NETLMM WG S. Gundavelli
Internet-Draft K. Leung
Intended status: Standards Track Cisco
Expires: December 20, 2007 V. Devarapalli
Azaire Networks
K. Chowdhury
Starent Networks
B. Patil
Nokia Siemens Networks
June 18, 2007

Proxy Mobile IPv6
draft-ietf-netlmm-proxymip6-01.txt

Status of this Memo

Copyright Notice

Abstract

Host based IPv6 mobility is specified in Mobile IPv6 base specification [RFC3775]. In that model, the mobile node is

responsible for doing the signaling to its home agent to enable session continuity as it moves between subnets. The design principle in the case of host-based mobility relies on the mobile node being in control of the mobility management. Network based mobility allows IP session continuity for a mobile node without its involvement in mobility management. This specification describes a protocol solution for network based mobility management that relies on Mobile IPv6 signaling and reuse of home agent functionality. A proxy mobility agent in the network which manages the mobility for a mobile node is the reason for referring to this protocol as Proxy Mobile IPv6.

Table of Contents

1. Introduction

Mobile IPv6 [RFC-3775] is the enabler for IPv6 mobility. It requires Mobile IPv6 client functionality in the IPv6 stack of a mobile node. Signaling between the mobile node and home agent enables the creation and maintenance of a binding between the mobile node's home address and care-of-address. Mobile IPv6 has been designed to be an integral part of the IPv6 stack in a host. However there exist IPv6 stacks today that do not have Mobile IPv6 functionality and there would likely be IPv6 stacks without Mobile IPv6 client functionality in the future as well. It is desirable to support IP mobility for all hosts irrespective of the presence or absence of mobile IPv6 functionality in the IPv6 stack.

It is possible to support mobility for IPv6 nodes by extending Mobile IPv6 [RFC-3775] signaling and reusing the home agent via a proxy mobility agent in the network. This approach to supporting mobility does not require the mobile node to be involved in the signaling required for mobility management. The proxy mobility agent in the network performs the signaling and does the mobility management on behalf of the mobile node. Because of the use and extension of Mobile IPv6 signaling and home agent functionality, it is referred to as Proxy Mobile IPv6 (PMIP6) in the context of this document.

Network deployments which are designed to support mobility would be agnostic to the capability in the IPv6 stack of the nodes which it serves. IP mobility for nodes which have mobile IP client functionality in the IPv6 stack as well as those hosts which do not, would be supported by enabling Proxy Mobile IPv6 protocol functionality in the network. The advantages of developing a network based mobility protocol based on Mobile IPv6 are:

- Reuse of home agent functionality and the messages/format used in mobility signaling. Mobile IPv6 is a mature protocol with several implementations that have been through interoperability testing.

- A common home agent would serve as the mobility agent for all types of IPv6 nodes.

- Addresses a real deployment need.

The problem statement and the need for a network based mobility protocol solution has been documented in [RFC-4830]. Proxy Mobile

IPv6 is a solution that addresses these issues and requirements.

2. Conventions & Terminology

2.1. Conventions used in this document

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" used in this document are to be interpreted as described in RFC 2119.

2.2. Terminology

All the general mobility related terms used in this document are to be interpreted as defined in the Mobile IPv6 base specification [RFC-3775].

This document adopts the terms, Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG) from the NETLMM Goals document [RFC-4831]. This document also provides the following context specific explanation to the following terms used in this document.

Proxy Mobile IPv6 Domain (PMIPv6-Domain)

Proxy Mobile IPv6 domain refers to the network where the mobility management of a mobile node is handled using Proxy Mobile IPv6 protocol as defined in this specification. The Proxy Mobile IPv6 domain includes local mobility anchors and mobile access gateways between which security associations can be setup and authorization for sending Proxy Binding Updates on behalf of the mobile nodes can be ensured.

Local Mobility Anchor (LMA)

Local Mobility Anchor is the home agent for the mobile node in the Proxy Mobile IPv6 domain. It is the topological anchor point for the mobile node's home network prefix and is the entity that manages the mobile node's reachability state. It is important to understand that the local mobility anchor has the functional capabilities of a home agent as defined in Mobile IPv6 base specification [RFC-3775] and with the additional required capabilities for supporting Proxy Mobile IPv6 protocol as defined in this specification.

Mobile Access Gateway (MAG)

Mobile Access Gateway is a function that manages the mobility related signaling for a mobile node that is attached to its access link. It is responsible for tracking the mobile node's attachment to the link and for signaling the mobile node's local mobility anchor.

Mobile Node (MN)

Through out this document, the term mobile node is used to refer to an IP node whose mobility is managed by the network. The mobile node may be operating in IPv6 mode, IPv4 mode or in IPv4/IPv6 dual mode. The mobile node is not required to participate in any mobility related signaling for achieving mobility for an IP address that is obtained in that local domain. This document further uses explicit text when referring to a mobile node that is involved in mobility related signaling as per Mobile IPv6 specification [RFC-3775].

LMA Address (LMAA)

The address that is configured on the interface of the local mobility anchor and is the transport endpoint of the tunnel between the local mobility anchor and the mobile access gateway. This is the address to where the mobile access gateway sends the Proxy Binding Update messages. When supporting IPv4 traversal, i.e. when the network between the local mobility anchor and the mobile access gateway is an IPv4 network, this address will be an IPv4 address and will be referred to as IPv4-LMAA, as specified in [ID-IPV4-PMIP6].

Proxy Care-of Address (Proxy-CoA)

Proxy-CoA is the address configured on the interface of the mobile access gateway and is the transport endpoint of the tunnel between the local mobility anchor and the mobile access gateway. The local mobility anchor views this address as the Care-of Address of the mobile node and registers it in the Binding Cache entry for that mobile node. When the transport network between the mobile access gateway and the local mobility anchor is an IPv4 network and if the care-of address that is registered at the local mobility anchor is an IPv4 address, the term, IPv4-Proxy-CoA is used, as defined in [ID-IPV4-PMIP6].

Mobile Node's Home Address (MN-HoA)

MN-HoA is the home address of a mobile node in a Proxy Mobile IPv6 domain. It is an address obtained by the mobile node in that domain. The mobile node can continue to use this address as long as it is attached to the network that is in the scope of that Proxy Mobile IPv6 domain.

Mobile Node's Home Network Prefix (MN-HNP)

This is the on-link IPv6 prefix that the mobile node always sees in the Proxy Mobile IPv6 domain. The home network prefix is topologically anchored at the mobile node's local mobility anchor. The mobile node configures its interface with an address from this prefix.

Mobile Node's Home Link

This is the link on which the mobile node obtained its initial address configuration after it moved into that Proxy Mobile IPv6 domain. This is the link that conceptually follows the mobile node. The network will ensure the mobile node always sees this link with respect to the layer-3 network configuration, on any access link that it attaches to in that proxy mobile IPv6 domain.

Mobile Node Identifier (MN-Identifier)

The identity of the mobile node that is presented to the network as part of the access authentication. This is typically an identifier such as Mobile Node NAI [RFC-4283], or any other type of identifier which may be specific to the access technology.

Proxy Binding Update (PBU)

A signaling message sent by the mobile access gateway to a mobile node's local mobility anchor for establishing a binding between the mobile node's MN-HoA and the Proxy-CoA.

Proxy Binding Acknowledgement (PBA)

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

3. Proxy Mobile IPv6 Protocol Overview

This specification describes a network-based mobility management protocol. It is called Proxy Mobile IPv6 and is based on Mobile IPv6 [RFC-3775]. This protocol is for providing network-based mobility

management support to a mobile node, within a restricted and topologically localized portion of the network and with out requiring the participation of the mobile node in any mobility related signaling.

Every mobile node that roams in a Proxy Mobile IPv6 domain, would typically be identified by an identifier, MN-Identifier, and using that identifier the mobile node's policy profile can be obtained from the policy store. The policy profile typically contains the provisioned network-based mobility service characteristics and other related parameters such as the mobile node's Identifier, local mobility anchor address, permitted address configuration modes, roaming policy and other parameters that are essential for providing the network based mobility service.

Once a mobile node enters its Proxy Mobile IPv6 domain and performs access authentication, the network will ensure that the mobile node is always on its home network and can obtain its home address on any access link using any of the address configuration procedures. In other words, there is a home network prefix that is assigned to a mobile node and conceptually that address always follows the mobile node, where ever it roams within that Proxy Mobile IPv6 domain. From the perspective of the mobile node, the entire Proxy Mobile IPv6 domain appears as its home link or a single link.

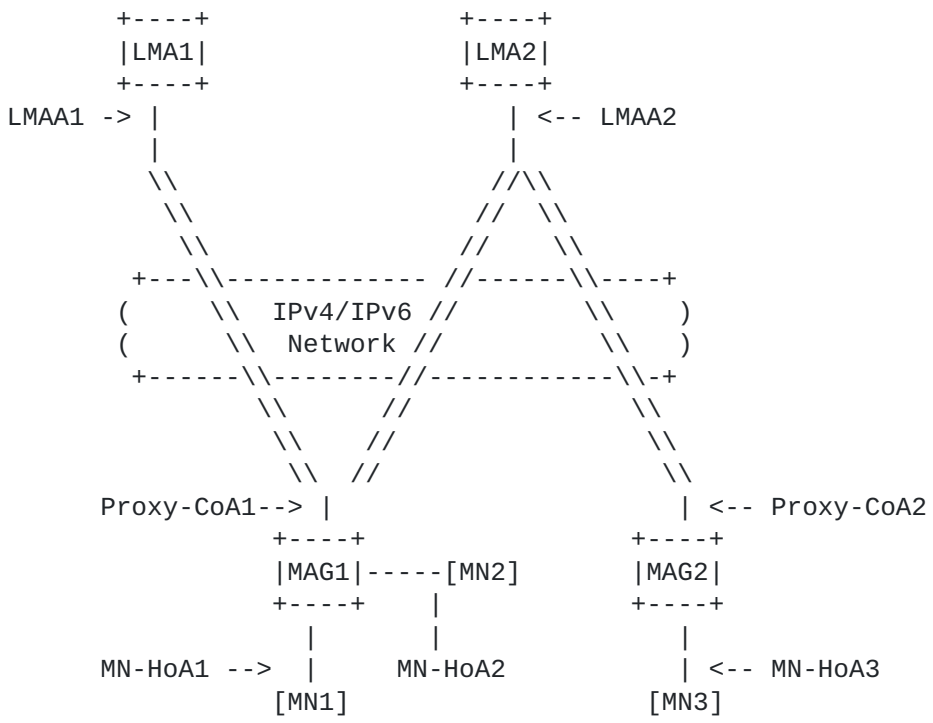


Figure 1: Proxy Mobile IPv6 Domain

The Proxy Mobile IPv6 scheme introduces a new function, the mobile access gateway. It is a function that is on the access link where the mobile node is anchored and does the mobility related signaling on its behalf. From the perspective of the local mobility anchor, the mobile access gateway is a special element in the network that is authorized to send Mobile IPv6 signaling messages on behalf of other mobile nodes.

When the mobile node attaches to an access link connected to the mobile access gateway, the mobile node presents its identity, MN-Identifier, as part of the access authentication procedure. After a successful access authentication, the mobile access gateway obtains the mobile node's profile from the policy store. The mobile access gateway would have all the required information for it to emulate the mobile node's home network on the access link. It sends Router Advertisement messages to the mobile node on the access link advertising the mobile node's home network prefix as the hosted on-link-prefix.

The mobile node on receiving these Router Advertisement messages on the access link will attempt to configure its interface either using stateful or stateless address configuration modes, based on modes that are permitted on that access link. At the end of a successful address configuration procedure, the mobile node would have obtained an address from its home network prefix. If the mobile node is IPv4 capable and if network offers IPv4 network mobility for the mobile node, the mobile node would have obtained an IPv4 address as well. The mobile node can be operating in IPv4-only mode, IPv6-only or in dual-mode and based on the services enabled for that mobile, the mobility is enabled only for those address types. Also, the network between the local mobility anchor and the mobile access gateway can be either IPv4, IPv6 or a private IPv4 with NAT translation devices.

For updating the local mobility anchor about the current location of the mobile node, the mobile access gateway sends a Proxy Binding Update message to the mobile node's local mobility anchor. The message will have the mobile node's NAI identifier option and other required options. Upon accepting the Proxy Binding Update message, the local mobility anchor sends a Proxy Binding Acknowledgment message including the mobile node's home network prefix option. It also sets up a route for the mobile node's home network prefix over the tunnel to the mobile access gateway.

The mobile access gateway on receiving this Proxy Binding Acknowledgment message sets up a bi-directional tunnel to the local mobility anchor and adds a default route over the tunnel to the local mobility anchor. All traffic from the mobile node gets routed to its local mobility anchor through the bi-directional tunnel.

At this point, the mobile node has a valid address from its home network prefix, at the current point of attachment. The serving mobile access gateway and the local mobility anchor also have proper routing states for handling the traffic sent to and from the mobile node using an address from its home network prefix.

The local mobility anchor, being the topological anchor point for the mobile node's home network prefix, receives any packet that is sent by any corresponding node to the mobile node. Local mobility anchor forwards the received packet to the mobile access gateway through the bi-directional tunnel. The mobile access gateway on other end of the tunnel, after receiving the packet, removes the outer header and forwards the packet on the access link to the mobile node.

The mobile access gateway typically acts as a default router on the access link and any packet that the mobile node sends to any corresponding node is received by the mobile access gateway and it

forwards the packet to its local mobility anchor through the bi-

directional tunnel. The local mobility anchor on the other end of the tunnel, after receiving the packet removes the outer header and routes the packet to the destination.

4. Proxy Mobile IPv6 Protocol Security

The signaling messages, Proxy Binding Update and Proxy Binding Acknowledgement, exchanged between the mobile access gateway and the local mobility anchor are protected using IPsec and using the established security association between them. The security association of the specific mobile node for which the signaling message is initiated is not required for protecting these messages.

ESP in transport mode with mandatory integrity protection is used for protecting the signaling messages. Confidentiality protection is not required.

IKEv2 is used to setup security associations between the mobile access gateway and the local mobility anchor to protect the Proxy Binding Update and Proxy Binding Acknowledgment messages. The mobile access gateway and the local mobility anchor can use any of the authentication mechanisms, as specified in IKEv2, for mutual authentication.

Mobile IPv6 specification requires the home agent to prevent a mobile node from creating security associations or creating binding cache entries for another mobile node's home address. In the protocol described in this document, the mobile node is not involved in creating security associations for protecting the signaling messages or sending binding updates. Therefore, this is not a concern. However, the local mobility anchor MUST allow only authorized mobile access gateways to create binding cache entries on behalf of the mobile nodes. The actual mechanism by which the local mobility anchor verifies if a specific mobile access gateway is authorized to send Proxy Binding Updates on behalf of a mobile node is outside the scope of this document. One possible way this could be achieved is sending a query to the policy store such as by using AAA infrastructure.

4.1. Peer Authorization Database Entries

The following describes PAD entries on the mobile access gateway and the local mobility anchor. The PAD entries are only example configurations. Note that the PAD is a logical concept and a particular mobile access gateway or a local mobility anchor implementation can implement the PAD in an implementation specific

manner. The PAD state may also be distributed across various databases in a specific implementation.

```
    mobile access gateway PAD:
      - IF remote_identity = lma_identity_1
           Then authenticate (shared secret/certificate/EAP)
           and authorize CHILD_SA for remote address lma_addres_1

    local mobility anchor PAD:
      - IF remote_identity = mag_identity_1
           Then authenticate (shared secret/certificate/EAP)
           and authorize CHILD_SAs for remote address mag_address_1
```

The list of authentication mechanisms in the above examples is not exhaustive. There could be other credentials used for authentication stored in the PAD.

4.2. Security Policy Database Entries

The following describes the security policy entries on the mobile access gateway and the local mobility anchor required to protect the Proxy Mobile IPv6 signaling messages. The SPD entries are only example configurations. A particular mobile access gateway or a local mobility anchor implementation could configure different SPD entries as long as they provide the required security.

In the examples shown below, the identity of the mobile access gateway is assumed to be mag_1, the address of the mobile access gateway is assumed to be mag_address_1, and the address of the local mobility anchor is assumed to be lma_address_1.

```
   mobile access gateway SPD-S:
     - IF local_address = mag_address_1 &
          remote_address = lma_address_1 &
          proto = MH & local_mh_type = BU & remote_mh_type = BAck
       Then use SA ESP transport mode
       Initiate using IDi = mag_1 to address lma_1

   local mobility anchor SPD-S:
     - IF local_address = lma_address_1 &
          remote_address = mag_address_1 &
          proto = MH & local_mh_type = BAck & remote_mh_type = BU
       Then use SA ESP transport mode
```

5. Local Mobility Anchor Operation

For supporting the Proxy Mobile IPv6 scheme specified in this document, the Mobile IPv6 home agent entity, defined in Mobile IPv6 specification [RFC-3775], needs some enhancements. The local mobility anchor is an entity that has the functional capabilities of a home agent and with the additional required capabilities for supporting Proxy Mobile IPv6 protocol as defined in this specification. This section describes the operational details of the local mobility anchor.

The base Mobile IPv6 specification [RFC-3775], defines home agent and the mobile node as the two functional entities. The Proxy Mobile IPv6 scheme introduces a new entity, the mobile access gateway. This is the entity that will participate in the mobility related signaling. From the perspective of the local mobility anchor, the mobile access gateway is a special element in the network that has the privileges to send mobility related signaling messages on behalf of the mobile node. Typically, the local mobility anchor is provisioned with the list of mobile access gateways authorized to send proxy registrations.

When the local mobility anchor receives a Proxy Binding Update message from a mobile access gateway, the message is protected using the IPSec Security Association established between the local mobility anchor and the mobile access gateway. The local mobility anchor can distinguish between a Proxy Binding Update message received from a mobile access gateway from a Binding Update message received directly from a mobile node. This distinction is important for using the right security association for validating the Binding Update and this is achieved by relaxing the MUST requirement for having the Home Address Option presence in Destination Options header and by introducing a new flag in the Binding Update message. The local mobility anchor as a traditional IPSec peer can use the SPI in the IPSec header [RFC-4306] of the received packet for locating the correct security association and for processing the Proxy Binding Update message in the context of the Proxy Mobile IPv6 scheme.

For protocol simplicity, the current specification supports the Per-MN-Prefix addressing model. In this addressing model, each mobile node is allocated an exclusively unique home network prefix. The local mobility anchor in this model is just a topological anchor point for that prefix and the prefix is physically hosted on the access link where the mobile node is attached. The local mobility anchor is not required to perform any proxy ND operations [RFC-2461] for defending the mobile node's home address on the home link.

However, the local mobility anchor is required to manage the binding cache entry of the mobile node for managing the mobility session and

also the routing state for creating a proper route path for traffic to/from the mobile node.

5.1. Extensions to Binding Cache Conceptual Data Structure

The local mobility anchor maintains a Binding Cache entry for each currently registered mobile node. Binding Cache is a conceptual data structure, described in Section 9.1 of [RFC-3775]. For supporting this specification, the conceptual Binding Cache entry needs to be extended with the following additional fields.

- A flag indicating whether or not this Binding Cache entry is created due to a proxy registration. This flag is enabled for Binding Cache entries that are proxy registrations and is turned off for all other entries that are direct registrations from the mobile node.

- The identifier of the mobile node, MN-Identifier. This MN-Identifier is obtained from the NAI Option present in the Proxy Binding Update request [RFC-4285].

- A flag indicating whether or not the Binding Cache entry has a home address that is on virtual interface. This flag is enabled, if the home prefix of the mobile node is configured on a virtual interface. When the configured home prefix of a mobile is on a virtual interface, the home agent is not required to function as a Neighbor Discovery proxy for the mobile node.

- The IPv6 home network prefix of the mobile node.

- The IPv6 home network prefix length of the mobile node.

- The interface id of the bi-directional tunnel between the local mobility anchor and the mobile access gateway used for sending and receiving the mobile node's traffic.

5.2. Bi-Directional Tunnel Management

The bi-directional tunnel between the local mobility anchor and the mobile access gateway is used for routing the traffic to and from the mobile node. The tunnel hides the topology and enables a mobile node to use an IP address that is topologically anchored at the local mobility anchor, from any attached access link in that proxy mobile IPv6 domain. The base Mobile IPv6 specification [RFC-3775], does use the tunneling scheme for routing traffic to and from the mobile that

is using its home address. However, there are subtle differences in the way Proxy Mobile IPv6 uses the tunneling scheme.

As in Mobile IPv4 [RFC-3344], the tunnel between the local mobility anchor and the mobile access gateway is typically a shared tunnel and can be used for routing traffic streams for different mobile nodes attached to the same mobile access gateway. This specification extends that 1:1 relation between a tunnel and a binding cache entry to 1:m relation, reflecting the shared nature of the tunnel.

The tunnel is creating after accepting a Proxy Binding Update message for a mobile node from a mobile access gateway. The created tunnel may be shared with other mobile nodes attached to the same mobile access gateway and with the local mobility anchor having a binding cache entry for those mobile nodes. Some implementations may prefer to use static tunnels as supposed to creating and tearing them down on a need basis.

The one end point of the tunnel is the address configured on the interface of the local mobility anchor, LMAA. The other end point of the tunnel is the address configured on the interface of the mobile access gateway, Proxy-CoA. The details related to the supported encapsulation modes and transport protocols is covered in detail in Section 6.10.2.

Implementations typically use a software timer for managing the tunnel lifetime and a counter for keeping a count of all the mobiles that are sharing the tunnel. The timer value will be set to the accepted binding life-time and will be updated after each periodic registrations for extending the lifetime. If the tunnel is shared for multiple mobile node's traffic, the tunnel lifetime will be set to the highest binding life time across all the binding life time that is granted for all the mobiles sharing that tunnel.

5.3. Routing Considerations

This section describes how the data traffic to/from the mobile node is handled at the local mobility anchor.

When a local mobility anchor is serving a mobile node, it MUST attempt to intercept packets that are sent to any address that is in the mobile node's home network prefix address range. The local mobility anchor MUST advertise a connected route in to the Routing Infrastructure for that mobile node's home network prefix or for an aggregated prefix with a larger scope. This essentially enables routers in the IPv6 network to detect the local mobility anchor as the last-hop router for that prefix.

When forwarding any packets that have the destination address matching the mobile node's home network prefix, the local mobility anchor MUST encapsulate the packet with the outer IPv6 header, as

specified in Generic Packet Tunneling in IPv6 specification [RFC-2473]. If the negotiated encapsulation header is either IPv6-over-IPv4 or IPv6-over-IPv4-UDP, as specified in the companion document, IPv4 support for Proxy Mobile IP6 [ID-Pv4-PMIP6], the packet must be encapsulated and routed as specified in that specification.

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

5.4. Local Mobility Anchor Address Discovery

Dynamic Home Agent Address Discovery, as explained in Section 10.5 of [RFC-3775], allows a mobile node to discover all the home agents on its home link by sending an ICMP Home Agent Address Discovery Request message to the Mobile IPv6 Home-Agents anycast address, derived from its home network prefix.

In Proxy Mobile IPv6, the address of the local mobility anchor configured to serve a mobile node can be discovered by the mobility entities in one or more ways. This MAY be a configured entry in the mobile node's policy profile, or it MAY be obtained through mechanisms outside the scope of this document. It is important to note that there is little value in using DHAAD message in the current form for discovering the local mobility anchor address dynamically. As a mobile node moves from one mobile access gateway to the another, the serving mobile access gateway will not predictably be able to locate the serving local mobility anchor for that mobile that has its binding cache entry for the mobile node. Hence, this specification does not support Dynamic Home Agent Address Discovery protocol.

5.5. Sequence Number and Time-Stamps for Message Ordering

Mobile IPv6 [RFC-3775] uses the Sequence Number field in registration messages as a way to ensure the correct packet ordering. The local mobility anchor and the mobile node are required to manage this counter over the lifetime of a binding.

In Proxy Mobile IPv6, the Proxy Binding Update messages that the local mobility anchor receives on behalf of a specific mobile node may not be from the same mobile access gateway as the previously received message. It creates certain ambiguity and the local mobility anchor will not be predictably order the messages. This could lead to the local mobility anchor processing an older message

from a mobile access gateway where the mobile node was previously attached, while ignoring the latest binding update message.

In the Proxy Mobile IPv6, the ordering of packets has to be established across packets received from multiple senders. The sequence number scheme as specified in [RFC-3775] will not be sufficient. A global scale, such as a time stamp, can be used to ensure the correct ordering of the packets. This document proposes the use of a Time Stamp Option, specified in Section 8.4, in all Proxy Binding Update messages sent by mobile access gateways. By leveraging the NTP [RFC-1305] service, all the entities in Proxy Mobile IPv6 domain will be able to synchronize their respective clocks. Having a time stamp option in Proxy Binding Update messages will enable the local mobility anchor to predictably identify the latest message from a list of messages delivered in an out-of-order fashion.

The Proxy Mobile IPv6 model, defined in this document requires the Proxy Binding Update messages sent by the mobile access gateway to have the Time Stamp option. The local mobility anchor processing a proxy registration MUST ignore the sequence number field and MUST the value from the Time Stamp option to establish ordering of the received Binding Update messages. If the local mobility anchor receives a Proxy Binding Update message with an invalid Time Stamp Option, the Proxy Binding Update MUST be rejected and a Proxy Binding Acknowledgement MUST be returned in which the Status field is set to 148 (invalid time stamp option).

In the absence of Time Stamp option in the Proxy Binding Update, the entities can fall back to Sequence Number scheme for message ordering, as defined in RFC-3775. However, the specifics on how different mobile access gateways synchronize the sequence number is outside the scope of this document.

When using the Time Stamp Option, the local mobility anchor or the mobile access gateway MUST set the timestamp field to a 64-bit value formatted as specified by the Network Time Protocol [RFC-1305]. The low-order 32 bits of the NTP format represent fractional seconds, and those bits which are not available from a time source SHOULD be generated from a good source of randomness.

5.6. Route Optimizations Considerations

Mobile IPv6 route optimization, as defined in [RFC-3775], enables a mobile node to communicate with a corresponding node directly using its care-of address and further the Return Routability procedure enables the corresponding node to have reasonable trust that the mobile node owns both the home address and care-of address.

In the Proxy Mobile IPv6 model, the mobile is not involved in any mobility related signaling and also it does not operate in the dual-

address mode. Hence, the return routability procedure as defined in RFC-3775 is not applicable for the proxy model.

5.7. Mobile Prefix Discovery Considerations

The ICMP Mobile Prefix Advertisement message, described in Section 6.8 and Section 11.4.3 of [RFC-3775], allows a home agent to send a Mobile Prefix Advertisement to the mobile node.

In Proxy Mobile IPv6, the mobile node's home network prefix is hosted on the access link connected to the mobile access gateway. but topologically anchored on the local mobility anchor. Since, there is no physical home-link for the mobile node's home network prefix on the local mobility anchor and as the mobile is always on the link where the prefix is hosted, any prefix change messages can just be advertised by the mobile access gateway on the access link and thus there is no applicability of this message for Proxy Mobile IPv6. This specification does not use Mobile Prefix Discovery.

5.8. Signaling Considerations

5.8.1. Initial Proxy Binding Registration

Upon receiving a Proxy Binding Update message from a mobile access gateway on behalf of mobile node, the local mobility anchor MUST process the request as defined in Section 10, of the base Mobile IPv6 specification [RFC-3775], with one exception that this request is a proxy request, the sender is not the mobile node and so the message has to be processed with the considerations explained in this section.

The local mobility anchor MUST apply the required policy checks, as explained in Section 4.0 of this document to verify the sender is a trusted mobile access gateway, authorized to send Proxy Binding Updates requests on behalf of that mobile nodes, using its own identity. The local mobility anchor must check the local/remote policy store to ensure the requesting node is authorized to send Proxy Binding Update messages.

The local mobility anchor MUST use the MN-Identifier from the NAI option of the Proxy Binding Update message for identifying the mobile node.

The local mobility anchor MUST ignore the sequence number field in the Proxy Binding Updates requests, if the Time-Stamp Option is present in the message. It must also skip all the checks related to sequence number that are required as per the Mobile IPv6 specification [RFC-3775]. However, the received sequence number

MUST

be copied and returned in the Proxy Binding Acknowledgement message sent to the mobile access gateway.

The local mobility anchor before accepting a Proxy Binding Update request containing the Home Network Prefix Option with a specific prefix, MUST ensure the prefix is owned by the local mobility anchor and further the mobile node is authorized to use that prefix. If the Home Network Prefix Option has the value 0::/0, the local mobility anchor MUST allocate a prefix for the mobile node and send a Proxy Binding Acknowledgement message with the Home Network Prefix Option containing the allocated value. The specific details on how the local mobility anchor allocates the home network prefix is outside the scope of this document.

Upon accepting a Proxy Binding Update request from a mobile access gateway, the local mobility anchor must check if there exists a binding cache entry for that mobile node, identified using the MN-Identifier, that was created due to a direct registration from the mobile node. If there exists a binding cache entry with the proxy registration flag turned off, the local mobility anchor MUST NOT modify that binding state, instead it must create a tentative binding cache entry and update the tentative binding cache entry fields of that binding cache entry.

Upon receiving a Binding Update request from a mobile node with lifetime value set to 0, from a tunnel between itself and a trusted mobile access gateway, the local mobility anchor upon accepting that de-registration message, MUST forward the Binding Acknowledgement message in the tunnel from where it received the Binding Update request. It must also replace the binding cache entry with the tentative binding cache entry and enable routing for the mobile node's home network prefix through the proxy mobile IPv6 tunnel.

Upon accepting this Proxy Binding Update message, the local mobility anchor must create a Binding Cache entry and must set up a tunnel to the mobile access gateway serving the mobile node. This bi-directional tunnel between the local mobility anchor and the mobile access gateway is used for routing the mobile node's traffic.

The Proxy Binding Acknowledgment message must be constructed as shown below.

```
IPv6 header (src=LMAA, dst=Proxy-CoA)
     Mobility header
         -BA /*P flag is set*/
        Mobility Options
           - Home Network Prefix Option
```

- TimeStamp Option (optional)
- NAI Option

Proxy Binding Acknowledgment message contents

5.8.2. Extending the binding lifetime

Upon accepting the Proxy Binding Update request for extending the lifetime of a currently active binding, the local mobility anchor MUST update the lifetime for that binding and send a Proxy Binding Acknowledgment message to the mobile access gateway. The Proxy Binding Acknowledgment message MUST be constructed as specified in Section 5.8.1.

5.8.3. De-registration of the binding

Upon accepting the Proxy Binding Update request sent with the lifetime value of zero, the local mobility anchor MUST delete the binding from its Binding Cache and MUST send a Proxy Binding Acknowledgment message to the mobile access gateway. The message MUST be constructed as specified in Section 6.9.1.

The local mobility anchor MUST also remove the prefix route over the tunnel for that mobile node's home network prefix.

5.9. Local Mobility Anchor Operational Summary

- For supporting this scheme, the local mobility anchor MUST satisfy all the requirements listed in Section 8.4 of Mobile IPv6 specification [RFC-3775] with the following considerations.

- For supporting the per-MN-Prefix addressing model as defined in this specification, the local mobility anchor service MUST NOT be tied to a specific interface. It SHOULD be able to accept Proxy Binding Update requests sent to any of the addresses configured on any of its interfaces.

- The requirement for a home agent to maintain a list of home agents for a mobile node's home link is not applicable for the local mobility anchor, when supporting Per-MN-Prefix addressing model.

- The local mobility anchors SHOULD drop all HoTI messages received for a home address that has corresponding Binding Cache entry with the proxy registration flag set.

- The local mobility anchor must handle the mobile node's data traffic as explained in the Routing Considerations section of

this

document.

6. Mobile Access Gateway Operation

The Proxy Mobile IPv6 scheme specified in this document, introduces a new functional entity, the Mobile Access Gateway (MAG). It is the entity that detects the mobile node's movements and initiates the signaling with the mobile node's local mobility anchor for updating the route to the mobile node's home address. In essence, the mobile access gateway performs mobility management on behalf of the mobile node.

From the perspective of the local mobility anchor, the mobile access gateway is a special element in the network that sends Mobile IPv6 signaling messages on behalf of a mobile node, but using its own identity. It is the entity that binds the mobile node's home address to an address on its own access interface.

The mobile access gateway has the following functional roles.

- Responsible for detecting the mobile node's attachment or detachment on the connected access link and for initiating the mobility signaling with the mobile node's local mobility anchor.

- Emulation of the mobile node's home link on the access link.

- Registering the binding state at the mobile node's local mobility anchor.

- Responsible for setting up the data path for enabling the mobile node to use an address from its home network prefix and use it from the access link.

The mobile access gateway is a function that typically runs on an access router. However, implementations MAY choose to split this function and run it across multiple systems. The specifics on how that is achieved is beyond the scope of this document.

6.1. Supported Access Link Types

This specification supports only point-to-point access link types and thus it assumes that the link between the mobile node and the mobile access gateway is a dedicated link and that the mobile node and the mobile access gateway are the only two nodes present on that link. The assumed properties for the point-to-point link type are just as assumed by the Neighbor Discovery specification [RFC-2461] for that link type. The link is assumed to have multicast capability and the

interfaces connecting to the link can be configured with a link-local address.

Support for shared links or other link types is left for the future work.

6.2. Supported Home Network Prefix Models

This specification supports Per-MN-Prefix model and does not support Shared-Prefix model. As per the Per-MN-Prefix model, there will be a unique home network prefix assigned for each mobile node and no other host shares an address from that prefix. The prefix is always hosted on the access link where the mobile node is anchored. Conceptually, the prefix follows the mobile node as it moves within the proxy mobile IPv6 domain. However, from the routing perspective, the home network prefix is topologically anchored on the local mobility anchor.

6.3. Supported Address Configuration Models

A mobile node in the proxy mobile IPv6 domain can configure one or more IPv6 addresses on its interface using Stateless or Stateful address autoconfiguration procedures. The Router Advertisement messages sent on the access link, specify the address configuration methods permitted on that access link for that mobile node. The exact semantics of the flags that are enabled, the options that are carried in these advertisement messages is as per the Neighbor Discovery specification [RFC-2461]. However, the advertised flags with respect the address configuration will be consistent for a mobile node, on any of the access links in that proxy mobile IPv6 domain. Typically, these configuration settings will be based on the domain wide policy or based on a policy specific to each mobile node.

This specification requires that all the mobile access gateways in a given proxy mobile IPv6 domain MUST ensure that the permitted address configuration procedures or the address configuration parameters that are sent in the Router Advertisements are consistent for a mobile node when attached to on any of the access links in the proxy mobile IPv6 domain.

When stateless address autoconfiguration is supported on the link, the mobile node can generate one or more IPv6 addresses by combining the network prefix advertised on the access link with an interface identifier, using the techniques described in Stateless Autoconfiguration specification [RFC-2462] or in Privacy extension

specification [RFC-3041].

When stateful address autoconfiguration is supported on the link, the mobile node obtains the address configuration from the DHCPv6 server

using DHCPv6 client protocol, as specified in DHCPv6 specification [RFC-3315].

In addition to this, other address configuration mechanisms specific to the access link between the mobile node and the mobile access gateway may also be used for pushing the address configuration to the mobile node.

6.4. Access Authentication & Mobile Node Identification

When a mobile node attaches to an access link connected to the mobile access gateway, the deployed access security protocols on that link will ensure that the network-based mobility management service is offered only after authenticating and authorizing the mobile node for that service. The exact specifics on how this is achieved or the interactions between the mobile access gateway and the access security service is outside the scope of this document. This specification goes with the stated assumption of having an established trust and a secured communication link between the mobile node and mobile access gateway, before the protocol operation begins.
The specification also requires that the mobile access gateway MUST be able to identify the mobile node by its MN-Identifier and it must also be able to associate this identity to the sender of any IPv4 or IPv6 packets on the access link. The mobile access gateway MUST also be able to obtain the mobile node's policy profile using the MN-Identifier.

6.5. Mobile Node's Policy Profile

A mobile node's policy profile contains the essential operational parameters that are required by the network entities for managing the mobile node's mobility service. These policy profiles are stored in a local or a remote policy store, the mobile access gateway and the local mobility anchor MUST be able to obtain a mobile node's policy profile using its MN-Identifier. The policy profile may also be handed over to a serving mobile access gateway as part of a context transfer procedure during a handoff. The exact details on how this achieved is outside the scope of this document. However, this specification requires that a mobile access gateway serving a mobile node MUST have access to its policy profile.

The following are the mandatory fields of the policy profile:

- The mobile node's identifier (MN-Identifier)

- The IPv6 address of the local mobility anchor (LMAA)

- Supported address configuration procedures on the link (Stateful, Stateless or both)

The following are the optional fields of the policy profile:

- The mobile node's IPv6 home network prefix (MN-HoA)
- The mobile node's IPv6 home network prefix length

6.6. Conceptual Data Structures

Every mobile access gateway MUST maintain a Binding Update List for each currently attached mobile node. The Binding Update List is a conceptual data structure, described in Section 11.1 of Mobile IPv6 base specification [RFC-3775]. For supporting this specification, the conceptual Binding Update List data structure must be extended with the following new additional fields.

- The Identifier of the mobile node, MN-Identifier.
- The MAC address of the mobile node's connected interface.
- The IPv6 home network prefix of the mobile node.
- The IPv6 home network prefix length of the mobile node.
- The interface identifier of the point-to-point link to the mobile node.
- The interface identifier of the tunnel between the mobile access gateway and the mobile node's local mobility anchor.

6.7. Home Network Emulation

One of the key functions of a mobile access gateway is to emulate the mobile node's home network prefix on the access link. It must ensure, the mobile node believes it is still connected to its home link or on the link where it obtained its address configuration after it moved into that proxy mobile IPv6 domain.

After detecting new mobile node on its access link and after a successful access authentication and authorization of the mobile node for network-based mobility service, the mobile access gateway MUST to emulate the mobile node's home link by sending the Router Advertisements with the mobile node's home network prefix as the hosted on-link prefix. The Router Advertisement MUST be sent in

response to a Router Solicitation message that it received from the mobile node. The Router Advertisement messages MAY also be sent periodically, based on the interface configuration on the mobile access gateway.

For emulating the mobile node's home link on the access link, the mobile access gateway must know the home network prefix of the mobile node for constructing the Router Advertisement. Typically and as a default method, the mobile access gateway learns the mobile node's home network prefix information from the Proxy Binding Acknowledgement message, it received in response to the Proxy Binding Update message that it sent to the mobile node's local mobility anchor for that mobile node.

However, it is also possible, the mobile node's home network prefix information may be statically configured in the mobile node's policy profile or it may be handed over to the mobile access gateway as part of a context transfer procedure. If the mobile access gateway can predictably know the mobile node's home network prefix information, it MAY choose to send the Router Advertisement prior to receiving the Proxy Binding Acknowledgement message from the local mobility anchor. However, in the event, the local mobility anchor rejects the Proxy Binding Update message, or if the prefix that is received from the local mobility anchor for that mobile node is a different prefix than what the mobile access gateway previously advertised, the mobile access gateway MUST withdraw the prefix by sending a Router Advertisement message with zero lifetime for the prior advertised prefix.

If the access link connecting the mobile access gateway and the mobile node is a point-to-point link, the Router Advertisements advertising a specific home network prefix is received only by the respective mobile node and hence there is clearly a unique link for each mobile node that is attached to that mobile access gateway.

6.7.1. Home Network Prefix Renumbering

If the mobile node's home network prefix gets renumbered or becomes invalid during the middle of a mobility session, the mobile access gateway MUST withdraw the prefix by sending a Router Advertisement on the access link with zero prefix lifetime for the mobile node's home network prefix. Also, the local mobility anchor and the mobile access gateway MUST delete the routing state for that prefix. However, the specific details on how the local mobility anchor notifies the mobile access gateway is outside the scope of this

document.

6.8. Link-Local and Global Address Uniqueness

A mobile node in the proxy mobile IPv6 domain, as it moves from one mobile access gateway to the other, it will continue to detect its home network and thus making the node believe it is still on the same link. Every time the mobile node attaches to a new link, the event related to the interface state change, will trigger the mobile node to perform DAD operation on the link-local and global addresses. However, if the node is DNAv6 enabled, as specified in [ID-DNAV6], it may not detect the link change due to DNAv6 optimizations and hence it will not trigger the duplicate address detection (DAD) procedure for establishing the link-local address uniqueness on that new link. Further, if the mobile node uses an interface identifier that is not based on EUI-64 identifier, such as specified in IPv6 Stateless Autoconfiguration specification [RFC-2462], there is a possibility, with the odds of 1 to billion, of a link-local address collision between the two neighbors, the mobile node and the mobile access gateway.

One of the workarounds for this issue is to set the DNAv6 configuration parameter, DNASameLinkDADFlag to TRUE and that will force the mobile node to redo DAD operation every time the interface comes up, even when DNAv6 does detect a link change .

However, this issues will not impact point-to-point links based on PPP session. Each time the mobile node moves and attaches to a new mobile access gateway, either the PPP session [RFC-1661] is reestablished or the PPP session may be moved as part of context transfer procedures between the old and the new mobile access gateway.

When the mobile node tries to establish a PPP session with the mobile access gateway, the PPP goes through the Network layer Protocol phase and the IPv6 Control Protocol, IPCP6 [RFC-2472] gets triggered. Both the PPP peers negotiate a unique identifier using Interface-Identifier option in IPV6CP and the negotiated identifier is used for generating a unique link-local address on that link. Now, if the mobile node moves to a new mobile access gateway, the PPP session gets torn down with the old mobile access gateway and a new PPP session gets established with the new mobile access gateway, and the mobile node obtains a new link-local address. So, even if the mobile node is DNAv6 capable, the mobile node always configures a new link-local address when ever it moves to a new link.

If the PPP session state is moved to the new mobile access gateway,

as part of context transfer procedures that are in place, there will not be any change to the interface identifiers of the two nodes on that point-to-point change. The whole link is moved to the new

mobile access gateway and there will not be any need for establishing link-local address uniqueness on that link.

This issue is not relevant to the mobile node's global address. Since, there is a unique home network prefix for each mobile node, the uniqueness for the mobile node's global address is ensured on the access link.

6.9. Signaling Considerations

6.9.1. Initial Attachment and binding registration

After detecting a new mobile node on its access link after a successful access authentication and authorization, the mobile access gateway MUST send a Proxy Binding Update message to the mobile node's local mobility anchor.

The Proxy Binding Update message must be constructed as shown below.

```
IPv6 header (src=Proxy-CoA, dst=LMAA)
     Mobility header
         -BU /*P flag is set*/
        Mobility Options
           - Home Network Prefix Option*
           - TimeStamp Option (optional)
           - NAI Option
```

*Home Network Prefix option may contain 0::/0 or a specific prefix.

Proxy Binding Update message contents

The Proxy Binding Update message that the mobile access gateway sends to the mobile node's local mobility anchor MUST have the NAI option, identifying the mobile node, the Home Network Prefix option and optionally the Time Stamp option SHOULD be present. The Time Stamp option is not required if the mobile access gateway can send a valid sequence number that matches the sequence number maintained by the local mobility anchor for that mobile node in its binding cache entry. The message MUST be protected by using IPsec ESP, using the security association existing between the local mobility anchor and the mobile access gateway, created either dynamically or statically.

If the mobile access gateway learns the mobile node's home network prefix either from its policy store or from other means, the mobile access gateway MAY choose to specify the same in the Home Network

that prefix. If the specified value is 0::/0, then the local mobility anchor will allocate a prefix to the mobile node.

After receiving a Proxy Binding Acknowledgment with the status code indicating the acceptance of the Proxy Binding Update, the mobile access gateway MUST setup a tunnel to the mobile node's local mobility anchor, as explained in section 6.10. The mobile access gateway MUST also add a policy route for tunneling all the packets that it receives from the mobile node to its local mobility anchor.

If the local mobility anchor rejects the Proxy Binding Update message, the mobile access gateways MUST NOT advertise the mobile node's home prefix on the access link and there by denying mobility service to the mobile node.

6.9.2. Extending the binding lifetime

For extending the lifetime of a currently existing binding at the local mobility, the mobile access gateway MUST send a Proxy Binding Update message with a specific lifetime. The message MUST be constructed as specified in Section 6.9.1.

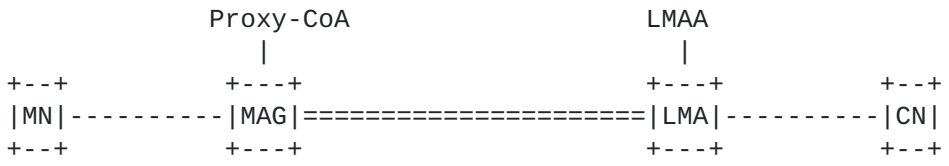
6.9.3. De-registration of the binding

At any point, the mobile access gateway detects that the mobile node has moved away from its access link, it MUST send a Proxy Binding Update message to the mobile node's local mobility anchor with the lifetime value set to zero. The message MUST be constructed as specified in Section 6.9.1.

The mobile access gateway MUST also remove the default route over the tunnel for that mobile node and delete the Binding Update List for that mobile node, either upon receiving an Proxy Binding Acknowledgment message from the local mobility anchor or after a certain timeout waiting for the acknowledgment message.

6.10. Routing Considerations

This section describes how the mobile access gateway handles the traffic to/from the mobile node that is attached to one of its access interface.



IPv6 Tunnel

6.10.1. Transport Network

The transport network between the local mobility anchor and the mobile access can be either an IPv6 or IPv4 network. However, this specification only deals with the scenario where the transport network between the mobility entities is IPv6-only and requires reachability between the local mobility anchor and the mobile access gateway over IPv6 transport. Just as in Mobile IPv6 specification [RFC-3775], the negotiated tunnel transport between the local mobility anchor and the mobile access gateway is IPv6, by default. The companion document, IPv4 support for Proxy Mobile IPv6 [IPv4-PMIP6-SPEC] specifies the required extensions for negotiating IPv4 tunneling mechanism and a specific encapsulation mode for supporting this protocol operation over IPv4 transport network.

6.10.2. Tunneling & Encapsulation Modes

The IPv6 address that a mobile node uses from its home network prefix is topologically anchored at the local mobility anchor. For a mobile node to use this address from an access network attached to a mobile access gateway, proper tunneling techniques have to be in place. Tunneling hides the network topology and allows the mobile node's IPv6 datagrams to be encapsulated as a payload of another IPv6 packet and be routed between the local mobility anchor and the mobile access gateway. The Mobile IPv6 base specification [RFC-3775] defines the use of IPv6-over-IPv6 tunneling, between the home agent and the mobile node and this specification extends the use of the same tunneling mechanism between the local mobility anchor and the mobile access gateway.

On most operating systems, tunnels are implemented as a virtual point-to-point interface. The source and the destination address of the two end points of this virtual interface along with the encapsulation mode are specified for this virtual interface. Any packet that is routed over this interface, get encapsulated with the outer header and the addresses as specified for that point to point tunnel interface. For creating a point to point tunnel to any local mobility anchor, the mobile access gateway may implement a tunnel interface with the source address field set to its Proxy-CoA address and the destination address field set to the LMA address.

The following are the supported packet encapsulation modes that can be used by the mobile access gateway and the local mobility anchor for routing mobile node's IPv6 datagrams.

o IPv6-In-IPv6 - IPv6 datagram encapsulated in an IPv6 packet. This mechanism is defined in the Generic Packet Tunneling for IPv6 specification [RFC-2473].

o IPv6-In-IPv4 - IPv6 datagram encapsulation in an IPv4 packet. The details related to this encapsulation mode and the specifics on how this mode is negotiated is specified in the companion document, IPv4 support for Proxy Mobile IPv6 [ID-IPv4-PMIP6].

o IPv6-In-IPv4-UDP - IPv6 datagram encapsulation in an IPv4 UDP packet. The details related to this mode are covered in the companion document, IPv4 support for Proxy Mobile IPv6 [IPv4-PMIP6-SPEC].

6.10.3. Routing State

The following section explain the routing state for a mobile node on the mobile access gateway. This routing state reflects only one specific way of implementation and one MAY choose to implement it in other ways. The policy based route defined below acts as a traffic selection rule for routing a mobile node's traffic through a specific tunnel created between the mobile access gateway and that mobile node's local mobility anchor and with the specific encapsulation mode, as negotiated.

The below example identifies the routing state for two visiting mobile nodes, MN1 and MN2 with their respective local mobility anchors LMA1 and LMA2.

For all traffic from the mobile node, identified by the mobile node's MAC address, ingress interface or source prefix (MN-HNP) to _ANY_DESTINATION_ route via interface tunnel0, next-hop LMAA.

Packet Source	Destination Address	Destination Interface
MAC_Address_MN1, (IPv6 Prefix or Input Interface)	_ANY_DESTINATION_	Tunnel0
	Locally Connected	Tunnel0
MAC_Address_MN2	_ANY_DESTINATION_	Tunnel1
	Locally Connected	direct

Example - Policy based Route Table

Interface	Source Address	Destination Address	Encapsulation
Tunnel0	Proxy-CoA	LMAA1	IPv6-in-IPv6
Tunnel1	IPv4-Proxy-CoA	IPv4-LMA2	IPv6-in-IPv4

Example - Tunnel Interface Table

6.10.4. Local Routing

If there is data traffic between a visiting mobile node and a corresponding node that is locally attached to an access link connected to the mobile access gateway, the mobile access gateway MAY optimize on the delivery efforts by locally routing the packets and by not reverse tunneling them to the mobile node's local mobility anchor. However, this has an implication on the mobile node's accounting and policy enforcement as the local mobility anchor is not in the path for that traffic and it will not be able to apply any traffic policies or do any accounting for those flows.

This decision of path optimization SHOULD be based on the configured policy configured on the mobile access gateway, but enforced by the mobile node's local mobility anchor. The specific details on how this is achieved is beyond of the scope of this document.

6.10.5. Tunnel Management

All the considerations mentioned in Section 5.2, for the tunnel management on the local mobility anchor apply for the mobile access gateway as well.

As explained in Section 5.2, the life of the Proxy Mobile IPv6 tunnel should not be based on a single visiting mobile node's lifetime. The tunnel may get created as part of creating a mobility state for a visiting mobile node and later the same tunnel may be associated with other mobile nodes. So, the tearing down logic of the tunnel must be based on the number of visitors over that tunnel.

6.10.6. Forwarding Rules

Upon receipt of an encapsulated packet sent to its configured Proxy-CoA address i.e. on receiving a packet from a tunnel, the mobile access gateway MUST use the destination address of the inner packet

for forwarding it to the interface where the prefix for that address is hosted. The mobile access gateway MUST remove the outer header

before forwarding the packet. If the mobile access gateway cannot find the connected interface for that destination address, it MUST silently drop the packet. For reporting an error in such scenario, in the form of ICMP control message, the considerations from Generic Packet Tunneling specification [RFC-2473] apply.

On receiving a packet from a mobile node connected to its access link, the mobile access gateway MUST ensure that there is an established binding for that mobile node with its local mobility anchor before forwarding the packet directly to the destination or before tunneling the packet to the mobile node's local mobility anchor.

On receiving a packet from a mobile node connected to its access link, to a destination that is locally connected, the mobile access gateway MUST check the configuration variable, EnableMAGLocalRouting, to ensure the mobile access gateway is allowed to route the packet directly to the destination. If the mobile access gateway is not allowed to route the packet directly, it MUST route the packet through the bi-directional tunnel established between itself and the mobile's local mobility anchor.

On receiving a packet from the mobile node to any destination i.e. not directly connected to the mobile access gateway, the packet MUST be forwarded to the local mobility anchor through the bi-directional tunnel established between itself and the mobile's local mobility anchor. However, the packets that are sent with the link-local source address MUST not be forwarded.

6.11. Interaction with DHCP Relay Agent

If Stateful Address Configuration using DHCP is supported on the link on which the mobile node is attached, the DHCP relay agent [RFC-3315] needs to be configured on the access router. When the mobile node sends a DHCPv6 Request message, the relay agent function on the access router MUST set the link-address field in the DHCPv6 message to the mobile node's home network prefix, so as to provide a prefix hint to the DHCP Server. Since, the access link is a point-to-point link with the configured mobile node's prefix as the on-link prefix, the normal DHCP relay agent configuration on the MAG will ensure the prefix hint is set to the mobile node's home network prefix.

6.12. Mobile Node Detachment Detection and Resource Cleanup

Before sending a Proxy Binding Update message to the local mobility anchor for extending the lifetime of a currently existing binding of a mobile node, the mobile access gateway MUST make sure the mobile node is still attached to the connected link by using some reliable

method. If the mobile access gateway cannot predictably detect the presence of the mobile node on the connected link, it MUST NOT attempt to extend the registration lifetime of the mobile node. Further, in such scenario, the mobile access gateway MUST terminate the binding of the mobile node by sending a Proxy Binding Update message to the mobile node's local mobility anchor with lifetime value set to 0. It MUST also remove any local state such as the Binding Update List created for that mobile node.

The specific detection mechanism of the loss of a visiting mobile node on the connected link is specific to the access link between the mobile node and the mobile access gateway and is outside the scope of this document. Typically, there are various link-layer specific events specific to each access technology that the mobile access gateway can depend on for detecting the node loss. In general, the mobile access gateway can depend on one or more of the following methods for the detection presence of the mobile node on the connected link:

- Link-layer event specific to the access technology
- PPP Session termination event on point-to-point link types
- IPv6 Neighbor Unreachability Detection event from IPv6 stack
- Notification event from the local mobility anchor
- Absence of data traffic from the mobile node on the link for a certain duration of time

6.13. Allowing network access to other IPv6 nodes

In some proxy mobile IPv6 deployments, network operators may want to provision the mobile access gateway to offer network-based mobility management service only to some visiting mobile nodes and enable just regular IPv6/IPv4 access to some other nodes attached to that mobile access gateway. This requires the network to have the control on when to enable network-based mobility management service to a mobile node and when to enabled a regular IPv6 access. This specification does not disallow such configuration.

Upon obtaining the mobile node's profile after a successful access authentication and after a policy consideration, the mobile access gateway MUST determine if the network based mobility service should be offered to that mobile node. If the mobile node is entitled for such service, then the mobile access gateway must ensure the mobile node believes it is on its home link, as explained in various sections of this specification.

If the mobile node is not entitled for the network-based mobility management service, as enforced by the policy, the mobile access gateway MAY choose to offer regular IPv6 access to the mobile node and hence the normal IPv6 considerations apply. If IPv6 access is enabled, the mobile node SHOULD be able to obtain any IPv6 address using normal IPv6 address configuration mechanisms. The obtained address must be from a local visitor network prefix. This essentially ensures, the mobile access gateway functions as any other access router and does not impact the protocol operation of a mobile node attempting to use host-based mobility management service when it attaches to an access link connected to a mobile access gateway in a proxy mobile IPv6 domain.

7. Mobile Node Operation

This non-normative section discusses the mobile node's operation in a Proxy Mobile IPv6 domain.

Once the mobile node enters a Proxy Mobile IPv6 domain and attaches to an access network and after the access authentication, the network ensures, the mobile using any of the address configuration mechanisms permitted by the network for that mobile node, will be able to obtain an address and move anywhere in that proxy mobile IPv6 domain. From the perspective of the mobile, the entire proxy mobile IPv6 domain appears as a single link, the network ensures the mobile believes it is always on the same link.

The mobile node can be operating in an IPv4-only mode, IPv6-only mode or in dual IPv4/IPv6 mode. However, the specific details on how the IPv4 network-based mobility management service is offered to the mobile node is specified in the companion document, IPv4 Support for Proxy Mobile IPv6 [ID-IPV4-PMIP6].

Typically, the configured policy in the network determines if the mobile node is authorized for IPv6, IPv4 or IPv6/IPv4 home address mobility. If the configured policy for a mobile node is for IPv6-only home address mobility, the mobile node will be able to obtain its IPv6 home address, any where in that Proxy Mobile IPv6 domain, otherwise the obtained address will be from a local prefix and not from a prefix that is topologically anchored at the local mobility anchor and hence the mobile will loose that address after it moves to a new link.

7.1. Booting up in a Proxy Mobile IPv6 Domain

When a mobile node moves into a proxy mobile IPv6 domain and attaches

to an access link, the mobile node will present its identity, MN-Identity, to the network as part of the access authentication procedure. Once the authentication procedure is complete and the mobile node is authorized to access the network, the network or specifically the mobile access gateway on the access link will have the mobile node's profile and so it would know the mobile node's home network prefix and the permitted address configuration modes. The mobile node's home network prefix may also be dynamically assigned by the mobile node's local mobility anchor and the same may be learnt by the mobile access gateway.

If the mobile node is IPv6 enabled, on attaching to the link and after access authentication, the mobile node typically would send a Router Solicitation message. The mobile access gateway on the attached link will respond to the Router Solicitation message with a Router Advertisement. The Router Advertisement will have the mobile node's home network prefix, default-router address and other address configuration parameters. The address configuration parameters such as Managed Address Configuration, Stateful Configuration flag values will typically be consistent through out that domain for that mobile node.

If the Router Advertisement has the Managed Address Configuration flag set, the mobile node, as it would normally do, will send a DHCPv6 Request and the mobile access gateway on that access link will ensure, the mobile node gets an address from its home network prefix as a lease from the DHCP server.

If the Router Advertisement does not have the Managed Address Configuration flag set and if the mobile node is allowed to use an autoconfigured address, the mobile node will generate an interface identifier, as per the Autoconf specification [RFC-2462] or using privacy extensions as specified in Privacy Extensions specification [RFC-3041].

If the mobile node is IPv4 enabled or IPv4-only enabled, the mobile node after the access authentication, will be able to obtain the IPv4 address configuration for the connected interface by using DHCPv4.

Once the address configuration is complete, the mobile node can continue to use the obtained address configuration as long as it is with in the scope of that Proxy Mobile IPv6 domain.

7.2. Roaming in the Proxy Mobile IPv6 Network

After booting in the Proxy Mobile IPv6 domain and obtaining the address configuration, the mobile node as it roams in the network

between access links, will always detect its home network prefix on

the link, as long as the attached access network is in the scope of that Proxy Mobile IPv6 domain. The mobile node can continue to use its IPv4/IPv6 MN-HoA for sending and receiving packets. If the mobile node uses DHCP for address configuration, it will always be able to obtain its MN-HoA using DHCP. However, the mobile node will always detect a new default-router on each connected link, but still advertising the mobile node's home network prefix as the on-link prefix and with the other configuration parameters consistent with its home link properties.

7.3. IPv6 Host Protocol Parameters

This specification assumes the mobile node to be a normal IPv6 node, with its protocol operation consistent with the base IPv6 specification [RFC-2460]. All aspects of Neighbor Discovery Protocol, including Router Discovery, Neighbor Discovery, Address Configuration procedures will just remain consistent with the base IPv6 Neighbor Discovery Specification [RFC-2461]. However, this specification recommends that the following IPv6 operating parameters on the mobile node be adjusted to the below recommended values for protocol efficiency and for achieving faster hand-offs.

Lower Default-Router List Cache Time-out:

As per the base IPv6 specification [RFC-2460], each IPv6 host will maintain certain host data structures including a Default-Router list. This is the list of on-link routers that have sent Router Advertisement messages and are eligible to be default routers on that link. The Router Lifetime field in the received Router Advertisement defines the life of this entry.

In the Proxy Mobile IPv6 scenario, when the mobile node moves from one link to another, the received Router Advertisement messages advertising the mobile's home network prefix will be from a different link-local address and thus making the mobile node believe that there is a new default-router on the link. It is important that the mobile node uses the newly learnt default-router as supposed to the previously learnt default-router. The mobile node must update its default-router list with the new default router entry and must age out the previously learnt default router entry from its cache, just as specified in Section 6.3.5 of the base IPv6 ND specification [RFC-2461]. This action is critical for minimizing packet losses during a hand off switch.

On detecting a reachability problem, the mobile node will certainly detect the neighbor or the default-router unreachability by performing a Neighbor Unreachability Detection procedure, but it is

important that the mobile node times out the previous default router entry at the earliest. If a given IPv6 host implementation has the provision to adjust these flush timers, still conforming to the base IPv6 ND specification, it is desirable to keep the flush-timers to suit the above consideration.

However, if the mobile access gateway has the ability to withdraw the previous default-router entry, by sending a Router Advertisement using the link-local address that of the previous mobile access gateway and with the Router Lifetime field set to value 0, then it is possible to force the flush of the Previous Default-Router entry from the mobile node's cache. This certainly requires some context-transfer mechanisms in place for notifying the link-local address of the default-router on the previous link to the mobile access gateway on the new link.

There are other solutions possible for this problem, including the assignment of a unique link-local address for all the mobile access gateways in a Proxy Mobile IPv6 domain. In any case, this is an implementation choice and has no bearing on the protocol interoperability. Implementations are free to adopt the best approach that suits their target deployments.

8. Message Formats

This section defines extensions to the Mobile IPv6 [RFC-3775] protocol messages.

8.1. Proxy Binding Update

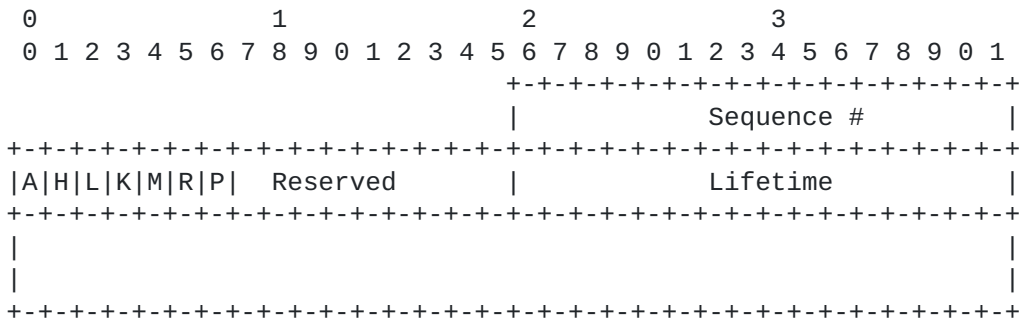


Figure 9: Proxy Binding Update Message

A Binding Update message that is sent by mobile access gateway is referred to as the Proxy Binding Update message.

Proxy Registration Flag (P)

The Proxy Registration Flag is set to indicate to the local mobility anchor that the Binding Update is from a mobile access gateway acting as a proxy mobility agent. The flag MUST be set to the value of 1 for proxy registrations and MUST be set to 0 for direct registrations sent by a mobile node when using host-base mobility.

For descriptions of other fields present in this message, refer to the section 6.1.7 of Mobile IPv6 specification [RFC3775].

8.2. Proxy Binding Acknowledgment

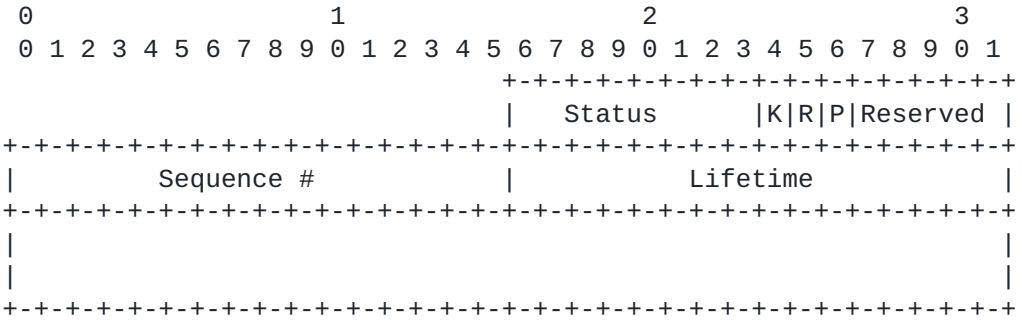


Figure 10: Proxy Binding Acknowledgment Message

A Binding Acknowledgment message that is sent by the local mobility anchor to the mobile access gateway is referred to as "Proxy Binding Acknowledgement".

Proxy Registration Flag (P)

A new flag (P) is included in the Binding Acknowledgement message to indicate that the local mobility anchor that processed the corresponding Proxy Binding Update message supports Proxy Registrations. The flag is set only if the corresponding Proxy Binding Update had the Proxy Registration Flag (P) set to value of 1.

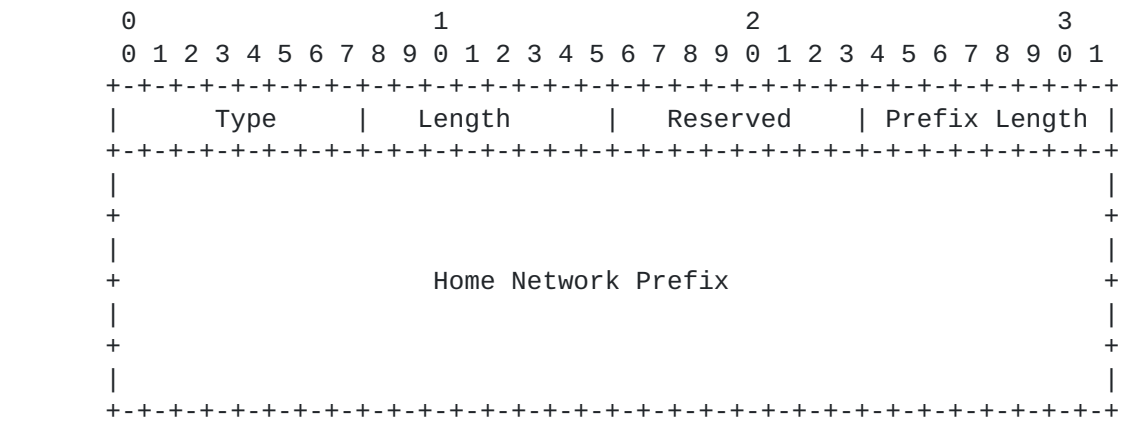
The rest of the Binding Acknowledgement format remains the same, as defined in [RFC-3775].

For descriptions of other fields present in this message, refer to the section 6.1.8 of Mobile IPv6 specification [RFC3775].

8.3. Home Network Prefix Option

A new option, Home Network Prefix Option is defined for using it in the Proxy Binding Update and Acknowledgment messages exchanged between the local mobility anchor and the mobile access gateway. This option can be used for exchanging the mobile node's home network prefix information.

The home network prefix Option has an alignment requirement of 8n+4. Its format is as follows:



Type
<IANA>

Length

8-bit unsigned integer indicating the length in octets of the option, excluding the type and length fields. This field MUST be set to 18.

Reserved

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

Prefix Length

8-bit unsigned integer indicating the prefix length of the IPv6 prefix contained in the option.

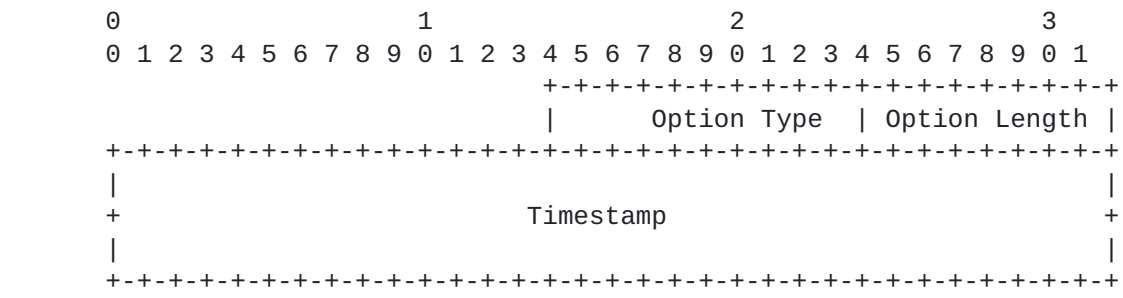
Home Network Prefix

A sixteen-byte field containing the mobile node's IPv6 Home Network Prefix.

Figure 11: Home Network Prefix Option

8.4. Time Stamp Option

A new option, Time Stamp Option is defined for use in the Proxy Binding Update and Acknowledgement messages. This option can be used in Proxy Binding Update and Proxy Binding Acknowledgement messages.



Type
<IANA>

Length

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

Timestamp

64-bit time stamp

Figure 12: Time Stamp Option

8.5. Status Codes

This document defines the following new Binding Acknowledgement status values:

145: Proxy Registration not supported by the local mobility anchor

146: Proxy Registrations from this mobile access gateway not allowed

147: Home Network prefix for this NAI is not configured and the Home Network Prefix Option not present in the Proxy Binding Update.

148: Invalid Time Stamp Option in the received Proxy Binding Update message.

Status values less than 128 indicate that the Binding Update was processed successfully by the receiving nodes. Values greater than 128 indicate that the Binding Update was rejected by the local mobility anchor.

The value allocation for this usage needs to be approved by the IANA

and must be updated in the IANA registry.

9. Protocol Configuration Variables

The mobile access gateway MUST allow the following variables to be configured by the system management.

EnableMAGLocalrouting

This flag indicates whether or not the mobile access gateway is allowed to enable local routing of the traffic exchanged between a visiting mobile node and a corresponding node that is locally connected to one of the interfaces of the mobile access gateway. The corresponding node can be another visiting mobile node as well, or a local fixed node.

The default value for this flag is set to "FALSE", indicating that the mobile access gateway MUST reverse tunnel all the traffic to the mobile node's local mobility anchor.

When the value of this flag is set to "TRUE", the mobile access gateway MUST route the traffic locally.

This aspect of local routing MAY be defined as policy on a per mobile basis and when present will take precedence over this flag.

10. IANA Considerations

This document defines a two new Mobility Header Options, the Home Network Prefix Option and the Time Stamp Option. These options are described in Sections 8.3 and 8.5 respectively. The Type value for these options needs to be assigned from the same numbering space as allocated for the other mobility options, as defined in [RFC-3775].

This document also defines new Binding Acknowledgement status values as described in Section 8.5. The status values MUST be assigned from the same space used for Binding Acknowledgement status values, as defined in [RFC-3775].

11. Security Considerations

The potential security threats against any general network-based mobility management protocol are covered in the document, Security Threats to Network-Based Localized Mobility Management [RFC-4832]. This section analyses those vulnerabilities in the context of Proxy

Mobile IPv6 protocol solution and covers all aspects around those identified vulnerabilities.

A compromised mobile access gateway can potentially send Proxy Binding Update messages on behalf of the mobile nodes that are not attached to its access link. This threat is similar to an attack on a typical routing protocol or equivalent to the compromise of an on-path router. This threat exists in the network today and this specification does not make this vulnerability any worse than what it is. However, to eliminate this vulnerability, the local mobility anchor before accepting Proxy Binding Update message received from a mobile access gateway, MUST ensure the mobile node is attached to the mobile access gateway that sent the Proxy Binding Update message. This can be achieved using out of band mechanisms and the specifics of how that is achieved is beyond the scope of this document.

This document does not cover the security requirements for authorizing the mobile node for the use of the access link. It is assumed that there are proper Layer-2/Layer-3 based authentication procedures, such as EAP, are in place and will ensure the mobile node is properly identified and authorized before permitting it to access the network. It is further assumed that the same security mechanism will ensure the mobile session is not hijacked by malicious nodes on the access link.

This specification requires that all the signaling messages exchanged between the mobile access gateway and the local mobility anchor MUST be authenticated by IPsec [RFC-4301]. The use of IPsec to protect Mobile IPv6 signaling messages is described in detail in the HA-MN IPsec specification [RFC-3776] and the applicability of that security model to Proxy Mobile IPv6 protocol is covered in Section 4.0 of this document.

As described in the base Mobile IPv6 specification [RFC-3775], both the mobile node (in case of Proxy Mobile IPv6, its the mobile access gateway) and the local mobility anchor MUST support and SHOULD use the Encapsulating Security Payload (ESP) header in transport mode and MUST use a non-NULL payload authentication algorithm to provide data origin authentication, data integrity and optional anti-replay protection.

The proxy solution allows one device creating a routing state for some other device at the local mobility anchor. It is important that the local mobility anchor has proper authorization services in place

to ensure a given mobile access gateway is permitted to be a proxy for a specific mobile node. If proper security checks are not in place, a malicious node may be able to hijack a session or may do a denial-of-service attacks.

12. Acknowledgements

The authors would like to specially thank Julien Laganier, Christian Vogt, Pete McCann, Brian Haley, Ahmad Muhanna, JinHyeock Choi for their thorough review of this document.

The authors would also like to thank the Gerardo Giaretta, Kilian Weniger, Alex Petrescu, Mohamed Khalil, Fred Templing, Nishida Katsutoshi, James Kempf, Vidya Narayanan, Henrik Levkowetz, Phil Roberts, Jari Arkko, Ashutosh Dutta, Hesham Soliman, Behcet Sarikaya, George Tsirtsis and many others for their passionate discussions in the working group mailing list on the topic of localized mobility management solutions. These discussions stimulated much of the thinking and shaped the draft to the current form. We acknowledge that !

The authors would also like to thank Ole Troan, Akiko Hattori, Parviz Yegani, Mark Grayson, Michael Hammer, Vojislav Vucetic, Jay Iyer and Tim Stammers for their input on this document.

13. References

13.1. Normative References

[RFC-1305] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, March 1992.

[RFC-2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC-2461] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC-2462] Thompson, S., Narten, T., "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

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

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

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

[RFC-3776] Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to

Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

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

[RFC-4301] Kent, S. and Atkinson, R., "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

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

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

[RFC-4830] Kempf, J., Leung, K., Roberts, P., Nishida, K., Giaretta, G., Liebsch, M., "Problem Statement for Network-based Localized Mobility Management", September 2006.

[RFC-4831] Kempf, J., Leung, K., Roberts, P., Nishida, K., Giaretta, G., Liebsch, M., "Goals for Network-based Localized Mobility Management", October 2006.

[RFC-4832] Vogt, C., Kempf, J., "Security Threats to Network-Based Localized Mobility Management", September 2006.

[ID-IPV4-PMIP6] Wakikawa, R. and Gundavelli, S., "IPv4 Support for Proxy Mobile IPv6", draft-ietf-netlmm-pmip6-ipv4-support-00.txt, May 2007.

[ID-DSMIP6] Soliman, H. et al, "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)", draft-ietf-mip6-nemo-v4traversal-03.txt, October 2006.

13.2. Informative References

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

[RFC-1661] Simpson, W., Ed., "The Point-To-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[RFC-2472] Haskin, D. and Allen, E., "IP version 6 over PPP", RFC 2472, December 1998.

[RFC-2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC-3041] Narten, T. and Draves, R., "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[RFC-3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[RFC-3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[ID-DNAV6] Kempf, J., et al "Detecting Network Attachment in IPv6 Networks (DNAv6)", draft-ietf-dna-protocol-03.txt, October 2006.

[ID-MIP6-IKEV2] Devarapalli, V. and Dupont, F., "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture", draft-ietf-mip6-ikev2-ipsec-08.txt, December 2006.

Appendix A. Proxy Mobile IPv6 interactions with AAA Infrastructure

Every mobile node that roams in a proxy Mobile IPv6 domain, would typically be identified by an identifier, MN-Identifier, and that identifier will have an associated policy profile that identifies the mobile node's home network prefix, permitted address configuration modes, roaming policy and other parameters that are essential for providing network-based mobility service. This information is typically configured in AAA. It is possible the home network prefix is dynamically allocated for the mobile node when it boots up for the first time in the network, or it could be a statically configured value on per mobile node basis. However, for all practical purposes, the network entities in the proxy Mobile IPv6 domain, while serving a mobile node will have access to this profile and these entities can query this information using RADIUS/DIAMETER protocols.

Appendix B. Supporting Shared-Prefix Model using DHCPv6

For supporting shared-prefix model, i.e, if multiple mobile nodes are configured with a common IPv6 network prefix, as in Mobile IPv6 specification, it is possible to support that configuration under the following guidelines:

The mobile node is allowed to use stateful address configuration

using DHCPv6 for obtaining its address configuration. The mobile nodes is not allowed to use any of the stateless autoconfiguration techniques. The permitted address configuration models for the

mobile node on the access link can be enforced by the mobile access gateway, by setting the relevant flags in the Router Advertisements, as per ND Specification, [RFC-2461].

The Home Network Prefix Option that is sent by the mobile access gateway in the Proxy Binding Update message, must contain the 128-bit host address that the mobile node obtained via DHCPv6.

Routing state at the mobile access gateway:

For all IPv6 traffic from the source MN-HoA::/128 to _ANY_DESTINATION_, route via tunnel0, next-hop LMAA, where tunnel0 is the MAG to LMA tunnel.

Routing state at the local mobility anchor:

For all IPv6 traffic to destination MN-HoA::/128, route via tunnel0, next-hop Proxy-CoA, where tunnel0 is the LMA to MAG tunnel.

Authors' Addresses

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

Email: sgundave@cisco.com

Kent Leung
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: kleung@cisco.com

Vijay Devarapalli
Azaire Networks
4800 Great America Pkwy
Santa Clara, CA 95054
USA

Email: vijay.devarapalli@azairenet.com

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury, MA

Email: kchowdhury@starentnetworks.com

Basavaraj Patil
Nokia Siemens Networks
6000 Connection Drive
Irving, TX 75039
USA

Email: basavaraj.patil@nsn.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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