NETLMM WG
Internet-Draft
Intended status: Standards Track
Expires: June 27, 2008

S. Gundavelli (Editor)
K. Leung
Cisco
V. Devarapalli
Azaire Networks
K. Chowdhury
Starent Networks
B. Patil
Nokia Siemens Networks
December 25, 2007

Proxy Mobile IPv6
draft-ietf-netlmm-proxymip6-08.txt

Status of this Memo

Copyright Notice

Abstract

Network-based mobility management enables IP mobility for a host without requiring its participation in any mobility related

signaling. The Network is responsible for managing IP mobility on behalf of the host. The mobility entities in the network are responsible for tracking the movements of the host and initiating the required mobility signaling on its behalf. This specification describes a network-based mobility management protocol and is referred to as Proxy Mobile IPv6.

Table of Contents

1. Introduction

IP mobility for IPv6 hosts is specified in Mobile IPv6 [RFC-3775]. Mobile IPv6 requires client functionality in the IPv6 stack of a mobile node. Exchange of signaling messages between the mobile node and home agent enables the creation and maintenance of a binding between the mobile node's home address and its care-of-address. Mobility as specified in [RFC-3775] requires the IP host to send IP mobility management signaling messages to the Home Agent, which is located in the network.

Network-based mobility is another approach to solving the IP mobility challenge. It is possible to support mobility for IPv6 nodes without host involvement by extending Mobile IPv6 [RFC-3775] signaling messages and reusing the home agent. This approach to supporting mobility does not require the mobile node to be involved in the exchange of signaling messages between itself and the Home Agent. A proxy mobility agent in the network performs the signaling with the home agent and does the mobility management on behalf of the mobile node attached to the network. Because of the use and extension of Mobile IPv6 signaling and home agent functionality, this protocol is referred to as Proxy Mobile IPv6 (PMIPv6).

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 undergone interoperability testing.

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

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 key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [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 the 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 binding state. The local mobility anchor has the functional capabilities of a home agent as defined in Mobile IPv6 base specification [RFC-3775] with the additional capabilities required 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 movements on the access link and for signaling the mobile node's local mobility anchor.

Mobile Node (MN)

Throughout this document, the term mobile node is used to refer to an IP host 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 IP mobility related signaling for achieving mobility for an IP address that is obtained in that Proxy Mobile IPv6 domain. This document further uses explicit text when referring to a mobile node that is involved in mobility related signaling as per the 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 bi-directional tunnel established 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 specified 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 from its home network prefix obtained by a mobile node in a Proxy Mobile IPv6 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 is always present in the Router Advertisements that the mobile node receives when it is attached to any of the access links in that Proxy Mobile IPv6 domain. This 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. If the mobile node connects to the Proxy Mobile IPv6 domain through multiple interfaces, simultaneously, each of the connected interface will be assigned a unique home network prefix and under a different mobility session.

Mobile Node's Home Link

This is the link on which the mobile node obtained its Layer-3 address configuration for the attached interface 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.

Multihomed Mobile Node

A mobile node that connects to the Proxy Mobile IPv6 domain through more than one interface and uses these interfaces simultaneously is referred to as a multihomed mobile node.

Mobile Node Identifier (MN-Identifier)

The identity of a mobile node in the Proxy Mobile IPv6 domain. This is the stable identifier of a mobile node that the mobility entities in a Proxy Mobile IPv6 domain can always acquire and use it for predictably identifying a mobile node. This is typically an identifier such as NAI or other identifier such as a MAC address.

Mobile Node Interface Identifier (MN-Interface-Identifier)

The interface identifier that identifies a given interface of a mobile node. For those interfaces that have a layer-2 identifier, the interface identifier can be based on that layer-2 identifier. The interface identifier in some cases is generated by the mobile node and conveyed to the access router or the mobile access gateway. In some cases, there might not be any interface identifier associated with the mobile node's interface.

Policy Profile

Policy Profile is an abstract term for referring to a set of configuration parameters that are configured for a given mobile node. The mobility entities in the Proxy Mobile IPv6 domain require access to these parameters for providing the mobility management to a given mobile node. The specific details on how the network entities obtain this policy profile is outside the scope of this document.

Proxy Binding Update (PBU)

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

Proxy Binding Acknowledgement (PBA)

A binding registration reply message sent by a local mobility anchor in response to a Proxy Binding Update request 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].

Proxy Mobile IPv6 protocol is intended for providing network-based IP mobility management support to a mobile node, without requiring the participation of the mobile node in any IP mobility related signaling. The mobility entities in the network will track the mobile node's movements and will initiate the mobility signaling and setup the required routing state.

The core functional entities in the NETLMM infrastructure are the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). The local mobility anchor is responsible for maintaining the mobile node's reachability state and is the topological anchor point for the mobile node's home network prefix. The mobile access gateway is the entity that performs the mobility management on behalf of a mobile node and it resides on the access link where the mobile node is anchored. The mobile access gateway is responsible for detecting the mobile node's movements on its access link and for sending binding registrations to the mobile node's local mobility anchor. The architecture of a Proxy Mobile IPv6 domain is shown in Figure 1.

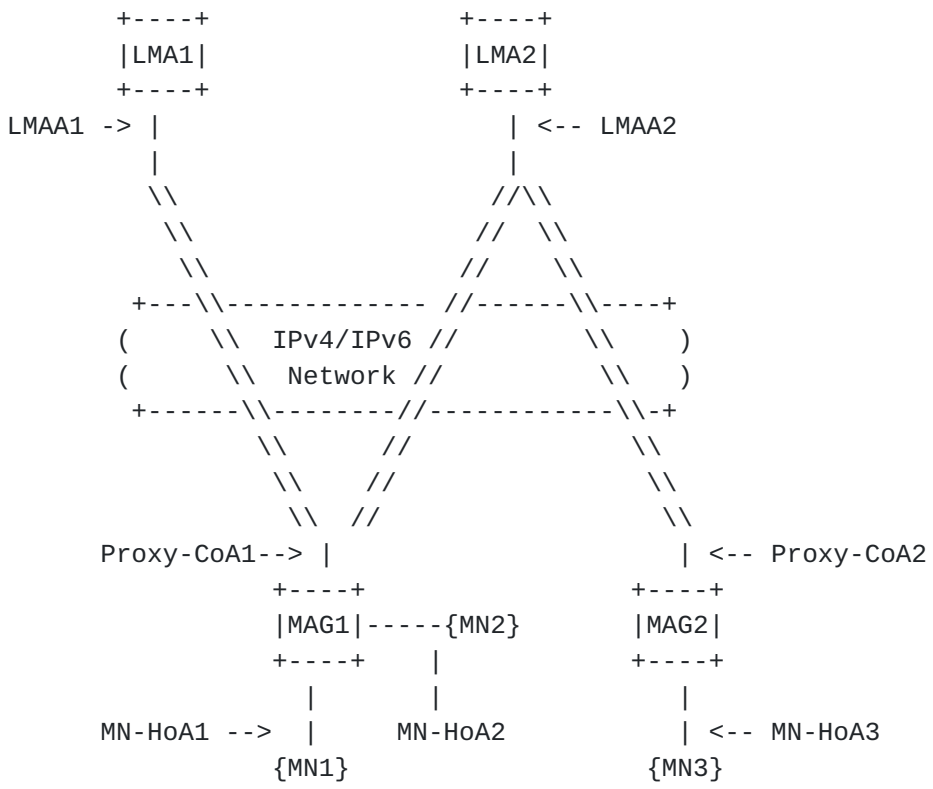


Figure 1: Proxy Mobile IPv6 Domain

Once a mobile node enters a Proxy Mobile IPv6 domain and attaches to an access link, the mobile access gateway on that access link, after identifying the mobile node and acquiring its identity, will determine if the mobile node is authorized for the network-based mobility management service.

If the network determines that the network-based mobility management service needs to be offered to that mobile node, the network will ensure that the mobile node using any of the address configuration mechanisms permitted by the network will be able to obtain the address configuration on the connected interface and move anywhere in that Proxy Mobile IPv6 domain. The obtained address configuration includes the address(es) from its home network prefix, the default-router address on the link and other related configuration parameters. From the perspective of the mobile node, the entire Proxy Mobile IPv6 domain appears as a single link, the network ensures that the mobile node believes it is always on the same link where it obtained its initial address configuration, even after

changing its point of attachment in that network.

The mobile node may be operating in an IPv4-only mode, IPv6-only mode or in dual IPv4/IPv6 mode. Based on what is enabled in the network for that mobile node, the mobile node will be able to obtain an IPv4, IPv6 or dual IPv4/IPv6 addresses and move anywhere in that Proxy Mobile IPv6 domain. However, the specific details related to the IPv4 addressing or IPv4 transport support are specified in the companion document [ID-IPV4-PMIP6].

If the mobile node connects to the Proxy Mobile IPv6 domain, through multiple interfaces and over multiple access networks, the network will allocate a unique home network prefix for each of the connected interfaces and the mobile node will be able to configure an address(es) on those interfaces from the respective home network prefixes. If the mobile node performs a handover from one interface to another in the same Proxy Mobile IPv6 domain, then the local mobility anchor will assign the same prefix to the new interface, if it receives the handover hints from the mobile access gateway in the signaling messages.

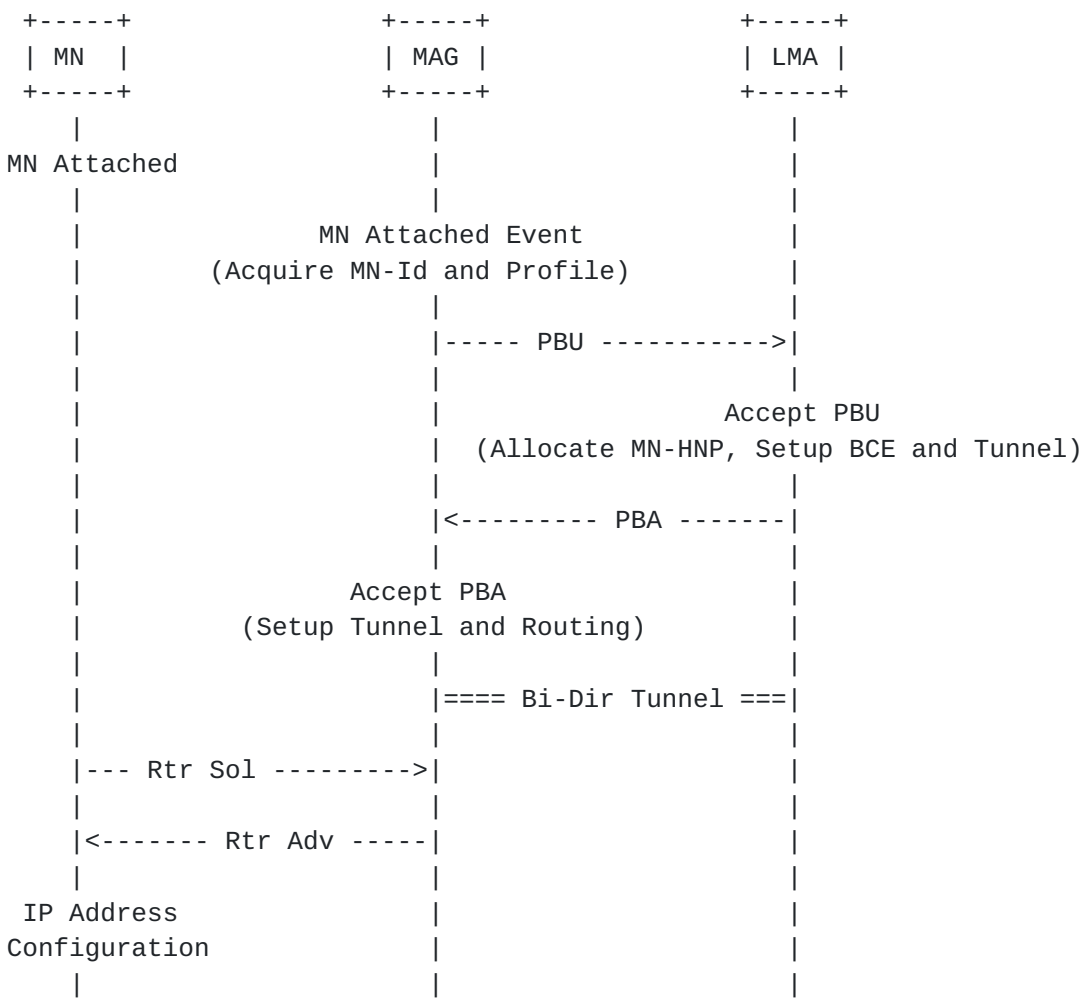


Figure 2: Mobile Node Attachment - Signaling Call Flow

Figure 2 shows the signaling call flow when the mobile node enters the Proxy Mobile IPv6 domain.

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. Upon accepting this Proxy Binding Update message, the local mobility anchor sends a Proxy Binding Acknowledgement message including the mobile node's home network prefix. It also creates the Binding Cache entry and establishes a bi-directional tunnel to the mobile access gateway.

The mobile access gateway on receiving the Proxy Binding Acknowledgement message sets up a bi-directional tunnel to the local mobility anchor and sets up the data path for the mobile node's traffic. At this point the mobile access gateway will have all the required information for emulating the mobile node's home 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 the modes that are permitted on that access link. At the end of a successful address configuration procedure, the mobile node will end up with an address from its home network prefix.

Once the address configuration is complete, 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 packets that are sent by any correspondent node to the mobile node. The local mobility anchor forwards these received packets 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. Any packet that the mobile node sends to any correspondent node will be received by the mobile access gateway and will be sent 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.

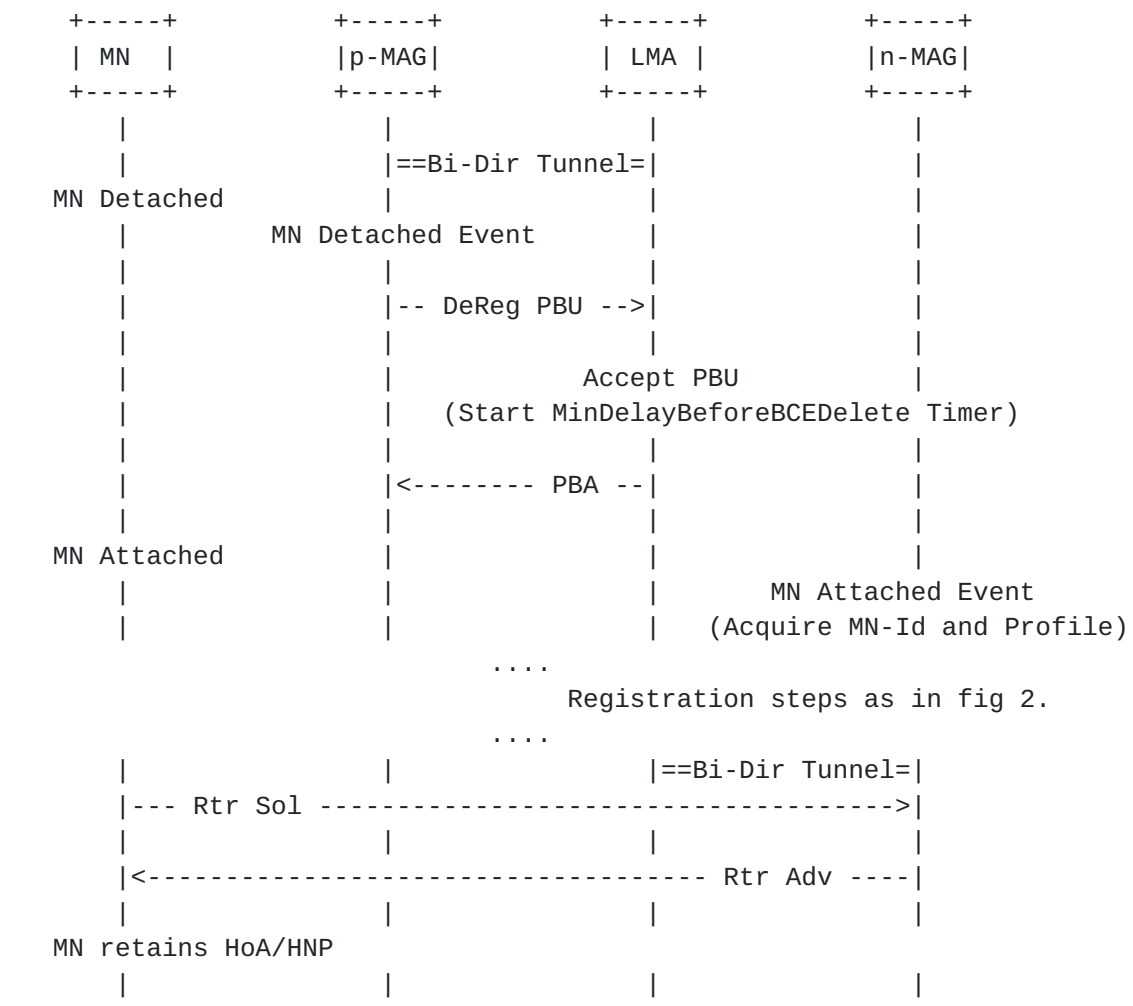


Figure 3: Mobile Node Handoff - Signaling Call Flow

Figure 3 shows the signaling call flow for the mobile node's handoff from previously attached mobile access gateway (p-MAG) to the newly attached mobile access gateway (n-MAG).

After obtaining the initial address configuration in the Proxy Mobile IPv6 domain, if the mobile node changes its point of attachment, the mobile access gateway on the previous link will detect the mobile node's detachment from the link and will signal the local mobility anchor and will remove the binding and routing state for that mobile node. However, the local mobility anchor upon accepting the request will wait for certain amount of time before it deletes the binding, for allowing a smooth handoff.

The mobile access gateway on the new access link upon detecting the

mobile node on its access link will signal the local mobility anchor for updating the binding state. Once that signaling is complete, the mobile node will continue to receive the Router Advertisements containing its home network prefix, making it believe it is still on the same link and it will use the same address configuration on the new access link.

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 MUST be protected using end-to-end security association(s) offering integrity and data origin authentication.

The mobile access gateway and the local mobility anchor MUST implement IPsec for protecting the Proxy Mobile IPv6 signaling messages [RFC-4301]. IPsec is the default security mechanism for securing the signaling messages. However in certain deployments of this protocol, other security mechanisms MAY be applied and the signaling messages must be protected using the semantics provided by that respective mechanism. The specification of the other security mechanisms are beyond the scope of this document

IPsec ESP [RFC-4303] in transport mode with mandatory integrity protection SHOULD be used for protecting the signaling messages. Confidentiality protection of these messages is not required.

IKEv2 [RFC-4306] SHOULD be used to setup security associations between the mobile access gateway and the local mobility anchor to protect the Proxy Binding Update and Proxy Binding Acknowledgement messages. The mobile access gateway and the local mobility anchor can use any of the authentication mechanisms, as specified in IKEv2, for mutual authentication.

The Mobile IPv6 specification [RFC-3775] 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, 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 by sending a query to the

policy store, such as AAA.

4.1. Peer Authorization Database Entries

This section describes PAD entries [RFC-4301] 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 any 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
```

Figure 4: PAD Entries

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

This section describes the security policy entries [RFC-4301] 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 = BA
    Then use SA ESP transport mode
    Initiate using IDi = mag_1 to address lma_address_1

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

Figure 5: SPD Entries

5. Local Mobility Anchor Operation

The local mobility anchor MUST support the home agent function as defined in [RFC-3775] and additionally the extensions defined in this specification. A home agent with these modifications and enhanced capabilities for supporting Proxy Mobile IPv6 protocol is referred to as the local mobility anchor.

This section describes the operational details of the local mobility anchor.

5.1. Extensions to Binding Cache Entry Data Structure

Every local mobility anchor MUST maintain a Binding Cache entry for each currently registered mobile node. Binding Cache entry is a conceptual data structure, described in Section 9.1 [RFC-3775].

For supporting this specification, the Binding Cache Entry data structure 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 created due to the registrations directly sent by the mobile node.

- The identifier of the registered mobile node, MN-Identifier. This identifier is obtained from the Mobile Node Identifier Option [RFC-4283] present in the received Proxy Binding Update request.

- The interface identifier of the mobile node's connected interface on the access link. This identifier can be acquired from the Mobile Node Interface Identifier option, present in the received Proxy Binding Update request. If the option was not present in the request, this value MUST be set to ALL_ZERO.

- The Link-local address of the mobile node on the interface attached to the access link. This is obtained from the Link-local Address option, present in the Proxy Binding Update request.

- The IPv6 home network prefix of the registered mobile node. The home network prefix of the mobile node may have been statically configured in the mobile node's policy profile, or, it may have been dynamically allocated by the local mobility anchor. The IPv6 home network prefix also includes the corresponding prefix length.

- The interface identifier of the bi-directional tunnel established between the local mobility anchor and the mobile access gateway where the mobile node is currently anchored. The tunnel interface identifier is acquired during the tunnel creation.

- The access technology through which the mobile node is currently connected. This is obtained from the Access Technology Type option, present in the Proxy Binding Update message.

- The 64-bit timestamp value of the most recently accepted Proxy Binding Update request sent for this mobile node. This is obtained from the Timestamp option, present in the request.

Typically, the MN-Identifier is the key for locating a Binding Cache entry. However, when supporting multihoming there MAY be more than one Binding Cache entry with the same MN-Identifier and in such cases the entry can be located using any of the following key combinations:

- MN-Identifier, MN-HNP

- MN-Identifier, Proxy-CoA

- MN-Identifier, MN-Interface-Identifier

- MN-Identifier, Access Technology Type (When MN-Interface-Identifier is not present)

5.2. 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 to each mobile node and no other node shares an address from that prefix. The assigned prefix is unique to a mobile node and also unique to a given interface of the mobile node. If the mobile node attaches to the Proxy Mobile IPv6 domain through multiple interfaces and simultaneously, each of those connected interfaces will be assigned a different prefix.

The mobile node's home network prefix is always hosted on the access link where the mobile node is anchored. Conceptually, the entire home network prefix follows the mobile node as it moves within the Proxy Mobile IPv6 domain. The local mobility anchor is not required to perform any proxy ND operations [RFC-4861] for defending the mobile node's home address on the home link. However, from the routing perspective, the home network prefix is topologically anchored on the local mobility anchor.

5.3. Signaling Considerations

This section provides the rules for processing the signaling messages. The processing rules specified in this section and other related sections are chained and are in a specific order. When applying these considerations for processing the signaling messages, the specified order MUST be maintained.

Processing Binding Registrations

Upon receiving a Proxy Binding Update request (a Binding Update Request with the 'P' flag set) from a mobile access gateway on behalf of a mobile node, the local mobility anchor MUST process the request as defined in Section 10.3 [RFC-3775]; additionally the following considerations must be applied.

1. The local mobility anchor MUST observe the rules described in Section 9.2 [RFC-3775] when processing Mobility Headers in the received Proxy Binding Update request.

2. The local mobility anchor MUST identify the mobile node from the identifier present in the Mobile Node Identifier option [RFC-4283] of the Proxy Binding Update request. If the Mobile Node Identifier option is not present in the Proxy Binding Update request, the local mobility anchor MUST reject the request and

send a Proxy Binding Acknowledgement message with Status field set to MISSING_MN_IDENTIFIER_OPTION (Missing mobile node identifier) and the identifier in the Mobile Node Identifier Option MUST be set to a zero length identifier.

3. If the local mobility anchor cannot authorize the mobile node based on the Mobile Node Identifier option [RFC-4283] present in the request, it MUST reject the Proxy Binding Update request and send a Proxy Binding Acknowledgement message with Status field set to 133 (Not home agent for this mobile node).

4. If the local mobility anchor determines that the mobile node is not authorized for the network-based mobility management service, it MUST reject the request and send a Proxy Binding Acknowledgement message with Status field set to PROXY_REG_NOT_ENABLED (Proxy Registration not enabled).

5. The local mobility anchor MUST ignore the check, specified in Section 10.3.1 [RFC-3775], related to the presence of Home Address destination option in the Proxy Binding Update request.

6. The local mobility anchor MUST authenticate the Proxy Binding Update request as described in Section 4.0. When IPsec is used for message authentication, the SPI in the IPsec header [RFC-4306] of the received packet is needed for locating the security association, for authenticating the Proxy Binding Update request.

7. The local mobility anchor MUST apply the required policy checks, as explained in Section 4.0, to verify the sender is a trusted mobile access gateway, authorized to send Proxy Binding Update requests on behalf of this mobile node.

8. If the local mobility anchor determines that the requesting node is not authorized to send Proxy Binding Update requests, it MUST reject the request and send a Proxy Binding Acknowledgement message with Status field set to MAG_NOT_AUTHORIZED_FOR_PROXY_REG (Not authorized to send proxy registrations).

9. If the Home Network Prefix option is not present in the Proxy Binding Update request, the local mobility anchor MUST reject the request and send a Proxy Binding Acknowledgement message with Status field set to MISSING_HOME_NETWORK_PREFIX_OPTION (Missing mobile node's home network prefix option).

10. If the Access Technology Type option is not present in the Proxy Binding Update request, the local mobility anchor MUST reject

the request and send a Proxy Binding Acknowledgement message with Status field set to MISSING_ACCESS_TECH_TYPE_OPTION (Missing mobile node's access technology type).

11. The local mobility anchor MUST apply the considerations specified in Section 5.5, for processing the Sequence Number field and the Timestamp option, in the Proxy Binding Update request.

12. The local mobility anchor MUST use the identifier from the Mobile Node Identifier Option [RFC-4283] present in the Proxy Binding Update request and MUST apply multihoming considerations specified in Section 5.4 for performing the Binding Cache entry existence test or for identifying the mobility session. If the entry does not exist, the local mobility anchor MUST consider this request as an initial binding registration request. If the entry exists, the local mobility anchor MUST consider this request as a binding re-registration request. However, from the perspective of the mobile access gateway that sent the request, this binding re-registration request may be an initial Binding Update request after the mobile node's attachment to that mobile access gateway.

Initial Binding Registration:

1. If the Home Network Prefix option present in the Proxy Binding Update request has the value 0::/0, the local mobility anchor SHOULD allocate a prefix for the mobile node and send a Proxy Binding Acknowledgement message including the Home Network Prefix option containing the allocated prefix value. The local mobility anchor MUST ensure the allocated prefix is not in use by any other node.

2. If the local mobility anchor is unable to allocate a home network prefix for the mobile node, it MUST reject the request and send a Proxy Binding Acknowledgement message with Status field set to 130 (Insufficient resources).

3. If the Home Network Prefix option present in the request has a specific prefix hint, the local mobility anchor before accepting that request, MUST ensure the prefix is owned by the local mobility anchor and further the mobile node is authorized to use that prefix. If the mobile node is not authorized to use that prefix, the local mobility anchor MUST reject the request and send a Proxy Binding Acknowledgement message with Status field set to NOT_AUTHORIZED_FOR_HOME_NETWORK_PREFIX (Mobile node not authorized to use that prefix).

4. Upon accepting the request, the local mobility anchor MUST create a Binding Cache entry for the mobile node. It must set the fields in the Binding Cache entry to the accepted values for that binding. If there is a Link-local Address option present in the request, the address must be copied to the link-local address field in the Binding Cache entry.

5. Upon accepting the Proxy Binding Update request, the local mobility anchor MUST establish a bi-directional tunnel to the mobile access gateway, as described in [RFC-2473]. Considerations from Section 5.6 must be applied.

Binding Re-Registration:

1. If the requesting prefix in the Home Network Prefix option is a non 0::/0 value and is different from what is present in the currently active Binding Cache entry for that mobile node, the local mobility anchor MUST reject the request and send a Proxy Binding Acknowledgement message with Status field set to 129 (Administratively Prohibited).

2. If there is a Link-local Address option present in the request with a value other than ALL_ZERO (not set), and upon accepting the binding re-registration request, the local mobility anchor MUST update the link-local address field in the Binding Cache entry to the address value received in the request.

3. Upon accepting a Proxy Binding Update request for extending the lifetime of a currently active binding for a mobile node, the local mobility anchor MUST update the existing Binding Cache entry for this mobile node. Unless there exists an established bi-directional tunnel to the mobile access gateway with the same transport and encapsulation mode, the local mobility anchor MUST create a tunnel to the mobile access gateway, as described in [RFC-2473] and also delete the existing tunnel route to the previous mobile access gateway. It MUST also send a Proxy Binding Acknowledgement message to the mobile access gateway with the Status field set to 0 (Proxy Binding Update Accepted).

Binding De-Registration:

1. If the received Proxy Binding Update request with the lifetime value of zero and the prefix in the Home Network Prefix option is a non 0::/0 value and is different from what is present in the currently active Binding Cache entry for that mobile node, the local mobility anchor MUST reject the request and send a Proxy

Binding Acknowledgement message with Status field set to 129 (Administratively Prohibited).

2. If the received Proxy Binding Update request with the lifetime value of zero, has a Source Address in the IPv6 header different from what is present in the Proxy-CoA address field in the Binding Cache entry existing for that mobile node, the local mobility anchor SHOULD ignore the request.

3. Upon accepting the Proxy Binding Update request for a mobile node, with the lifetime value of zero, the local mobility anchor MUST wait for MinDelayBeforeBCEDelete amount of time, before it deletes the mobile node's Binding Cache entry. Within this wait period, if the local mobility anchor receives a Proxy Binding Update request message for the same mobile node with the lifetime value of greater than zero, and if that request is accepted, then the Binding Cache entry MUST NOT be deleted, but must be updated with the newly accepted registration values. The local mobility anchor MUST send the Proxy Binding Acknowledgement message, immediately upon accepting the request. However, within this wait period, if the local mobility anchor does not receive any valid binding registration request for that mobile node, then at the end of this wait period, it MUST delete the mobile node's Binding Cache entry and remove the routing state created for that mobile node. In addition, during this MinDelayBeforeBCEDelete wait period, the local mobility anchor MUST continue to route the mobile node's data traffic.

Constructing the Proxy Binding Acknowledgement Message:

o The local mobility anchor when sending the Proxy Binding Acknowledgement message to the mobile access gateway MUST construct the message as specified below.

```
IPv6 header (src=LMAA, dst=Proxy-CoA)
     Mobility header
         -BA /*P flag is set*/
        Mobility Options
           - Home Network Prefix Option
           - Link-local Address Option (optional)
           - Timestamp Option (optional)
           - Mobile Node Identifier Option (Mandatory)
           - Access Technology Type option (Mandatory)
           - Mobile Node Interface Identifier option
             (Optional)
```

Figure 6: Proxy Binding Acknowledgement message format

- The Source Address field in the IPv6 header of the message MUST be set to the destination address of the received Proxy Binding Update request.

- The Destination Address field in the IPv6 header of the message MUST be set to the source address of the received Proxy Binding Update request.

- The Home Network Prefix option MUST be present in the Proxy Binding Acknowledgement message. If the option was not present in the request and if the Status field value is set to MISSING_HOME_NETWORK_PREFIX_OPTION, the value MUST be set to ALL_ZERO.

- The Access Technology Type option MUST be present. The access technology type value in the option MUST be copied from the Access Technology Type option in the received Proxy Binding Update request. If the option was not present in the request and if the Status field value is set to MISSING_ACCESS_TECH_TYPE_OPTION, the value MUST be set to 0.

- The Mobile Node Interface Identifier option MAY be present, if the same option was present in the corresponding Proxy Binding Update request message.

- If the Status field is set to a value greater than or equal to 128, i.e., if the binding request was rejected, then the prefix value in the Home Network Prefix option MUST be set to the prefix value from the received Home Network Prefix option. For all other cases, the prefix value MUST be set to the allocated prefix value for that mobile node.

- The Link-local Address option MUST be present in the Proxy Binding Acknowledgement message if and only if the same option was present in the corresponding Proxy Binding Update request message.

- If the Status field is set to a value greater than or equal to 128, i.e., if the binding request was rejected, then the link-local address value in the Link-local Address option MUST be set to the value from the received Link-local Address option.

- If there is an existing Binding Cache entry for the mobile node with the link-local address value of ALL_ZERO (value not set), or if there was no existing Binding Cache entry, then the link-local address MUST be copied from the Link-local Address option in the received Proxy Binding Update request. For all other cases, it

MUST be copied from the mobile node's Binding Cache entry.

- Considerations from Section 5.5 must be applied for constructing the Timestamp option.

- The identifier in the Mobile Node Identifier option [RFC-4283] MUST be copied from the received Proxy Binding Update request. If the Status field value is set to MISSING_MN_IDENTIFIER_OPTION, the identifier in the Mobile Node Identifier Option MUST be set to a zero length identifier.

- If IPsec is used for protecting the signaling messages, the message MUST be protected, using the security association existing between the local mobility anchor and the mobile access gateway.

- The Type 2 Routing header MUST NOT be present in the IPv6 header of the packet.

5.4. Multihoming Support

When a mobile node connects to a Proxy Mobile IPv6 domain through multiple interfaces simultaneously, the local mobility anchor MUST allocate a unique home network prefix for each of the connected interfaces.

The local mobility anchor MUST manage each of the allocated home network prefixes as part of a separate mobility session, each under a separate Binding Cache entry and with its own lifetime.

The local mobility anchor MUST allow for a handover between two different interfaces of the mobile node. In such a case, the home network prefix that is associated with a specific interface identifier of a mobile node will be updated with the new interface identifier. The decision on when to create a new mobility session and when to update an existing mobility session MUST be based on the Handover hint present in the signaling messages and under the considerations specified in this section.

The local mobility anchor MUST apply the following multihoming considerations when processing a received Proxy Binding Update request message.

Processing De-Registration Message:

1. If the received Proxy Binding Update message has lifetime value of zero, the local mobility anchor MUST verify if there is an

existing Binding Cache entry for the mobile node, identified by the MN-Identifier and with the Proxy-CoA address matching the source address in the IPv6 header of the received packet. If there exists a Binding Cache entry, the local mobility anchor MUST consider the message as a request for de-registering that specific mobility session. If there does not exist a Binding Cache entry, the message MUST be ignored.

Home Network Prefix Option (Non-Zero Prefix) present in the request:

1. The local mobility anchor MUST verify if there is an existing Binding Cache entry for the mobile node, identified by the MN-Identifier and with the home network prefix value matching the prefix value in the Home Network Prefix Option of the request. If there is a Mobile Node Interface Identifier Option present in the request, it MUST be ignored for this search. If there exists a Binding Cache entry matching the specified criteria, the local mobility anchor MUST consider the message as a request for updating that specific mobility session. The local mobility anchor upon accepting the request MUST update the existing Binding Cache entry and assign the home network prefix present in the Binding Cache entry. If there does not exist a Binding Cache entry matching this specified criteria, the below considerations MUST be applied.

Mobile Node Interface Identifier Option not present in the request:

1. The local mobility anchor MUST verify if there is an existing Binding Cache entry for the mobile node, identified by the MN-Identifier and with the interface identifier value set to ALL_ZERO.

2. If there does not exist a Binding Cache entry, the local mobility anchor upon accepting the request MUST assign a new home network prefix and create a new Binding Cache entry.

3. If there exists a Binding Cache entry and if the Handoff Indicator field in the Access Technology Type option present in the received Proxy Binding Update message is set to value 1 (Attachment over a new interface), the local mobility anchor upon accepting the request MUST assign a new home network prefix and create a new Binding Cache entry.

4. If there exists a Binding Cache entry and if the Handoff Indicator field in the Access Technology Type option present in the received Proxy Binding Update message is set to either value

2 (Handoff between interfaces) or 3 (Handoff between mobile access gateways for the same mobile node's interface), the local mobility anchor upon accepting the request MUST update the existing Binding Cache entry and assign the home network prefix present in the Binding Cache entry.

5. If there exists a Binding Cache entry and if the Handoff Indicator field in the Access Technology Type option present in the received Proxy Binding Update message is set to value 4 (Handoff state unknown), the local mobility anchor SHOULD wait till the existing Binding Cache entry is de-registered by the previously serving mobile access gateway, before it assigns the same home network prefix or updates the existing Binding Cache entry. However, if there is no de-registration message that is received within MinDelayBeforeNewBCEAssign amount of time, the local mobility anchor upon accepting the request MUST assign a new home network prefix and create a new Binding Cache entry. The local mobility anchor MAY also choose to assign a new home network prefix and without waiting for a de-registration message. It can use the access technology type value present in the request and as inputs for this decision.

6. Either upon creating a new Binding Cache entry or from matching an existing Binding Cache entry, after applying the above considerations, the access technology field in the Binding Cache entry MUST be copied from the Access Technology type option present in the received Proxy Binding Update message. The interface identifier field in the Binding Cache entry MUST be set to ALL_ZERO.

Mobile Node Interface Identifier Option present in the request:

1. The local mobility anchor MUST verify if there is an existing Binding Cache entry for the mobile node, identified by the MN-Identifier and with the interface identifier value matching the identifier value present in the received Mobile Node Interface Identifier Option.

2. If there exists a Binding Cache entry, the local mobility anchor upon accepting the request MUST update the existing Binding Cache entry and assign the home network prefix present in the Binding Cache entry.

3. If there does not exist a Binding Cache entry and if the Handoff Indicator field in the Access Technology Type option present in the received Proxy Binding Update message is set to value 1 (Attachment over a new interface), the local mobility anchor upon

accepting the request MUST assign a new home network prefix and create a new Binding Cache entry.

4. If there does not exist a Binding Cache entry and if the Handoff Indicator field in the Access Technology Type option present in the received Proxy Binding Update message is set to value 2 (Handoff between interfaces), the local mobility anchor MUST verify if there exists one and only one Binding Cache entry for the mobile node, identified by the MN-Identifier and with any interface identifier value. If there exists such an entry, the local mobility anchor upon accepting the request MUST update the existing Binding Cache entry and assign the home network prefix present in the Binding Cache entry.

5. If there does not exist a Binding Cache entry and if the Handoff Indicator field in the Access Technology Type option present in the received Proxy Binding Update message is set to value 2 (Handoff between interfaces), the local mobility anchor MUST verify if there exists a Binding Cache entry for the mobile node, identified by the MN-Identifier and with the home network prefix value matching the prefix value in the received Home Network Prefix option. If there exists a Binding Cache entry, the local mobility anchor upon accepting the request MUST assign the same prefix, else it MUST assign a new home network prefix and create a new Binding Cache entry.

6. If there exists a Binding Cache entry and if the Handoff Indicator field in the Access Technology Type option present in the received Proxy Binding Update message is set to value 4 (Handoff state unknown), the local mobility anchor SHOULD wait till the existing Binding Cache entry is de-registered by the previously serving mobile access gateway. However, if there is no de-registration message that is received within a given time, the local mobility anchor upon accepting the request MUST assign a new home network prefix and create a new Binding Cache entry. The local mobility anchor MAY also choose to assign a new home network prefix and without waiting for a de-registration message.

7. Either upon creating a new Binding Cache entry or from matching an existing Binding Cache entry, after applying the above considerations, the interface identifier field in the Binding Cache entry MUST be set to the value present in the received Mobile Node Interface Identifier Option and the access technology type MUST be copied from the Access Technology type option present in the received Proxy Binding Update message.

5.5. Timestamp Option for Message Ordering

Mobile IPv6 [RFC-3775] uses the Sequence Number field in binding registration messages as a way for the home agent to process the binding updates in the order they were sent by a mobile node. The home agent and the mobile node are required to manage this counter over the lifetime of a binding. However, in Proxy Mobile IPv6, as the mobile node moves from one mobile access gateway to another and in the absence of mechanisms such as context transfer between the mobile access gateways, the serving mobile access gateway will be unable to determine the sequence number that it needs to use in the signaling messages. Hence, the sequence number scheme, as specified in [RFC-3775], will be insufficient for Proxy Mobile IPv6.

If the local mobility anchor cannot determine the sending order of the received binding registration messages, it may potentially process an older message sent by a mobile access gateway where the mobile node was previously anchored, resulting in an incorrect Binding Cache entry.

For solving this problem, this specification adopts two alternative solutions. One is based on timestamps and the other based on sequence numbers, as defined in [RFC-3775].

The basic principle behind the use of timestamps in binding registration messages is that the node generating the message inserts the current time-of-day, and the node receiving the message checks that this timestamp is greater than all previously accepted timestamps. The timestamp based solution may be used, when the serving mobile access gateways in a Proxy Mobile IPv6 domain do not have the ability to obtain the last sequence number that was sent in a binding registration message for updating a given mobile node's binding.

As an alternative to the Timestamp based approach, the specification also allows the use of Sequence Number based scheme, as per [RFC-3775]. However, for this scheme to work, the serving mobile access gateways in a Proxy Mobile IPv6 domain MUST have the ability to obtain the last sequence number that was sent in a binding registration message for updating a given mobile node's binding. The sequence number MUST be maintained on a per mobile node basis and MUST be synchronized between the serving mobile access gateways. This may be achieved by using context transfer schemes or by maintaining the sequence number in a policy store. However, the specific details on how the mobile node's sequence number is synchronized between different mobile access gateways is outside the scope of this document.

Using Timestamps based approach:

1. A local mobility anchor implementation MUST support Timestamp option. If the Timestamp option is present in the received Proxy Binding Update request message, then the local mobility anchor MUST include a valid Timestamp option in the Proxy Binding Acknowledgement message that it sends to the mobile access gateway.

2. All the mobility entities in a Proxy Mobile IPv6 domain that are exchanging binding registration messages using the Timestamp option must have adequately synchronized time-of-day clocks. This is the essential requirement for this solution to work. If this requirement is not met, the solution will not predictably work in all cases.

3. The mobility entities in a Proxy Mobile IPv6 domain SHOULD synchronize their clocks to a common time source. For synchronizing the clocks, the nodes may use Network Time Protocol [RFC-4330]. Deployments may also adopt other approaches suitable for that specific deployment. Alternatively, if there is mobile node generated timestamp that is increasing at every attachment to the access link and if that timestamp is available to the mobile access gateway (Ex: The timestamp option in the SEND messages that the mobile node sends), the mobile access gateway can use this timestamp or sequence number in the Proxy Binding Update messages and does not have to depend on any external clock source. However, the specific details on how this is achieved is outside the scope of this document.

4. When generating the timestamp value for building the Timestamp option, the mobility entities MUST ensure that the generated timestamp is the elapsed time past the same reference epoch, as specified in the format for the Timestamp option [Section 8.7].

5. If the Timestamp option is present in the received Proxy Binding Update message, the local mobility anchor MUST ignore the sequence number field in the message. However, it MUST copy the sequence number from the received Proxy Binding Update message to the Proxy Binding Acknowledgement message.

6. Upon receipt of a Proxy Binding Update message with the Timestamp option, the local mobility anchor MUST check the timestamp field for validity. In order for it to be considered valid, the timestamp value contained in the Timestamp option MUST be close enough to the local mobility anchor's time-of-day clock and the timestamp MUST be greater than all previously accepted timestamps in the Proxy Binding Update messages sent for that mobile node.

7. If the timestamp value in the received Proxy Binding Update is valid (validity as specified in the above considerations), the local mobility anchor MUST return the same timestamp value in the Timestamp option included in the Proxy Binding Acknowledgement message that it sends to the mobile access gateway.

8. If the timestamp value in the received Proxy Binding Update is lower than the previously accepted timestamp in the Proxy Binding Update messages sent for that mobility binding, the local mobility anchor MUST reject the Proxy Binding Update request and send a Proxy Binding Acknowledgement message with Status field set to TIMESTAMP_LOWER_THAN_PREV_ACCEPTED (Timestamp lower than previously accepted timestamp). The message MUST also include the Timestamp option with the value set to the current time-of-day on the local mobility anchor.

9. If the timestamp value in the received Proxy Binding Update is not valid (validity as specified in the above considerations), the local mobility anchor MUST reject the Proxy Binding Update and send a Proxy Binding Acknowledgement message with Status field set to TIMESTAMP_MISMATCH (Timestamp mismatch). The message MUST also include the Timestamp option with the value set to the current time-of-day on the local mobility anchor.

Using Sequence Number based approach:

1. If the Timestamp option is not present in the received Proxy Binding Update request, the local mobility anchor MUST fallback to the Sequence Number based scheme. It MUST process the sequence number field as specified in [RFC-3775]. Also, it MUST NOT include the Timestamp option in the Proxy Binding Acknowledgement messages that it sends to the mobile access gateway.

2. An implementation MUST support Sequence Number based scheme, as per [RFC-3775].

5.6. Routing Considerations

5.6.1. Bi-Directional Tunnel Management

- A bi-directional tunnel MUST be established between the local mobility anchor and the mobile access gateway with IP-in-IP encapsulation, as described in [RFC-2473]. The tunnel end points are the Proxy-CoA and LMAA. When using IPv4 transport with a specific encapsulation mode, the end points of the tunnel are the

IPv4-LMAA and IPv4-Proxy-CoA, as specified in [ID-IPV4-PMIP6].

- The bi-directional tunnel MUST be used for routing the mobile node's data traffic between the mobile access gateway and the local mobility anchor. The tunnel hides the topology and enables a mobile node to use an address from its home network prefix from any access link attached to the mobile access gateway.

- The bi-directional tunnel is established after accepting the Proxy Binding Update request message. 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. Implementations MAY choose to use static tunnels instead of dynamically creating and tearing them down on a need basis.

- Implementations MAY use a software timer for managing the tunnel lifetime and a counter for keeping a count of all the mobile nodes that are sharing the tunnel. The timer value MUST be set to the accepted binding lifetime and will be updated after each periodic re-registration for extending the lifetime. If the tunnel is shared for multiple mobile nodes, the tunnel lifetime MUST be set to the highest binding lifetime that is granted to any one of those mobile nodes sharing that tunnel.

5.6.2. Forwarding Considerations

Intercepting Packets Sent to the Mobile Node's Home Network:

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

Forwarding Packets to the Mobile Node:

- On receiving a packet from a correspondent node with the destination address matching a mobile node's home network prefix, the local mobility anchor MUST forward the packet through the bi-directional tunnel setup for that mobile node. The format of the tunneled packet is shown below. However, when using IPv4 transport, the format of the packet is as described in [ID-IPV4-PMIP6].

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

Figure 7: Tunneled Packets from LMA to MAG

Forwarding Packets Sent by the Mobile Node:

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

5.7. Local Mobility Anchor Address Discovery

Dynamic Home Agent Address Discovery, as explained in Section 10.5 [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.

The DHAAD message in the current form cannot be used in Proxy Mobile IPv6 for discovering the address of the mobile node's local mobility anchor. In Proxy Mobile IPv6, the local mobility anchor will not be able to receive any messages sent to the Mobile IPv6 Home-Agents anycast address corresponding to the mobile node's home network prefix, as the prefix is not hosted on any of its interfaces. Further, the mobile access gateway will not predictably be able to locate the serving local mobility anchor that has the mobile node's binding cache entry. Hence, this specification does not support Dynamic Home Agent Address Discovery protocol.

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 other 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.

5.8. 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 it is 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 node 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. Hence, this specification does not support Mobile Prefix Discovery.

5.9. Route Optimizations Considerations

The Route Optimization in Mobile IPv6, as defined in [RFC-3775], enables a mobile node to communicate with a correspondent node directly using its care-of address and further the Return Routability procedure enables the correspondent node to have reasonable trust that the mobile node is reachable at both its home address and care-of address.

In Proxy Mobile IPv6, the mobile node is not involved in any IP mobility related signaling. The mobile node uses only its home address for all its communication and the Care-of address (Proxy-CoA) is not visible to the mobile node. Hence, the Return Routability procedure as defined in Mobile IPv6 cannot be used in Proxy Mobile IPv6.

6. Mobile Access Gateway Operation

The Proxy Mobile IPv6 protocol described in this document introduces a new functional entity, the Mobile Access Gateway (MAG). The mobile access gateway is the entity that is responsible for detecting the mobile node's movements on its access link and sending the binding registration requests to the local mobility anchor. In essence, the mobile access gateway performs mobility management on behalf of a mobile node.

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 or the signaling interactions between those functional entities are beyond the scope of this document.

The mobile access gateway has the following key functional roles:

- It is responsible for detecting the mobile node's movements on the 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 by sending Router Advertisements with the mobile node's home network prefix information.

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

6.1. Extensions to Binding Update List Entry Data Structure

Every mobile access gateway MUST maintain a Binding Update List. Each entry in the Binding Update List represents a mobile node's mobility binding with its local mobility anchor. The Binding Update List is a conceptual data structure, described in Section 11.1 [RFC-3775].

For supporting this specification, the conceptual Binding Update List entry data structure needs be extended with the following additional fields.

- The Identifier of the attached mobile node, MN-Identifier. This identifier is acquired during the mobile node's attachment to the access link through mechanisms outside the scope of this document.

- The interface identifier of the mobile node's connected interface. This address can be acquired from the received Router Solicitation messages from the mobile node or during the mobile node's attachment to the access network. This is typically a Layer-2 identifier conveyed by the mobile node; however, the specific details on how that is conveyed is out of scope for this specification.

- The IPv6 home network prefix of the attached mobile node. The home network prefix of the mobile node is acquired from the mobile node's local mobility anchor through the received Proxy Binding Acknowledgement messages. The IPv6 home network prefix also includes the corresponding prefix length.

- The Link-local address of the mobile node on the interface attached to the access link.

- The IPv6 address of the local mobility anchor serving the attached mobile node. This address is acquired from the mobile node's policy profile or from other means.

- The Interface identifier (If-Id) of the access link where the mobile node is currently attached. This is internal to the mobile

access gateway and is used to associate the Proxy Mobile IPv6 tunnel to the right access link where the mobile node is attached.

- The interface identifier (If-Id) of the bi-directional tunnel between the mobile node's local mobility anchor and the mobile access gateway. This is internal to the mobile access gateway. The tunnel interface identifier is acquired during the tunnel creation.

6.2. 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. The policy profile MAY also be handed over to a serving mobile access gateway as part of a context transfer procedure during a handoff or the serving mobile access gateway MAY be able to dynamically generate this profile. 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)

The following are the optional fields of the policy profile:

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

- Supported address configuration procedures (Stateful, Stateless or both) on the access links in the Proxy Mobile IPv6 domain

6.3. Supported Access Link Types

This specification supports only point-to-point access link types and thus it assumes that the mobile node and the mobile access gateway are the only two nodes on the access link. The link is assumed to have multicast capability. This protocol may also be used on other link types, as long as the link is configured in such a way that it guarantees a point-to-point delivery between the mobile node and the mobile access gateway for all the protocol traffic.

6.4. 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. However, the advertised flags with respect to 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.

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-4862] or as per Privacy extension specification [RFC-4941].

When stateful address autoconfiguration is supported on the link, the mobile node can obtain the address configuration from the DHCPv6 server using DHCPv6 client protocol, as specified in DHCPv6 specification [RFC-3315].

Additionally, 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.

6.5. 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 SHOULD 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 between the mobile node and mobile access gateway, before the protocol operation begins.

6.6. Acquiring Mobile Node's Identifier

All the network entities in a Proxy Mobile IPv6 domain MUST be able to identify a mobile node, using its MN-Identifier. This identifier MUST be stable across the Proxy Mobile IPv6 domain and the entities

must be able to use this identifier in the signaling messages. Typically, this identifier is obtained as part of the access authentication or through other means as specified below.

- The identifier of the mobile node that the mobile access gateway obtains typically as part of the access authentication or from the notified network attachment event, can be a temporary identifier and this identifier may also change at each re-authentication. However, the mobile access gateway MUST be able to use this identifier and obtain the mobile node's MN-Identifier from the policy store, such as from the RADIUS attribute, Chargeable-User-Identifier [RFC-4372].

- The MN-Identifier that the policy store delivers to the mobile access gateway may not be the true identifier of the mobile node. However, the mobility access gateway MUST be able to use this identifier in the signaling messages exchanged with the local mobility anchor.

- The mobile access gateway MUST be able identify the mobile node by its MN-Identifier and it MUST be able to associate this identity to the sender of any IPv4 or IPv6 packets on the access link.

6.7. Home Network Emulation

One of the key functions of a mobile access gateway is to emulate the mobile node's home network 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 initial address configuration after it moved into that Proxy Mobile IPv6 domain.

For emulating the mobile node's home link on the access link, the mobile access gateway must be able to send Router Advertisements advertising the mobile node's home network prefix and other address configuration parameters consistent with its home link properties. Typically, these configuration settings will be based on the domain wide policy or based on a policy specific to each mobile node.

Typically, the mobile access gateway learns the mobile node's home network prefix information from the received Proxy Binding Acknowledgement message or it may be obtained from the mobile node's policy profile. However, the mobile access gateway SHOULD send the Router Advertisements advertising the mobile node's home network prefix only after successfully completing the binding registration with the mobile node's local mobility anchor.

When advertising the home network prefix in the Router Advertisement messages, the mobile access gateway MAY set the prefix lifetime value

for the advertised prefix to any chosen value at its own discretion. An implementation MAY choose to tie the prefix lifetime to the mobile node's binding lifetime. The prefix lifetime can also be an optional configuration parameter in the mobile node's policy profile.

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, will continue to detect its home network and thus making it 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 mobile node is DNAv6 enabled, as specified in [ID-DNAV6], it may not detect the link change due to DNAv6 optimizations and may 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-4862], there is a very low possibility of a link-local address collision between the two neighbors on that access link.

For solving this problem, this specification allows the mobile access gateway to upload the mobile node's link-local address to the local mobility anchor using the Link-local Address option, exchanged in the binding registration messages. The mobile access gateway can learn the mobile node's link-local address, by snooping the DAD messages sent by the mobile node for establishing the link-local address uniqueness on the access link. Subsequently, at each handoff, the mobile access gateway can obtain this address from the local mobility anchor to ensure link-local address uniqueness and change its own link-local address, if it detects a collision.

Alternatively, 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 on the global and link-local addresses every time the interface detects a handover, even when DNAv6 does not detect a link change.

However, this issue will not impact point-to-point links based on a 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, IPV6CP [RFC-5072] 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 whenever 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.

The issue of address collision is not relevant to the mobile node's global address. Since there is a unique home network prefix assigned for each mobile node, the uniqueness for the mobile node's global address is assured on the access link.

6.9. Signaling Considerations

6.9.1. Binding Registrations

Mobile Node Attachment and Initial Binding Registration:

1. After detecting a new mobile node on its access link, the mobile access gateway must identify the mobile node and acquire its MN-Identifier. If it determines that the network-based mobility management service needs to be offered to the mobile node, it MUST send a Proxy Binding Update message to the local mobility anchor. If there is no existing Binding Update List entry for that mobile node, the mobile access gateway MUST create a Binding Update List entry upon sending the Proxy Binding Update request.

2. The Proxy Binding Update message MUST include the Mobile Node Identifier option [RFC-4283], identifying the mobile node, the Home Network Prefix option, either the Timestamp option or a valid sequence number and optionally the Link-local Address option. When Timestamp option is added to the message, the mobile access gateway MAY set the Sequence Number field to a value of a monotonically increasing counter and the local mobility anchor will ignore this field, but will return the same

value in the Proxy Binding Acknowledgement message. This will be useful for matching the reply to the request message.

3. The Home Address option MUST NOT be present in the Destination Option extension header of the Proxy Binding Update message.

4. The Access Technology Type option MUST be present in the Proxy Binding Update message. The access technology Type field in the option MUST be set to the access technology using which the mobile node is currently attached to the mobile access gateway. The Handoff Indicator field in the Access Technology Type option MUST be set to the appropriate value. The specific details on how the mobile access gateway is able to determine if the mobile node's current attachment is due to a handoff of an existing mobility session or if it is as a result of an attachment over a different interface is outside the scope of this document.

5. The Handoff Indicator field in the Access Technology Type option MUST be set to value 1 (Attachment over a new interface), if the mobile access gateway predictably knows that the mobile node's attachment to the network using the current interface is due to neither a handover between two interfaces of the mobile node nor a handover of the mobility session for the same interface of the mobile node between two mobile access gateways. This essentially serves as a request to the local mobility anchor to allocate a new home network prefix for this mobility session and not update any existing Binding Cache entry created for the same mobile node connected to the Proxy Mobile IPv6 domain through a different interface.

6. The Handoff Indicator field in the Access Technology Type option MUST be set to value 2 (Handoff between interfaces), if the mobile access gateway definitively knows the mobile node's current attachment is due to a handoff of the mobility session between two interfaces of the mobile node.

7. The Handoff Indicator field in the Access Technology Type option MUST be set to value 3 (Handoff between mobile access gateways for the same interface), if the mobile access gateway definitively knows the mobile node's current attachment is due to a handoff of the mobility session between different mobile access gateways and for the same interface of the mobile node.

8. The Handoff Indicator field in the Access Technology Type option MUST be set to value 4 (Handoff State Unknown), if the mobile access gateway cannot predictably know if the mobile node's session is due to a handoff.

9. The Mobile Node Interface Identifier option carrying the identifier of the currently attached interface MUST be present in the Proxy Binding Update message, if the mobile access gateway knows the interface identifier of the mobile node's currently attached interface. The "P" Flag in the option MUST be set to 0, indicating that the carried identifier is the currently attached interface identifier. If the interface identifier is not known, this identifier MUST NOT be present.

10. 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 Prefix option for requesting the local mobility anchor to allocate that prefix. If the specified value is 0::/0, then the local mobility anchor will consider this as a request for prefix allocation.

Receiving Binding Registration Reply:

1. The mobile access gateway MUST observe the rules described in Section 9.2 [RFC-3775] when processing Mobility Headers in the received Proxy Binding Acknowledgement message (a Binding Acknowledgement message with the 'P' flag set).

2. The message MUST be authenticated as described in Section 4.0. When IPsec is used for message authentication, the SPI in the IPsec header [RFC-4306] of the received packet is needed for locating the security association, for authenticating the Proxy Binding Acknowledgement reply.

3. The mobile access gateway MUST apply the considerations specified in Section 5.5 for processing the Sequence Number field and the Timestamp option, in the message.

4. The mobile access gateway MUST ignore any checks, specified in [RFC-3775] related to the presence of Type 2 Routing header in the Proxy Binding Acknowledgement message.

5. If the Timestamp option is present in the received Proxy Binding Acknowledgement message and with the Status field value set to any value other than TIMESTAMP_MISMATCH (Invalid Timestamp), the mobile access gateway MAY use the timestamp value for matching the response to the request message that it sent recently. For all other cases, it MAY use the sequence number in combination with the identifier present in the Mobile Node Identifier option for matching the response to the request.

6. If the received Proxy Binding Acknowledgement message has the Status field value set to PROXY_REG_NOT_ENABLED (Proxy registration not enabled for the mobile node), the mobile access gateway SHOULD NOT send binding registration requests again for that mobile node. It must also deny the mobility service to that mobile node.

7. If the received Proxy Binding Acknowledgement message has the Status field value set to TIMESTAMP_LOWER_THAN_PREV_ACCEPTED (Timestamp lower than previously accepted timestamp), the mobile access gateway SHOULD try to register again to reassert the mobile node's presence to the mobility anchor. The mobile access gateway is not specifically required to synchronize its clock upon receiving this error code.

8. If the received Proxy Binding Acknowledgement message has the Status field value set to TIMESTAMP_MISMATCH (Invalid Timestamp), the mobile access gateway SHOULD try to register again only after it has synchronized its clock to a common time source that is used by all the mobility entities in that domain for their clock synchronization. The mobile access gateway SHOULD NOT synchronize its clock to the local mobility anchor's system clock, based on the timestamp present in the received message.

9. If the received Proxy Binding Acknowledgement message has the Status field value set to NOT_AUTHORIZED_FOR_HOME_NETWORK_PREFIX (Not authorized for that prefix), the mobile access gateway SHOULD try to request for that prefix in the binding registration request, only after it learned the validity of that prefix.

10. If the received Proxy Binding Acknowledgement message has the Status field value set to any value greater than or equal to 128 (i.e., if the binding is rejected), the mobile access gateway MUST NOT advertise the mobile node's home network prefix in the Router Advertisements sent on that access link and there by denying mobility service to the mobile node.

11. If the received Proxy Binding Acknowledgement message has the Status field value set to 0 (Proxy Binding Update accepted), the mobile access gateway MUST setup the routing state, as explained in section 6.10, and MUST also update the Binding Update List entry for reflecting the accepted binding registration status.

12. If the received Proxy Binding Acknowledgement message has the address in the Link-local Address option set to a value that matches its own link-local address on that access interface

where the mobile node is anchored, the mobile access gateway MUST change its link-local address on that interface.

Extending Binding Lifetime:

1. For extending the lifetime of a currently registered mobile node (i.e., if there exists a Binding Update List entry for that mobile node), the mobile access gateway MUST send a Proxy Binding Update message to the local mobility anchor. The prefix value in the Home Network Prefix option present in the request SHOULD be set to the currently registered home network prefix and the value in the Link-local Address option MAY be set to ALL_ZERO or to the link-local address of the mobile node.

Mobile Node Detachment and Binding De-Registration:

1. At any point, if the mobile access gateway detects that the mobile node has moved away from its access link, it SHOULD send a Proxy Binding Update message to the local mobility anchor with the lifetime value set to zero.

2. Either upon receipt of a Proxy Binding Acknowledgement message from the local mobility anchor or after a MinPBUReplyTime timeout waiting for the reply, the mobile access gateway MUST remove the Binding Cache entry for that mobile node from its Binding Update List and withdraw the mobile node's home network prefix as the hosted on-link prefix on that access link.

Constructing the Proxy Binding Update Message:

- The mobile access gateway when sending the Proxy Binding Update request to the local mobility anchor MUST construct the message as specified below.

```
IPv6 header (src=Proxy-CoA, dst=LMAA)
     Mobility header
         -BU /*P & A flags are set*/
        Mobility Options
           - Home Network Prefix option
           - Link-local Address option (Optional)
           - Timestamp Option (optional)
           - Mobile Node Identifier option
           - Access Technology Type option (Mandatory)
           - Mobile Node Interface Identifier option
             (Optional)
```

Figure 8: Proxy Binding Update message format

- The Source Address field in the IPv6 header of the message MUST be set to the address of the mobile access gateway.
- The Destination Address field in the IPv6 header of the message MUST be set to the local mobility anchor address.
- The Home Network Prefix option MUST be present. The prefix value MAY be set 0::/0 or to a specific prefix value.
- The Link-local Address option MAY be present. The value MAY be set to ALL_ZERO or the mobile node's link-local address.
- The Access Technology Type option MUST be present. The value MUST be set to the type of the access technology using which the mobile node is currently attached to the mobile access gateway.
- The Mobile Node Interface Identifier option MAY be present.
- Considerations from Section 5.5 must be applied for constructing the Timestamp option.
- The Mobile Node Identifier option [RFC-4283] MUST be present, the identifier field in the option MUST be set to mobile node's identifier, MN-Identifier.
- If IPsec is used for protecting the signaling messages, the message MUST be protected, using the security association existing between the local mobility anchor and the mobile access gateway.

6.9.2. Router Solicitation Messages

The mobile node may send a Router Solicitation message on the access link whenever the link-layer detects a media change. The Source Address in the IPv6 header of the Router Solicitation message may either be the link-local address of the mobile node or an unspecified address (::).

1. The mobile access gateway on receiving the Router Solicitation message SHOULD send a Router Advertisement containing the mobile node's home network prefix as the on-link prefix. However, before sending the Router Advertisement message containing the mobile node's home network prefix, it SHOULD complete the binding registration process with the mobile node's local mobility anchor.

2. If the local mobility anchor rejects the binding registration request, or, if the mobile access gateway failed to complete the binding registration process for whatever reasons, the mobile access gateway MUST NOT advertise the mobile node's home network prefix in the Router Advertisement messages that it sends on the access link. However, it MAY choose to advertise a local visited network prefix to enable the mobile node for regular IPv6 access.

6.9.3. Retransmissions and Rate Limiting

The mobile access gateway is responsible for retransmissions and rate limiting the binding registration requests that it sends for updating a mobile node's binding. Implementations MUST follow the below guidelines.

1. When the mobile access gateway sends a Proxy Binding Update request, it should use the constant, INITIAL_BINDINGACK_TIMEOUT [RFC-3775], for configuring the retransmission timer.

2. If the mobile access gateway fails to receive a valid matching response within the retransmission interval, it SHOULD retransmit the message until a response is received. However, the mobile access gateway MUST ensure the mobile node is still attached to the connected link before retransmitting the message.

3. As specified in Section 11.8 [RFC-3775], the mobile access gateway MUST use an exponential back-off process in which the timeout period is doubled upon each retransmission, until either the node receives a response or the timeout period reaches the value MAX_BINDACK_TIMEOUT [RFC-3775]. The mobile access gateway

MAY continue to send these messages at this slower rate indefinitely.

4. If Timestamp based scheme is in use, the retransmitted Proxy Binding Update messages MUST use the latest timestamp. If Sequence number scheme is in use, the retransmitted Proxy Binding Update messages MUST use a Sequence Number value greater than that used for the previous transmission of this Proxy Binding Update message, just as specified in [RFC-3775].

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.

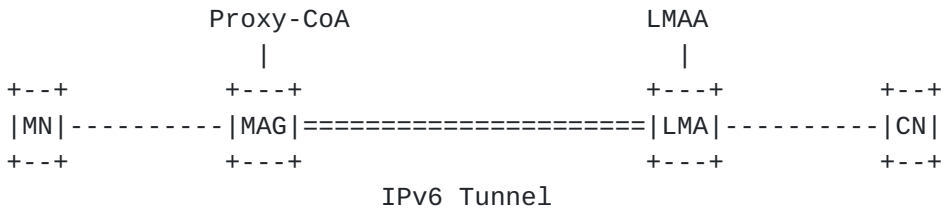


Figure 9: Proxy Mobile IPv6 Tunnel

6.10.1. Transport Network

The transport network between the local mobility anchor and the mobile access gateway can be either an IPv6 or IPv4 network. However, this specification only deals with the IPv6 transport and the companion document [ID-IPV4-PMIP6] specifies the required extensions for negotiating IPv4 transport and the corresponding encapsulation mode for supporting this protocol operation.

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 datagram to be encapsulated as a payload of another IPv6 packet and to 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 gets 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.

- IPv6-In-IPv6 - IPv6 datagram encapsulated in an IPv6 packet [RFC-2473].

- IPv6-In-IPv4 - IPv6 datagram encapsulation in an IPv4 packet. The details on how this mode is negotiated is specified in [ID-IPV4-PMIP6].

- IPv6-In-IPv4-UDP - IPv6 datagram encapsulation in an IPv4 UDP packet. This mode is specified in [ID-IPV4-PMIP6].

6.10.3. Routing State

The following section explains 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, (IPv6 Prefix or Input Interface	_ANY_DESTINATION_	Tunnel1
	Locally Connected	direct

Figure 10: 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

Figure 11: Example - Tunnel Interface Table

6.10.4. Local Routing

If there is data traffic between a visiting mobile node and a correspondent 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. The configuration variable, EnableMAGLocalRouting MAY be used for controlling this aspect. However, in some systems, this may have 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 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 are beyond of the scope of this document.

6.10.5. Tunnel Management

All the considerations mentioned in Section 5.6.1 for the tunnel management on the local mobility anchor apply for the mobile access gateway as well.

6.10.6. Forwarding Rules

Forwarding Packets sent to the Mobile Node's Home Network:

- On receiving a packet from the bi-directional tunnel established with the mobile node's local mobility anchor, the mobile access gateway MUST use the destination address of the inner packet for forwarding it on the interface where the destination network prefix 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 a scenario, in the form of ICMP control message, the considerations from Generic Packet Tunneling specification [RFC-2473] must be applied.

- On receiving a packet from a correspondent node that is locally connected and which is destined to a mobile node that is on another locally connected access link, 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 mobile node. 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 node's local mobility anchor. Otherwise, it can route the packet directly to the mobile node.

Forwarding Packets Sent by the Mobile Node:

- 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 node's local mobility anchor. Otherwise, it can route the packet directly to the destination.

- On receiving a packet from the mobile node connected to its access link, to a destination that is not directly connected, the packet MUST be forwarded to the local mobility anchor through the bi-directional tunnel established between itself and the mobile node's local mobility anchor. However, the packets that are sent with the link-local source address MUST NOT be forwarded. The format of the tunneled packet is shown below. However, when using IPv4 transport, the format of the tunneled packet is as described in [ID-IPV4-PMIP6].

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

Figure 12: Tunneled Packets from MAG to LMA

6.11. Supporting DHCPv6 based Address Configuration on the Access Link

This section explains how Stateful Address Configuration using DHCPv6 can be enabled on the access link attached to a mobile access gateway and how a mobile node attached to that link can obtain an address from its home network prefix using DHCPv6.

- For supporting Stateful Address Configuration using DHCPv6, the DHCPv6 relay agent [RFC-3315] service MUST be enabled on each of the access links in the Proxy Mobile IPv6 domain. Further, as specified in Section 20 [RFC-3315], the relay agent should be configured to use a list of destination addresses, which MAY include unicast addresses, the All_DHCP_Servers multicast address, or other addresses selected by the network administrator.

- The DHCPv6 server in the Proxy Mobile IPv6 domain can be configured with a list of prefix pools (P1, P2, ..., Pn). Each one of these prefix pools corresponds to a home network prefix that a local mobility anchor allocates to a mobile node in that domain. However, the DHCPv6 server will not know the relation between a given address pool and a mobile node to which the corresponding prefix is allocated. It just views these pools as prefixes hosted on different links in that domain.

- When a mobile node sends a DHCPv6 request message, the DHCP relay agent function on the access link will set the link-address field in the DHCP message to an address in the mobile node's home network prefix, so as to provide a prefix hint to the DHCP Server for the address pool selection. The DHCP server on receiving the request from the mobile node, will allocate an address from the prefix pool present in the link-address field of the request.

- Once the mobile node obtains an address and moves to a different link and sends a DHCP request, the DHCP relay agent on the new link will set the prefix hint in the DHCP messages to the mobile node's home network prefix. The DHCP server will identify the client from the Client-DUID option and present in the request and will allocate the same address as before.

- The DHCP based address configuration is not recommended for deployments where the local mobility anchor and the mobile access gateways are located in different administrative domains. For this configuration to work, all the mobile access gateways in the Proxy Mobile IPv6 domain should be able to ensure that the DHCP requests from a given mobile node anchored on any of the access links in that domain, will always be handled by the same DHCP server.

- The DHCP server should be configured to offer low address lease times. A lease time that is too large prevents the DHCP server from reclaiming the address even after the local mobility anchor deletes the mobile node's binding cache entry.

6.12. 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 about the mobile node's home network prefix renumbering are outside the scope of this document.

6.13. 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 SHOULD 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

6.14. 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 IP access to some other nodes. This requires the network to have control on when to enable network-based mobility management service to a mobile node and when to enable regular IPv6 access. This specification does not disallow such configuration.

Upon detecting a mobile node on its access link and after policy considerations, the mobile access gateway MUST determine if network-based mobility management service should be offered to that mobile node. If the mobile node is entitled for network-based mobility management 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 determined from the policy considerations, the mobile access gateway MAY choose to offer regular IPv6 access to the mobile node and in such scenario the normal IPv6 considerations

apply. If IPv6 access is enabled, the mobile node SHOULD be able to obtain an IPv6 address using normal IPv6 address configuration procedures. The obtained address must be from a local visitor network prefix. This essentially ensures that the mobile access gateway functions as a normal access router to a mobile node attached to its access link and with out impacting its host-based mobility protocol operation.

7. Mobile Node Operation

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

7.1. Moving into a Proxy Mobile IPv6 Domain

Once a mobile node enters a Proxy Mobile IPv6 domain and attaches to an access network, the mobile access gateway on the access link detects the attachment of the mobile node and completes the binding registration with the mobile node's local mobility anchor. If the binding update operation is successfully performed, the mobile access gateway will create the required state and setup the data path for the mobile node's data traffic.

If the mobile node is IPv6 enabled, on attaching to the access link, it will typically send Router Solicitation message [RFC-4861]. The mobile access gateway on the access 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.

If the mobile access gateway on the access link, receives a Router Solicitation message from the mobile node, before it completed the signaling with the mobile node's local mobility anchor, the mobile access gateway may not know the mobile node's home network prefix and may not be able to emulate the mobile node's home link on the access link. In such scenario, the mobile node may notice a slight delay before it receives a Router Advertisement message.

If the received Router Advertisement has the Managed Address Configuration flag set, the mobile node, as it would normally do, will send a DHCPv6 Request [RFC-3315]. The DHCP relay service enabled on that access link will ensure the mobile node will obtain its IPv6 address as a lease from its home network prefix.

If the received 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 be able to obtain

an IPv6 address using an interface identifier generated as per the Autoconf specification [RFC-4862] or as per the Privacy Extensions specification [RFC-4941].

If the mobile node is IPv4 enabled and if the network permits, it will be able to obtain the IPv4 address configuration for the connected interface by using DHCP [RFC-2131]. The details related to IPv4 support is specified in the companion document [ID-IPV4-PMIP6].

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

7.2. Roaming in the Proxy Mobile IPv6 Domain

After obtaining the address configuration in the Proxy Mobile IPv6 domain, as the mobile node moves and changes its point of attachment from one mobile access gateway to the other, it can still continue to use the same address configuration. As long as the attached access network is in the scope of that Proxy Mobile IPv6 domain, the mobile node will always detect the same link, where it obtained its initial address configuration. If the mobile node performs DHCP operation, it will always obtain the same address as before.

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 does not require any changes to the mobile node's IP stack. It assumes the mobile node to be a normal IPv4/IPv6 node, with its protocol operation consistent with the respective specifications.

However, for achieving protocol efficiency and for faster hand-offs, implementations may choose to adjust the following IPv6 operating parameters on the mobile node be adjusted to the below recommended values.

Lower Default-Router List Cache Time-out:

As per the base IPv6 specification [RFC-4861], each IPv6 host is required to 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 case of Proxy Mobile IPv6, when a mobile node moves from one link to another, the source address of the received Router Advertisement messages advertising the mobile node'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 and not the previously known 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 [RFC-4861]. This action will help in minimizing packet losses during a hand off switch.

On detecting a reachability problem, the mobile node will certainly detect the default-router loss by performing the 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.

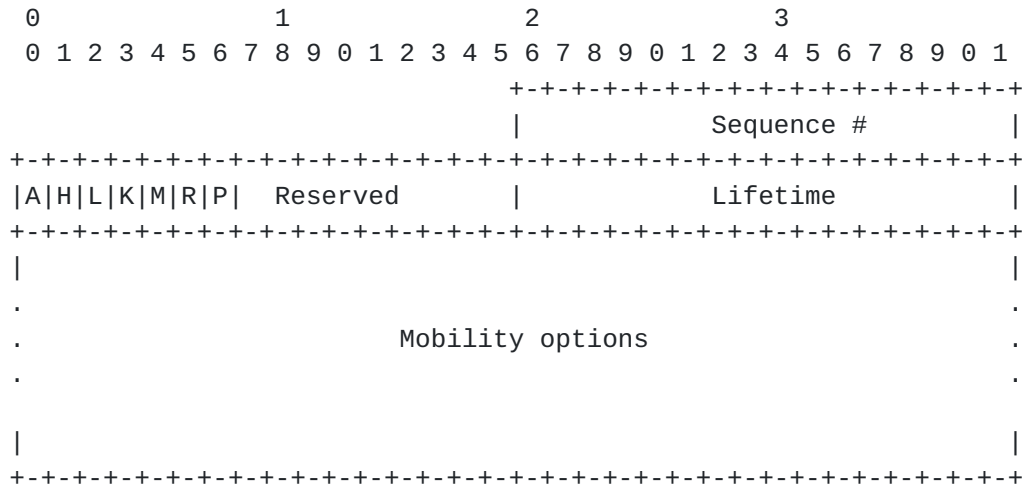
In access network where SEND [RFC-3971] is not deployed, the mobile access gateway may withdraw the previous default-router entry, by sending a Router Advertisement using the link-local address that of the previous mobile access gateway and with the Router Lifetime field set to value 0, then this will force the flush of the Previous Default-Router entry from the mobile node's cache. This certainly requires 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 fixed link-local address for all the mobility entities in a Proxy Mobile IPv6 domain and where SEND [RFC-3971] is not deployed. In such scenario, the mobile node is not required to update the default-router entry. However, 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 Message



A Binding Update message that is sent by a mobile access gateway to a local mobility anchor is referred to as the "Proxy Binding Update" message. A new flag (P) is included in the Binding Update message. The rest of the Binding Update message format remains the same as defined in [RFC-3775] and with the additional (R) and (M) flags as specified in [RFC-3963] and [RFC-4140] respectively.

Proxy Registration Flag (P)

A new flag (P) is included in the Binding Update message to indicate to the local mobility anchor that the Binding Update message is a proxy registration. 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.

Mobility Options

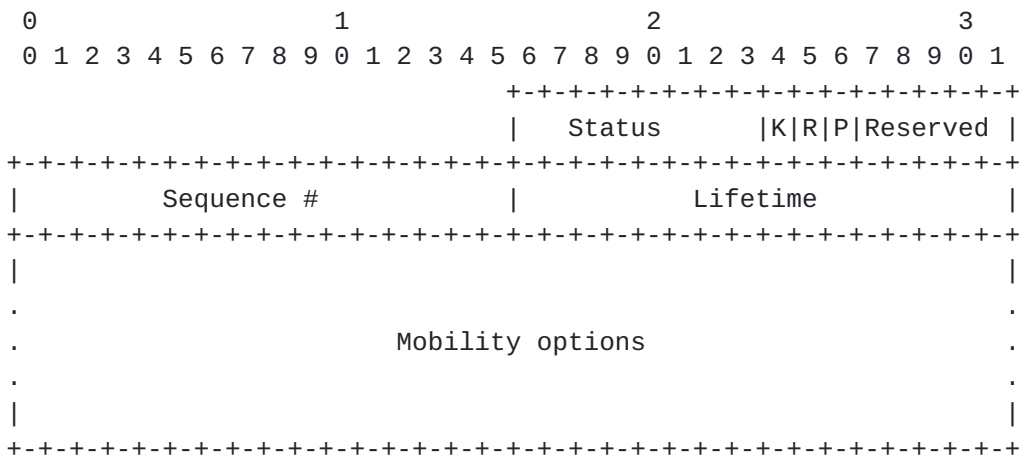
Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2 [RFC-3775]. The local mobility anchor MUST ignore and skip any options which it does not understand.

As per this specification, the following mobility options are valid in a Proxy Binding Update message:

- Home Network Prefix option
- Link-local Address option
- Mobile Node Identifier Option
- Access Technology Type option
- Mobile Node Interface Identifier option
- Timestamp option

For descriptions of other fields present in this message, refer to section 6.1.7 [RFC-3775].

8.2. Proxy Binding Acknowledgement Message



A Binding Acknowledgement message that is sent by a local mobility anchor to a mobile access gateway is referred to as the "Proxy Binding Acknowledgement" message. A new flag (P) is included in the Binding Acknowledgement message. The rest of the Binding Acknowledgement message format remains the same as defined in [RFC-3775] and with the additional (R) and (M) flags as specified in [RFC-3963] and [RFC-4140] respectively.

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.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The encoding and format of defined options are described in Section 6.2 [RFC-3775]. The mobile access gateway MUST ignore and skip any options which it does not understand.

As per this specification, the following mobility options are valid in a Proxy Binding Acknowledgement message:

- Home Network Prefix option
- Link-local Address option
- Mobile Node Identifier option
- Access Technology Type option
- Mobile Node Interface Identifier option
- Timestamp option

Status

8-bit unsigned integer indicating the disposition of the Proxy Binding Update. Values of the Status field less than 128 indicate that the Proxy Binding Update was accepted by the local mobility anchor. Values greater than or equal to 128 indicate that the binding registration was rejected by the local mobility anchor. Section 8.8 defines the Status values that can used in Proxy Binding Acknowledgement message.

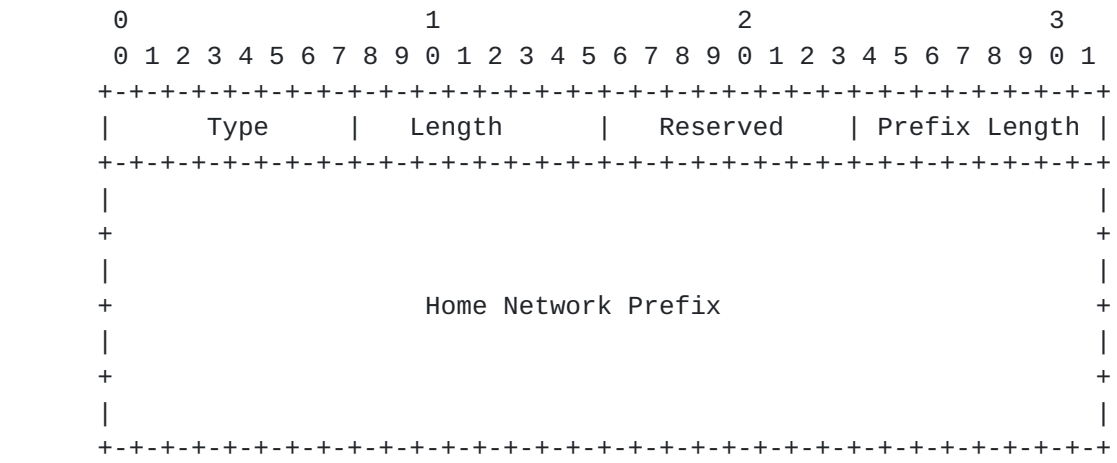
For descriptions of other fields present in this message, refer to the section 6.1.8 [RFC-3775].

8.3. Home Network Prefix Option

A new option, Home Network Prefix Option is defined for using it in the Proxy Binding Update and Proxy Binding Acknowledgement messages

exchanged between a local mobility anchor and a mobile access gateway. This option is 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 of the option in octets, excluding the type and length fields. This field MUST be set to 18.

Reserved (R)

This 8-bit 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.

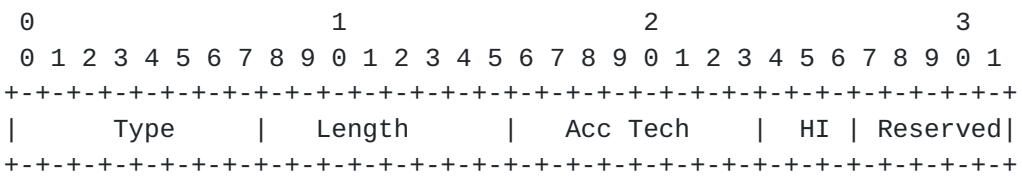
Home Network Prefix

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

8.4. Access Technology Type Option

A new option, Access Technology Type Option is defined for using it in the Proxy Binding Update and Proxy Binding Acknowledgement messages exchanged between a local mobility anchor and a mobile access gateway. This option is used for exchanging the type of the access technology using which the mobile node is currently attached to the mobile access gateway.

The Access Technology Type Option has no alignment requirement. Its format is as follows:



Type

<IANA>

Length

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

Access Technology Type (Acc Tech)

A 8-bit field that specifies the access technology through which the mobile node is connected to the access link on the mobile access gateway.

The values 0-255 will be allocated and managed by IANA. The following values are currently reserved for the below specified access technology types.

0x00: Reserved
0x01: Virtual
0x02: PPP
0x02: 802.3 (Ethernet)
0x03: 802.11a
0x04: 802.11b
0x05: 802.11g
0x06: 802.16e

0x07: CDMA2000 1xEV-DO Release 0
0x08: CDMA2000 1xEV-DO Revision A
0x09: CDMA2000 1xEV-DO Revision B
0x0a: 3GPP LTE

Handoff Indicator (HI)

A 3-bit field that specifies the type of handoff. The values (0-3) will be allocated and managed by IANA. The following values are currently reserved.

0: Reserved
1: Attachment over a new interface
2: Handoff between interfaces
3: Handoff between mobile access gateways for the same interface
4: Handoff state unknown

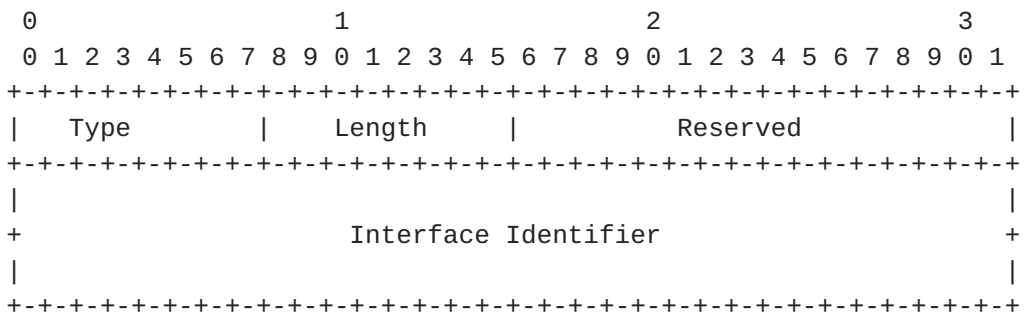
Reserved (R)

This 5-bit field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

8.5. Mobile Node Interface Identifier Option

A new option, Mobile Node Interface Identifier Option is defined for using it in the Proxy Binding Update and Proxy Binding Acknowledgement messages exchanged between a local mobility anchor and a mobile access gateway. This option is used for exchanging the mobile node's interface identifier.

The format of the Interface Identifier option when the interface identifier is 8 bytes is shown below. When the size is different, the option MUST be aligned appropriately, as per mobility option alignment requirements specified in [RFC-3775].



Type
<IANA>

Length
8-bit unsigned integer indicating the length of the option in octets, excluding the type and length fields. This field MUST be set to 10.

Reserved

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

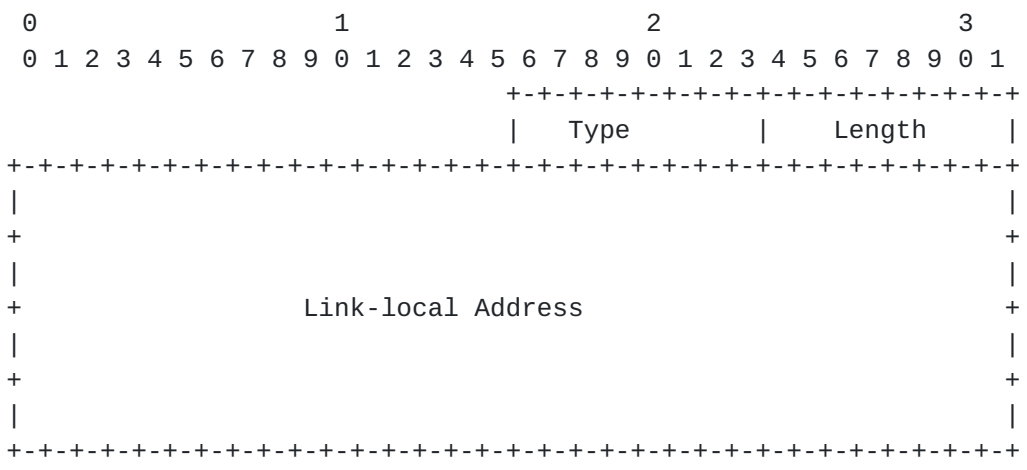
Interface Identifier

A variable length field containing the mobile node's interface identifier.

8.6. Link-local Address Option

A new option, Link-local Address Option is defined for using it in the Proxy Binding Update and Proxy Binding Acknowledgement messages exchanged between a local mobility anchor and a mobile access gateway. This option is used for exchanging the mobile node's link-local address.

The Link-local Address option has an alignment requirement of 8n+6. Its format is as follows:



Type
<IANA>

Length

8-bit unsigned integer indicating the length of the option in octets, excluding the type and length fields. This field MUST be set to 16.

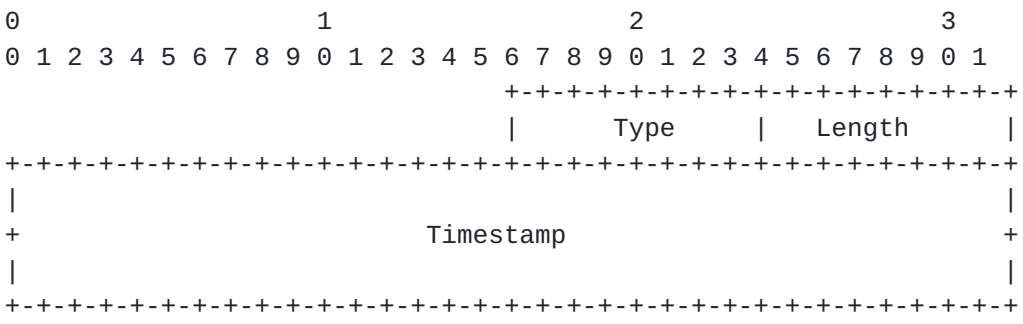
Link-local Address

A sixteen-byte field containing the mobile node's link-local address.

8.7. Timestamp Option

A new option, Timestamp Option is defined for use in the Proxy Binding Update and Proxy Binding Acknowledgement messages.

The Timestamp option has an alignment requirement of 8n+2. 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. The value for this field MUST be set to 8.

Timestamp

A 64-bit unsigned integer field containing a timestamp. The value indicates the number of seconds since January 1, 1970, 00:00 UTC, by using a fixed point format. In this format, the integer number of seconds is contained in the first 48 bits of the field, and the remaining 16 bits indicate the number of 1/65536 fractions of a second.

8.8. Status Values

This document defines the following new Status values for use in Proxy Binding Acknowledgement message. These values are to be allocated from the same number space, as defined in Section 6.1.8 [RFC-3775].

Status values less than 128 indicate that the Proxy Binding Update request was accepted by the local mobility anchor. Status values greater than 128 indicate that the Proxy Binding Update was rejected by the local mobility anchor.

PROXY_REG_NOT_ENABLED:

Proxy Registration not enabled for the mobile node.

MAG_NOT_AUTHORIZED_FOR_PROXY_REG:

The mobile access gateway is not authorized to send proxy binding. updates.

NOT_AUTHORIZED_FOR_HOME_NETWORK_PREFIX

The mobile node is not authorized for the requesting home network prefix.

TIMESTAMP_MISMATCH:

Invalid timestamp value in the received Proxy Binding Update message (the clocks are out of sync).

TIMESTAMP_LOWER_THAN_PREV_ACCEPTED:

The timestamp value in the received Proxy Binding Update message is lower than the previously accepted value.

MISSING_HOME_NETWORK_PREFIX_OPTION

Missing mobile node home network prefix option.

MISSING_MN_IDENTIFIER_OPTION:

Missing mobile node identifier in the Proxy Binding Update message.

MISSING_ACCESS_TECH_TYPE_OPTION

Missing mobile node's access technology type in the Proxy Binding Update message.

Additionally, the following Status values defined in [RFC-3775] can also be used in Proxy Binding Acknowledgement message.

0 Proxy Binding Update accepted

128 Reason unspecified

129 Administratively prohibited

130 Insufficient resources

133 Not local mobility anchor for this mobile node

9. Protocol Configuration Variables

The local mobility anchor MUST allow the following variables to be configured by the system management.

MinDelayBeforeBCEDelete

This variable specifies the amount of time in milliseconds the local mobility anchor MUST wait before it deletes a Binding Cache entry of a mobile node, upon receiving a Proxy Binding Update message from a mobile access gateway with a lifetime value of 0. During this wait time, if the local mobility anchor receives a Proxy Binding Update for the same mobility binding, with lifetime value greater than 0, then it must update the binding cache entry with the accepted binding values. By the end of this wait-time, if the local mobility anchor did not receive any valid Proxy Binding Update message for that mobility binding, it MUST delete the Binding Cache entry. This delay essentially ensures a mobile node's Binding Cache entry is not deleted too quickly and allows some time for the new mobile access gateway to complete the signaling for the mobile node.

The default value for this variable is 10000 milliseconds.

MinDelayBeforeNewBCEAssign

This variable specifies the amount of time in milliseconds the local mobility anchor MUST wait for the de-registration message for an existing mobility session before it decides to create a new mobility session.

The default value for this variable is 500 milliseconds.

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 correspondent node that is locally connected to one of the interfaces of the mobile access gateway. The correspondent 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.

MinPBUReplyTime

This variable specifies the amount of time in milliseconds the mobile access gateway SHOULD wait for the reply message for the Proxy Binding Update request that it sent to the local mobility anchor.

The default value for this variable is 2000 milliseconds.

10. IANA Considerations

This document defines five new Mobility Header Options, the Home Network Prefix option, Access Technology Type option, Interface Identifier option, Link-local Address option and Timestamp option. These options are described in Sections 8.3, 8.4, 8.5, 8.6 and 8.7 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].

The Mobility Header Option, Access Technology Type option defined in Section 8.4 of this document introduces a new Access Technology type numbering space, where the values from 0 to 5 have been reserved by this document. Approval of new Access Technology type numbers are to be made through IANA Expert Review.

This document also defines new Binding Acknowledgement status values as described in Section 8.8. The status values MUST be assigned from the same number space used for Binding Acknowledgement status values, as defined in [RFC-3775]. The allocated values for each of these status values MUST be greater than 128.

11. Security Considerations

The potential security threats against any network-based mobility management protocol are described in [RFC-4832]. This section explains how Proxy Mobile IPv6 protocol defends itself against those threats.

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

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

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

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

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 Alex Petrescu, Alice Qinxia, Alper Yegin, Ashutosh Dutta, Behcet Sarikaya, Fred Templin, Genadi Velev, George Tsirtsis, Gerardo Giaretta, Henrik Levkowetz, Hesham Soliman, James Kempf, Jari Arkko, Jean-Michel Combes, John Zhao, Jong-Hyouk Lee, Jonne Soininen, Jouni Korhonen, Kalin Getov, Kilian Weniger, Marco Liebsch, Mohamed Khalil, Nishida Katsutoshi, Phil Roberts, Ryuji Wakikawa, Sangjin Jeong, Suresh Krishnan, Ved Kafle, Vidya Narayanan, Youn-Hee Han 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-2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

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

13.2. Informative References

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

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

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

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

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

[RFC-4330] Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", RFC 2030, October 1996.

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

[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.

[RFC-4862] Thompson, S., Narten, T., Jinmei, T., "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC-4941] Narten, T., Draves, R., Krishnan, S., "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

[RFC-5072] Varada, S., Haskin, D. and Allen, E., "IP version 6 over PPP", RFC 5072, September 2007.

[ID-IPV4-PMIP6] Wakikawa, R. and Gundavelli, S., "IPv4 Support for Proxy Mobile IPv6", draft-ietf-netlmm-pmip6-ipv4-support-02.txt, November 2007.

[ID-DNAV6] Kempf, J., et al "Detecting Network Attachment in IPv6 Networks (DNAv6)", draft-ietf-dna-protocol-06.txt, October 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

This specification supports Per-MN-Prefix model. However, it is possible to support Shared-Prefix model under the following guidelines.

The mobile node is allowed to use stateful address configuration using DHCPv6 for obtaining its address configuration. The mobile node 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 [RFC-4861].

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).