triggers from the
     mobile node as shown above.
   * The MAG may choose to ignore the DHCPDISCOVER messages till the
     Proxy Mobile IPv6 signaling is successfully completed, or it may
     choose to send a delayed response for reducing the additional
     delay waiting for a new DHCPDISCOVER message from the mobile node.

    Figure 7: Overview of DHCP Server located at Mobile Access Gateway

   Initial IPv4 Home Address Assignment:

   o For acquiring the mobile node's IPv4 home address from the local
      mobility anchor, the mobile access gateway will initiate Proxy
      Mobile IPv6 signaling with the local mobility anchor.

   o After the successful completion of the Proxy Mobile IPv6 signaling
      and upon acquiring the mobile node's IPv4 home address from the
      local mobility anchor, the DHCP server on the mobile access
      gateway will send a DHCPOFFER message [RFC2131] to the mobile
      node. The offered address will be the mobile node's IPv4 home
      address, assigned by the local mobility anchor. The DHCPOFFER
      message will also have the subnet mask option [RFC2132] and router
      option [RFC2132], with the values in those options set to the
      mobile node's IPv4 home subnet mask and default router address
      respectively. Additionally, the Server Identifier option will be
      included and with the value in the option set to the default
      router address.

   o If the mobile node sends the DHCPREQUEST message, the DHCP server
      will send DHCPACK message, as per [RFC2131].

IPv4 Home Address Renewal with the DHCP server (No Handoff):

o Any time the mobile node goes into the DHCP RENEWING state
   [RFC2131], it simply unicasts the DHCPREQUEST message including
   the assigned IPv4 home address in the 'requested IP address'
   option. The DHCPREQUEST is sent to the address specified in
   Server Identifier option of the previously received DHCPOFFER and
   DHCPACK messages.

o The DHCP server will send a DHCPACK to the mobile node to
   acknowledge the assignment of the committed IPv4 address.

IPv4 Home Address Renewal with the DHCP server (After Handoff):

When the mobile node goes into the DHCP RENEWING state [RFC2131], it
directly unicasts the DHCPREQUEST message to the DHCP server that
currently provided the DHCP lease. However, if the mobile node
changed its point of attachment and is attached to a new mobile
access gateway, it is required that the mobile node updates the DHCP
server address and uses the address of the DHCP server that is co-
located with the new mobile access gateway. The following approach
can be adopted to ensure the mobile node uses the DHCP server on the
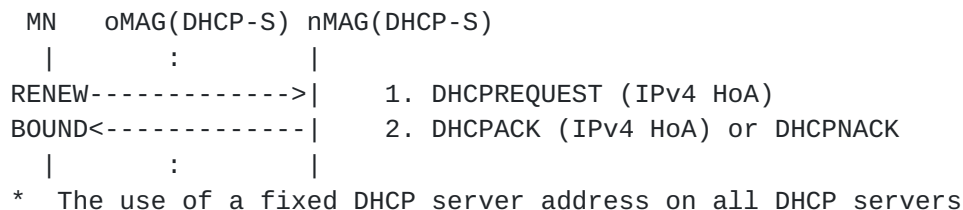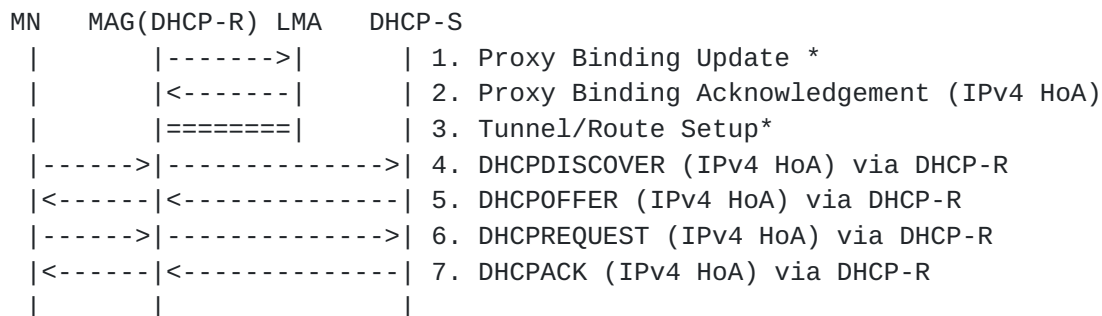attached link.


```
  MN    oMAG(DHCP-S) nMAG(DHCP-S)
    |        :        |
 RENEW------------->|    1. DHCPREQUEST (IPv4 HoA)
 BOUND<-------------|    2. DHCPACK (IPv4 HoA) or DHCPNACK
    |        :        |
  *  The use of a fixed DHCP server address on all DHCP servers
```


              Figure 8: Address renewal with the DHCP server

o The use of a stable address, either the IPv4 default router
   address of the mobile node, or a fixed IPv4 address common in that
   Proxy Mobile IPv6 domain, as the DHCP server Id will ensure the
   DHCPREQUEST message sent by the mobile node for renewing the
   address will be received by the new mobile access gateway on the
   attached link.

o The mobile access gateway after completing the Proxy Mobile IPv6
   signaling and upon acquiring the IPv4 home address of the mobile
   node will return the address in the DHCPACK message. However, if
   the mobile access gateway is unable to complete the Proxy Mobile
   IPv6 signaling or is unable to acquire the same IPv4 address as

requested by the mobile node, it will send a DHCPNACK message
[RFC2131] to the mobile node, as shown in Figure 8.

3.4.2. DHCP Relay Agent co-located with the Mobile Access Gateway

A DHCP relay agent is co-located with each mobile access gateway. A
DHCP server is located somewhere in the Proxy Mobile IPv6 domain
(e.g., is co-located with the local mobility anchor). Figure 9 shows
the sequence of IPv4 home address assignment using DHCP Relay.

```
MN    MAG(DHCP-R) LMA    DHCP-S
 |         |------->|        | 1. Proxy Binding Update *
 |         |<-------|        | 2. Proxy Binding Acknowledgement (IPv4 HoA)
 |         |=======|        | 3. Tunnel/Route Setup*
 |------>|------------->| 4. DHCPDISCOVER (IPv4 HoA) via DHCP-R
 |<------|<-------------| 5. DHCPOFFER (IPv4 HoA) via DHCP-R
 |------>|------------->| 6. DHCPREQUEST (IPv4 HoA) via DHCP-R
 |<------|<-------------| 7. DHCPACK (IPv4 HoA) via DHCP-R
 |       |              |
```
 * The Proxy Mobile IPv6 signaling (starting at Step-1) and the
   DHCP address configuration (starting at Step-4) may start in any
   order. However, the DHCPOFFER (Step-5) and the immediate steps
   following it will occur in the specified order and only after the
   Tunnel/Route Setup (Step-3).
 * It is possible the MAG may have initially completed the Proxy
   Mobile IPv6 signaling with the LMA only for requesting IPv6 home
   network prefix(es) and may later request IPv4 home address
   assignment after detecting the DHCP triggers from the mobile node
   (after Step-4).
 * The MAG may choose to ignore the DHCPDISCOVER messages till the
   Proxy Mobile IPv6 signaling is successfully completed, or it may
   choose to send a delayed response for reducing the additional
   delay waiting for a new DHCPDISCOVER message from the mobile node.

Figure 9: Overview of the DHCP relay located at mobile access gateway

Initial IPv4 Home Address Assignment:

o For acquiring the mobile node's IPv4 home address from the local
   mobility anchor, the mobile access gateway will initiate Proxy
   Mobile IPv6 signaling with the local mobility anchor.

o After the successful completion of the Proxy Mobile IPv6 signaling
   and upon acquiring the mobile node's IPv4 home address from the
   local mobility anchor, the mobile access gateway will enable
   forwarding for all the DHCP messages between the mobile node and

the DHCP server.

o The DHCP relay agent on the mobile access gateway will add the
   DHCP relay agent information option [RFC3046] to the DHCPDISCOVER
   message. The assigned IPv4 home address will be included in the
   Agent Remote ID Sub-option of the DHCP relay agent information
   option. This sub-option is used as a hint for requesting the DHCP
   server to allocate that specific IPv4 address.

o On receiving a DHCPOFFER message from the DHCP server, the mobile
   access gateway will ensure the assigned address is currently
   assigned by the local mobility anchor to that mobile node. If
   this address is different from what is assigned to the mobile
   node, then the mobile access gateway will drop the DHCPOFFER
   message and an administrative error message will be logged.

o When the DHCP messages are sent over administrative boundaries,
   the operators needs to ensure these messages are secured. All the
   DHCP messages relayed by the mobile access gateway can be tunneled
   to the local mobility anchor if needed. Alternatively, if the
   network in the Proxy Mobile IPv6 domain is secure enough, the
   mobile access gateway can just relay the DHCP messages to the
   server. To achieve this, all the mobile access gateways needs to
   have a route towards the DHCP server.

   IPv4 Home Address Renewal to the same DHCP server: (No Handoff)

o When the DHCP client goes into the DHCP RENEW STATE [RFC2131], it
   directly unicasts DHCPREQUEST messages to the DHCP server. The
   DHCP relay agent may not detect any changes in the DHCP state.
   For example, if the mobile node releases the IPv4 address, the
   relay agent would not be aware of it. The following describes
   additional mechanisms for the mobile access gateway to detect any
   changes in the DHCP state.

   * The DHCP relay agent can intercept all IPv4 DHCP packets
      destined to the set of addresses used within the Proxy Mobile
      IPv6 domain as DHCP addresses. Since the link between a mobile
      node and a mobile access gateway is the point-to-point link,
      the mobile access gateway will be in path for all the messages.

   * The DHCP relay agent can use the DHCP Server Identifier
      Override Sub-option [RFC5107] to be in path for all the DHCP
      message flows. The DHCP client uses the DHCP server address
      which is overridden by the DHCP relay agent address as a
      destination address of DHCPREQUEST. The DHCP Server Identifier
      Override Sub-option is recommended only when the fixed DHCP

   relay address is configured on all the mobile access gateways.
   Otherwise, the DHCP relay agent address is changed when the
   mobile node changes the attached mobile access gateway.

   o However, if the DHCP server is co-located with the local mobility
      anchor, then the DHCP relay agent is not required to intercept the
      unicast DHCP messages between the mobile node and the DHCP server.
      This is because the local mobility anchor will ensure that the
      DHCP state is consistent with the PMIPv6 binding that exists for
      the IPv4 address.

   o Once the mobile access gateway intercepts the DHCP message from
      the mobile node to the DHCP server, it can verify if the mobile
      node is negotiating the same IPv4 address that the local mobility
      anchor allocated for that mobile node. If the address in the
      DHCPREQUEST message does not match with the IPv4 address allocated
      for the mobile node, then the mobile access gateway SHOULD drop
      the DHCP message and an administrative error message can be
      logged.

   o Any time the mobile access gateway detects that the mobile node
      has released its IPv4 address, it can send a Proxy Binding Update
      to the local mobility anchor and de-register the IPv4 mobility
      session.

3.4.3. Common DHCP Considerations

   The following DHCP related considerations are common to both the
   supported configuration modes, specified in Section 3.4.1 and Section
   3.4.2.

   o When a mobile node sends a DHCPDISCOVER message [RFC2131], the
      DHCP server or the relay agent co-located with the mobile access
      gateway will trigger the mobile access gateway to complete the
      Proxy Mobile IPv6 signaling. This is the required interaction
      between these two protocols. The mobile access gateway on
      receiving this trigger will check if there is already an assigned
      IPv4 home address for the mobile node, from the local mobility
      anchor. If there is no assigned IPv4 home address assigned for
      that mobile node, the mobile access gateway will complete the
      Proxy Mobile IPv6 signaling with the local mobility anchor by
      sending a Proxy Binding Update message.

   o The mobile node needs to be identified by the MN-Identifier, as
      specified in Section 6.6 of [RFC5213]. This identity should be
      associated to the DHCP messages sent by the mobile node.

o The mobile access gateway will drop all the DHCPDISCOVER messages
   till it completes the Proxy Mobile IPv6 signaling. If the mobile
   access gateway is unable to complete the Proxy Mobile IPv6
   signaling, or, if the local mobility anchor does not assign an
   IPv4 address for the mobile node, the mobile access gateway MUST
   NOT enable IPv4 home address mobility support for the mobile node
   on that access link.

o The trigger for initiating Proxy Mobile IPv6 signaling can also be
   delivered to the mobile access gateway as part of a context
   transfer from the previous mobile access gateway, or delivered
   from the other network elements in the radio network, the details
   of which are outside the scope of this document.

o The DHCPOFFER message [RFC2131] sent to the mobile node MUST
   include the Subnet Mask option [RFC2132] and the Router option
   [RFC2132]. The values in the Subnet Mask option and Router option
   MUST be set to the mobile node's IPv4 home subnet mask and its
   default router address respectively.

o The DHCPOFFER message [RFC2131] sent to the mobile node MUST
   include the Interface MTU option [RFC2132]. The DHCP servers in
   the Proxy Mobile IPv6 domain MUST be configured to include the
   Interface MTU option. The MTU value SHOULD reflect the tunnel MTU
   for the bi-directional tunnel between the mobile access gateway
   and the local mobility anchor.

o The DHCP lease length allocated to the mobile node's IPv4 home
   address may be different from the binding lifetime at the local
   mobility anchor for that mobile node's session. It is not
   possible to keep these lifetimes synchronized and so its not
   required that the configured lifetimes should be kept same in both
   DHCP and Proxy Mobile IPv6.

o When the mobile node performs an handoff from one mobile access
   gateway to another, the mobile access gateway on the new link will
   initiate the Proxy Mobile IPv6 signaling with the local mobility
   anchor. On completing the Proxy Mobile IPv6 signaling, the mobile
   access gateway has the proper IPv4 address state that the local
   mobility anchor has allocated for the mobile node and which can be
   used for supporting DHCP based address configuration on that link.

o Any time the mobile node detects a link change event due to
   handoff, or due to other reasons such as re-establishment of the
   link-layer, the following are the mobile node's considerations
   with respect to the DHCP protocol.

        * If the mobile node is DNAv4 [RFC4436] capable and if it
           performs DNAv4 procedures after receiving a link change event,
           it would always detect the same default router on any of the
           access links in that Proxy Mobile IPv6 domain, as the mobile
           access gateway configures a fixed link-layer address on all the
           access links, as per the base Proxy Mobile IPv6 specification
           [RFC5213]. The mobile node will not perform any DHCP operation
           specifically due to this event.

        * If the mobile node is not DNAv4 [RFC4436] capable, after
           receiving the link change event it will enter INIT-REBOOT state
           [RFC2131] and will send a DHCPREQUEST message as specified in
           Section 3.7 of [RFC2131]. The mobile node will obtain the same
           address configuration as before, as the link change does not
           result in any change at the network layer.

   o The mobile node may release its IPv4 home address at any time by
      sending the DHCPRELEASE message [RFC2131]. When the mobile access
      gateway detects the DHCPRELEASE message sent by the mobile node,
      it should consider this as a trigger for de-registering the mobile
      node's IPv4 home address. It will apply the considerations
      specified in section 3.2.3.3 for performing the de-registration
      procedure. However, this operation MUST NOT release any IPv6 home
      network prefix(es) assigned to the mobile node.

4. **IPv4 Transport Support**

   The Proxy Mobile IPv6 specification [RFC5213] requires the signaling
   messages exchanged between the local mobility anchor and the mobile
   access gateway to be over an IPv6 transport. However, in some cases
   the local mobility anchor and the mobile access gateway are separated
   by an IPv4 network.

   The normal Proxy Mobile IPv6 specification [RFC5213] can be run over
   an IPv4 transport without any modifications by using a transition
   technology that allows IPv6 hosts to communicate over IPv4 networks.
   For example, the MAG and the LMA could have a simple configured IPv6-
   over-IPv4 tunnel. Instead of configured tunnels, various mechanisms
   for automatic tunneling could be used, too. To these tunnels, Proxy
   Mobile IPv6 would look just like any other application traffic
   running over IPv6.

   However, treating Proxy Mobile IPv6 just like any other IPv6 traffic
   would mean an extra layer of encapsulation for the mobile node's
   tunneled data traffic, adding 40 octets of overhead for each packet.
   The extensions defined in this section allow the MAG and the LMA to
   communicate over an IPv4 network without this overhead.

```
          IPv4-Proxy-CoA                        IPv4-LMAA
                |        + - - - - - - +          |
   +--+        +---+    /               \     +---+        +--+
   |MN|----------|MAG|=====   IPv4  Network  =====|LMA|----------|CN|
   +--+        +---+    \               /     +---+        +--+
                        + - - - - - - +
```
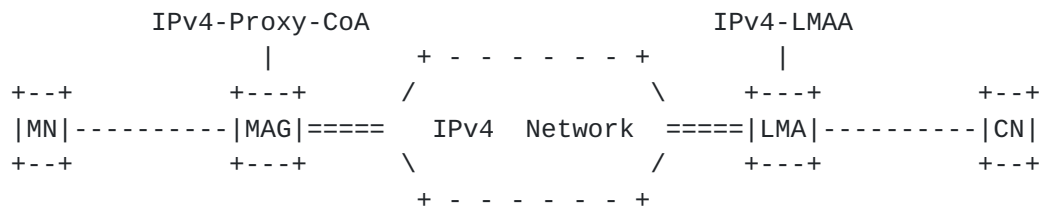
                   Figure 10: IPv4 Transport Network

   When the local mobility anchor and the mobile access gateway are
   configured and reachable using only IPv4 addresses, the mobile access
   gateway serving a mobile node can potentially send the signaling
   messages over IPv4 transport and register its IPv4 address as the
   care-of address in the mobile node's Binding Cache entry. An IPv4
   tunnel (with any of the supported encapsulation modes) can be used
   for tunneling the mobile node's data traffic. The following are the
   key aspects of this feature.

   o The local mobility anchor and the mobile access gateway are both
      configured and reachable using an IPv4 address of the same scope.

   o The IPv4 addresses used can be private IPv4 addresses, but it is
      assumed that there is no NAT between the LMA and the MAG.

      However, it is possible to use UDP encapsulation if other types of
      middleboxes are present.

   o The Mobility Header [RFC3775] is carried inside an IPv4 packet and
      UDP header, using an UDP port number for Proxy Mobile IPv6
      signalling over IPv4.

   o The mobile node can be an IPv6, IPv4 or a dual IPv4/IPv6 node and
      the IPv4 transport support specified in this section is agnostic
      to the type of address mobility enabled for that mobile node.

   o The mobile node's data traffic will be tunneled between the local
      mobility anchor and the mobile access gateway. There are several
      encapsulation modes available:

      * IPv4 (IPv4 or IPv6 Payload packet carried in an IPv4 packet).
         If payload protection using IPsec is enabled for the tunneled
         traffic, the ESP header follows the outer tunnel header.

      * IPv4-UDP (Payload packet carried in an IPv4 packet with UDP
         header, using a UDP port number for Proxy Mobile IPv6 data;
         this is different port than is used for signalling). If
         payload protection using IPsec is enabled, the ESP header
         follows the outer IPv4 header, as explained in Section 4.3.

      * IPv4-UDP-TLV (Payload packet carried in an IPv4 packet with UDP
         and TLV header) and IPv4-GRE (Payload packet carried in an IPv4
         packet with GRE header). Refer to
         [I-D.ietf-netlmm-grekey-option]. If payload protection using
         IPsec is enabled, the ESP header follows the outer IPv4 header,
         as explained in Section 4.3.

4.1. Local Mobility Anchor Considerations

4.1.1. Extensions to Binding Cache Entry

   To support this feature, the conceptual Binding Cache entry data
   structure maintained by the local mobility anchor [RFC5213] MUST be
   extended with the following additional parameters. It is to be noted
   that all of these parameters are specified in [RFC5555] and also
   required here in the present usage context, and are presented here
   only for completeness.

   o The IPv4 Proxy Care-of Address configured on the mobile access
      gateway that sent the Proxy Binding Update message. The address
      MUST be the same as the source address of the received IPv4 packet
      that contains the Proxy Binding Update message. However, if the
      received Proxy Binding Update message is not sent as an IPv4

packet, i.e., when using IPv6 transport, this field in the Binding
Cache entry MUST be set to ALL_ZERO value.

4.1.2. Extensions to Mobile Node's Policy Profile

To support the IPv4 Transport Support feature the mobile node's
policy profile, specified in Section 6.2 of [RFC5213] MUST be
extended with the following additional fields. These are mandatory
fields of the policy profile required for supporting this feature.

o The IPv4 address of the local mobility anchor (IPv4-LMAA).

4.1.3. Signaling Considerations

This section provides the rules for processing the Proxy Mobile IPv6
signaling messages received over IPv4 transport.

4.1.3.1. Processing Proxy Binding Updates

o If the Proxy Binding Update message is protected with IPsec ESP,
   IPsec processing happens before the packet is passed to Proxy
   Mobile IPv6.

o All the considerations from Section 5.3.1 of [RFC5213] except step
   1 (about IPsec) MUST be applied on the encapsulated Proxy Binding
   Update message. Note that the Checksum field in Mobility Header
   MUST be ignored.

o Upon accepting the request, the local mobility anchor MUST set up
   an IPv4 bi-directional tunnel to the mobile access gateway. The
   tunnel endpoint addresses are IPv4-LMAA and the IPv4-Proxy-CoA.
   The encapsulation mode MUST be determined by applying the
   following considerations:

   * If the (F) flag in the received Proxy Binding Update message is
      set to the value of (1), but if the configuration flag,
      AcceptForcedIPv4UDPEncapsulationRequest, is set to a value of
      (0), then the local mobility anchor MUST reject the request
      with the Status field value set to 129 (Administratively
      prohibited).

   * If the (T) flag is set to (1), or GRE Key option is included,
      see [I-D.ietf-netlmm-grekey-option].

   * If the (F) flag in the received Proxy Binding Update message is
      set to the value of (1), then the encapsulation mode MUST be
      set to IPv4-UDP. Otherwise the encapsulation mode MUST be set
      to IPv4.

o The local mobility anchor MUST send the Proxy Binding
   Acknowledgement message with the Status field value set to (0)
   (Proxy Binding Update Accepted). The message MUST be constructed
   as specified in Section 4.1.3.2.

4.1.3.2. Constructing the Proxy Binding Acknowledgement Message

The local mobility anchor when sending the Proxy Binding
Acknowledgement message to the mobile access gateway MUST construct
the message as specified in Section 5.3.6 of [RFC5213]. However, if
the Proxy Binding Update message was received over IPv4, the
following additional considerations MUST be applied.

o The IPv6 Header is removed, and the Mobility Header containing the
   Proxy Binding Acknowledgement is encapsulated in UDP (with source
   port set to TBD1 and destination port set to the source port of
   received Proxy Binding Update message). The Mobility Header
   Checksum field MUST be set to zero (and UDP checksum MUST be used
   instead).

o The source address in the IPv4 header of the message MUST be set
   to the destination IPv4 address of the received request.

o If IPsec ESP is used to protect signalling, the packet is
   processed using transport mode ESP as described in Section 4.3.

o Figure 11 shows the format of the Proxy Binding Acknowledgement
   message sent over IPv4 and protected using ESP.

   IPv4 header (src=IPv4-LMAA, dst=pbu_src_address)
     ESP header (in transport mode)
       UDP header (sport=TBD1, dport=TBD1)
         Mobility Header (PBA)

       Figure 11: Proxy Binding Acknowledgment (PBA) Message sent over
                                 IPv4

4.1.4. Routing Considerations

4.1.4.1. Forwarding Considerations

Forwarding Packets to the Mobile Node:

o On receiving an IPv4 or an IPv6 packet from a correspondent node
   with the destination address matching any of the mobile node's
   IPv4 or IPv6 home addresses, the local mobility anchor MUST

forward the packet through the bi-directional tunnel set up for
that mobile node.

o The format of the tunneled packet is shown below. The IPv4-UDP-
   TLV and IPv4-GRE encapsulation modes are described in
   [I-D.ietf-netlmm-grekey-option].


```
IPv4 Header (src=IPv4-LMAA, dst=IPv4-Proxy-CoA)] /* Tunnel Header */
  [UDP Header (src port=TBD2, dst port=TBD2]   /* If UDP encap nego */
   /* IPv6 or IPv4 Payload Packet */
   IPv6 header (src=CN, dst=MN-HOA)
     OR
   IPv4 header (src=CN, dst=IPv4-MN-HoA)
```


Figure 12: Tunneled IPv4 Packet from LMA to MAG (IPv4 or IPv4-UDP
                        encapsulation mode)

o Forwarding Packets Sent by the Mobile Node:

   * All the reverse tunneled packets (IPv4 and IPv6) that the local
      mobility anchor receives from the mobile access gateway, after
      removing the tunnel header (i.e., the outer IPv4 header along
      with the UDP and TLV header, if negotiated) MUST be routed to
      the destination specified in the inner packet header. These
      routed packets will have the source address field set to the
      mobile node's home address.

4.1.4.2. ECN & Payload Fragmentation Considerations

The ECN considerations specified in Section 5.6.3 of [RFC5213] apply
for the IPv4 transport tunnels as well. The mobility agents at the
tunnel entry and exit points MUST handle ECN information as specified
in that document.

The mobility agents at the tunnel entry and exit points MUST apply
the IP packet fragmentation considerations as specified in [RFC4213].
Additionally they MUST also apply the considerations related to
tunnel error processing and reporting as specified in the same
specification.

4.1.4.3. Bi-Directional Tunnel Management

The Tunnel Management considerations specified in section 5.6.1 of
[RFC5213] apply for the IPv4 transport tunnels as well, with just one
difference that the encapsulation mode is different.

4.2. **Mobile Access Gateway Considerations**

4.2.1. **Extensions to Binding Update List Entry**

   To support the IPv4 Transport Support feature, the conceptual Binding
   Update List entry data structure maintained by the mobile access
   gateway [RFC5213] MUST be extended with the following additional
   parameters.

   o The IPv4 address of the local mobility anchor. This address can
      be obtained from the mobile node's policy profile.

4.2.2. **Signaling Considerations**

   The mobile access gateway when sending a Proxy Binding Update message
   to the local mobility anchor MUST construct the message as specified
   in Section 6.9.1.5 of [RFC5213]. However, if the mobile access
   gateway is in an IPv4-only access network, the following additional
   considerations MUST be applied.

   o The Proxy Binding Update message MUST be sent over IPv4 as
      desribed in Section 4.2.2.1.

   o Just as specified in [RFC5213], when sending a Proxy Binding
      Update message for extending the lifetime of a currently existing
      mobility session or for de-registering the mobility session, the
      Proxy Binding Update message MUST be constructed just as the
      initial request.

   Receiving Proxy Binding Acknowledgement

   o If the received Proxy Binding Acknowledgement message is protected
      with IPsec ESP, IPsec processing happens before the packet is
      passed to Proxy Mobile IPv6. Considerations from Section 4 of
      [RFC5213] MUST be applied for authenticating and authorizing the
      message.

   o All the considerations from Section 6.9.1.2 of [RFC5213] MUST be
      applied on the encapsulated Proxy Binding Acknowledgement message.
      Note that the Checksum field in Mobility Header MUST be ignored.

   o If the Status field indicates Success, the mobile access gateway
      MUST setup a bi-directional tunnel to the local mobility anchor.

   o Upon accepting the request, the mobile access gateway MUST set up
      an IPv4 bi-directional tunnel to the local mobility anchor. The
      tunnel endpoint addresses are IPv4-Proxy-CoA and the IPv4-LMAA.

The encapsulation mode MUST be determined from the below
considerations:

* If the (T) flag is set to (1), or GRE Key option is included,
   see [I-D.ietf-netlmm-grekey-option].

* If there is a NAT Detection option [RFC5555] in the received
   Proxy Binding Acknowledgement message, and the (F) flag is set
   to value of (1), the encapsulation mode for the tunnel MUST be
   set to IPv4-UDP. Otherwise the encapsulation mode MUST be set
   to IPv4.

4.2.2.1. Constructing the Proxy Binding Update Message

o The IPv6 Header is removed, and the Mobility Header containing the
   Proxy Binding update message is encapsulated in UDP (with the
   destination port set to TBD1). The Mobility Header Checksum field
   MUST be set to zero (and UDP checksum MUST be used instead).

o The source address in the IPv4 header MUST be set to IPv4-Proxy-
   CoA of the mobile access gateway and the destination address MUST
   be set to the local mobility anchor's IPv4-LMAA.

o If the configuration variable ForceIPv4UDPEncapsulationSupport is
   set to value of (1), then the (F) flag in the Proxy Binding Update
   message MUST be set to value of (1).

o If IPsec ESP is used to protect signalling, the packet is
   processed using transport mode ESP as described in Section 4.3.

o Figure 13 shows the format of the Proxy Binding Update message
   sent over IPv4 and protected using ESP.


```
   IPv4 header (src=IPv4-Proxy-CoA, dst=IPv4-LMAA)
    ESP header (in transport mode)
      UDP header (sport=TBD1, dport=TBD1)
        Mobility Header (PBU)
```


        Figure 13: Proxy Binding Update (PBU) message sent over IPv4

4.2.2.2. Forwarding Considerations

Forwarding Packets Sent by the Mobile Node:

o On receiving an IPv4 or an IPv6 packet from the mobile node to any
   destination, the mobile access gateway MUST tunnel the packet to
   the local mobility anchor. The format of the tunneled packet is
   shown below. The IPv4-UDP-TLV and IPv4-GRE encapsulation modes
   are described in [I-D.ietf-netlmm-grekey-option]. However,
   considerations from Section 6.10.3 of [RFC5213] MUST be applied
   with respect the local routing and on the use of
   EnableMAGLocalRouting flag.

```
 IPv4 Header (src=IPv4-Proxy-CoA, dst=IPv4-LMAA)] /* Tunnel Header */
   [UDP Header (src port=TBD2, dst port=TBD2]   /* If UDP encap nego */
     /* IPv6 or IPv4 Payload Packet */
     IPv6 header (src=MN-HOA, dst=CN)
       OR
     IPv4 header (src=MN-HOA, dst=CN)
```

Figure 14: Tunneled IPv4 Packet from MAG to LMA (IPv4 or IPv4-UDP
                        encapsulation mode)

Forwarding Packets received from the bi-directional tunnel:

o On receiving a packet from the bi-directional tunnel established
   with the mobile node's local mobility anchor, the mobile access
   gateway MUST remove the outer header before forwarding the packet
   to the mobile node.

4.3. IPsec Considerations

4.3.1. PBU and PBA

The following section describes how IPsec is used for protecting the
signaling messages and data packets between the local mobility anchor
and mobile access gateway when using IPv4 transport.

The following are the SPD example entries to protect PBU and PBA on
the local mobility anchor and mobile access gateway.

```
        MAG SPD-S:
          - IF local_address = IPv4-Proxy-CoA_1 &
               remote_address = IPv4-LMAA_1 & proto = UDP &
               remote_port = TBD1
            Then use SA ESP transport mode

        LMA SPD-S:
          - IF local_address = IPv4-LMAA_1 &
               remote_address = IPv4-Proxy-CoA_1 & proto = UDP &
               local_port = TBD1
            Then use SA ESP transport mode
```

4.3.2. Payload Packet

The following are the SPD example entries to protect payload packets
on the local mobility anchor and mobile access gateway. Note that
the example SPDs protect all payload packets sent to and from mobile
nodes. If an operator needs to apply a different security mechanism
per mobile node, they need to create a SPD and a SA entry per mobile
node.

```
        MAG SPD-S:
          - IF interface = tunnel to LMAA_1 &
               local_address != Proxy-CoA_1 &
               remote_address != LMAA_1 & proto=any
            Then use SA ESP tunnel mode

        LMA SPD-S:
          - IF interface = tunnel to Proxy-CoA_1 &
               local_address != LMAA_1 &
               remote_address != Proxy-CoA_1 & proto=any
            Then use SA ESP tunnel mode
```

When payload packets are protected by IPsec, payload packets matching
to the SPDs are passed to the IPsec module and encapsulated using the
tunnel mode ESP. The tunnel mode ESP encapsulated payload packets
are then directly sent to the peer mobile access gateway or local
mobility anchor. If IPsec is not applied to payload packets, then
they are encapsulated as shown in Figures 12 and 14.

5. Protocol Configuration Variables

5.1. Local Mobility Anchor - Configuration Variables

   The local mobility anchor MUST allow the following variables to be
   configured by the system management. The configured values for these
   protocol variables MUST survive server reboots and service restarts.

   AcceptForcedIPv4UDPEncapsulationRequest

      This flag indicates whether or not the local mobility anchor
      should accept IPv4 UDP encapsulation request for the mobile node's
      data traffic. The default value for this flag is set to (0),
      indicating that plain IPv4 encapsulation (without UDP) is used for
      data traffic.

5.2. Mobile Access Gateway - Configuration Variables

   The mobile access gateway MUST allow the following variables to be
   configured by the system management. The configured values for these
   protocol variables MUST survive server reboots and service restarts.

   ForceIPv4UDPEncapsulationSupport

      This flag indicates whether or not the mobile access gateway
      should request the mobile node's local mobility anchor to use
      IPv4-UDP encapsulation mode for the mobile node's data traffic.
      The default value for this flag is set to (0), indicating that
      plain IPv4 encapsulation (without UDP) is used for data traffic.

6. IANA Considerations

   This document defines four new Mobility Header options, IPv4 Home
   Address Request option, IPv4 Home Address Reply option, IPv4 Default
   Router Address option and IPv4 DHCP Support Mode option. These
   options are described in Sections 3.3.1, 3.3.2, 3.3.3 and 3.3.4
   respectively. The Type value for these options needs to be assigned
   from the same number space as allocated for the other mobility
   options, as defined in [RFC3775].

   The IPv4 Home Address Reply option, described in Section 3.3.2 of
   this document, introduces a new number space, IPv4 Home Address Reply
   Status Codes. This document currently reserves the following values.
   Approval of any new status code values are to be made through IANA
   Expert Review.

   o 0 Success

   o 128 Failure, reason unspecified

   o 129 Administratively prohibited

   o 130 Incorrect IPv4 home address

   o 131 Invalid IPv4 address

   o 132 Dynamic IPv4 home address assignment not available

   The IPv4 DHCP Support Mode option, described in Section 3.3.4 of this
   document, introduces a new number space, IPv4 DHCP Support Mode
   Flags. This document reserves the value 0x1 for the (S) flag.
   Approval of this flag values are to be made through IANA Expert
   Review. At this point of time there are no thoughts on what the new
   flag allocations can be for and hence this document is leaving this
   to the discretion of the expert review.

   This document also defines new status values, used in Proxy Binding
   Acknowledgement message, as described in Section 3.3.5. These values
   are to be assigned from the same number space as allocated for other
   Status codes [RFC3775]. Each of these allocated values have to be
   greater than 128.

      NOT_AUTHORIZED_FOR_IPV4_MOBILITY_SERVICE: IANA

         Mobile node not authorized for IPv4 mobility service.

NOT_AUTHORIZED_FOR_IPV4_HOME_ADDRESS: IANA

Mobile node not authorized for the requesting IPv4 home address

NOT_AUTHORIZED_FOR_IPV6_MOBILITY_SERVICE: IANA

Mobile node not authorized for IPv6 mobility service.

MULTIPLE_IPV4_HOME_ADDRESS_ASSIGNMENT_NOT_SUPPORTED: IANA

Multiple IPv4 home address assignment not supported

IANA is requested to assign two UDP port numbers, TBD1 and TBD2, for "pmip6-cntl" and "pmip6-data", respectively.

7. Security Considerations

   All the security considerations from the base Proxy Mobile IPv6
   [RFC5213], Mobile IPv6 [RFC3775], and Dual-Stack Mobile IPv6
   [RFC5555] apply when using the extensions defined in this document.
   Additionally, the following security considerations need to be
   applied.

   This document defines new mobility options for supporting the IPv4
   Home Address assignment and IPv4 Transport Support features. These
   options are to be carried in Proxy Binding Update and Proxy Binding
   Acknowledgement messages. The required security mechanisms specified
   in the base Proxy Mobile IPv6 protocol for protecting these signaling
   messages are sufficient when carrying these mobility options.

   This specification describes the use of IPv4 transport for exchanging
   the signaling messages between the local mobility anchor and the
   mobile access gateway. These can be protected using IPsec as
   described in Section 4.3.

8. Contributors

   This document reflects discussions and contributions from several
   people (in alphabetical order):

   Kuntal Chowdhury

      kchowdhury@starentnetworks.com

   Vijay Devarapalli

      vijay.devarapalli@azairenet.com

   Sangjin Jeong

      sjjeong@etri.re.kr

   Basavaraj Patil

      basavaraj.patil@nokia.com

   Myungki Shin

      myungki.shin@gmail.com

9. Acknowledgments

   The IPv4 support for Proxy Mobile IPv6 was initially covered in the
   internet-draft [draft-sgundave-mip6-proxymip6-02.txt"/>. We would
   like to thank all the authors of the document and acknowledge that
   initial work.

   Thanks to Alper Yegin, Behcet Sarikaya, Bernard Aboba, Charles
   Perkins, Damic Damjan, Jari Arkko, Joel Hortelius, Jonne Soinnen,
   Julien Laganier, Mohana Jeyatharan, Niklas Nuemann, Pasi Eronen,
   Premec Domagoj, Ralph Droms, Sammy Touati, Vidya Narayanan, Yingzhe
   Wu and Zu Qiang for their helpful review of this document.

   Also, we would like to thank Spencer Dawkins, Tim Polk and Menachem
   Dodge, Adrian Farrel and Pekka Savola for their reviews of this
   document as part of the IESG review process. Finally, special thanks
   to Jouni Korohonen for his support in addressing the IPsec issues.

10. References

10.1. Normative References

[I-D.ietf-netlmm-grekey-option]
             Muhanna, A., Khalil, M., Gundavelli, S., and K. Leung,
             "GRE Key Option for Proxy Mobile IPv6",
             draft-ietf-netlmm-grekey-option-09 (work in progress),
             May 2009.

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

[RFC2131]   Droms, R., "Dynamic Host Configuration Protocol",
             RFC 2131, March 1997.

[RFC2132]   Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor
             Extensions", RFC 2132, March 1997.

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

[RFC3046]   Patrick, M., "DHCP Relay Agent Information Option",
             RFC 3046, January 2001.

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

[RFC4213]   Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms
             for IPv6 Hosts and Routers", RFC 4213, October 2005.

[RFC4361]   Lemon, T. and B. Sommerfeld, "Node-specific Client
             Identifiers for Dynamic Host Configuration Protocol
             Version Four (DHCPv4)", RFC 4361, February 2006.

[RFC5107]   Johnson, R., Kumarasamy, J., Kinnear, K., and M. Stapp,
             "DHCP Server Identifier Override Suboption", RFC 5107,
             February 2008.

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

[RFC5555]   Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and
             Routers", RFC 5555, June 2009.

10.2. Informative References

[RFC0925]   Postel, J., "Multi-LAN address resolution", RFC 925,
             October 1984.

   [RFC1332]   McGregor, G., "The PPP Internet Protocol Control Protocol
               (IPCP)", RFC 1332, May 1992.

   [RFC1918]   Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and
               E. Lear, "Address Allocation for Private Internets",
               BCP 5, RFC 1918, February 1996.

   [RFC3022]   Srisuresh, P. and K. Egevang, "Traditional IP Network
               Address Translator (Traditional NAT)", RFC 3022,
               January 2001.

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

   [RFC4436]   Aboba, B., Carlson, J., and S. Cheshire, "Detecting
               Network Attachment in IPv4 (DNAv4)", RFC 4436, March 2006.

   [RFC4977]   Tsirtsis, G. and H. Soliman, "Problem Statement: Dual
               Stack Mobility", RFC 4977, August 2007.

Authors' Addresses

   Ryuji Wakikawa
   TOYOTA InfoTechnology Center, U.S.A., Inc.
   465 Bernardo Avenue
   Mountain View, CA 94043
   USA

   Email: ryuji@us.toyota-itc.com

   Sri Gundavelli
   Cisco
   170 West Tasman Drive
   San Jose, CA 95134
   USA

   Email: sgundave@cisco.com