

NETLMM WG
Internet-Draft
Intended status: Standards Track
Expires: November 17, 2008

S. Gundavelli (Editor)
K. Leung
Cisco
V. Devarapalli
Wichorus
K. Chowdhury
Starent Networks
B. Patil
Nokia Siemens Networks
May 16, 2008

Proxy Mobile IPv6
draft-ietf-netlmm-proxymip6-15.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on November 17, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

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	4
2.	Conventions & Terminology	4
2.1.	Conventions used in this document	5
2.2.	Terminology	5
3.	Proxy Mobile IPv6 Protocol Overview	9
4.	Proxy Mobile IPv6 Protocol Security	15
4.1.	Peer Authorization Database (PAD) Example Entries	16
4.2.	Security Policy Database (SPD) Example Entries	17
5.	Local Mobility Anchor Operation	17
5.1.	Extensions to Binding Cache Entry Data Structure	18
5.2.	Supported Home Network Prefix Models	19
5.3.	Signaling Considerations	20
5.3.1.	Processing Binding Registrations	20
5.3.2.	Initial Binding Registration (New Mobility Session)	22
5.3.3.	Binding Lifetime Extension (No handoff)	23
5.3.4.	Binding Lifetime Extension (After handoff)	24
5.3.5.	Binding De-Registration	24
5.3.6.	Constructing the Proxy Binding Acknowledgement Message	25
5.4.	Multihoming Support	27
5.4.1.	Binding Cache entry lookup considerations	28
5.5.	Timestamp Option for Message Ordering	33
5.6.	Routing Considerations	36
5.6.1.	Bi-Directional Tunnel Management	36
5.6.2.	Forwarding Considerations	37
5.7.	Local Mobility Anchor Address Discovery	38
5.8.	Mobile Prefix Discovery Considerations	39
5.9.	Route Optimization Considerations	39
6.	Mobile Access Gateway Operation	39
6.1.	Extensions to Binding Update List Entry Data Structure	40
6.2.	Mobile Node's Policy Profile	41
6.3.	Supported Access Link Types	42
6.4.	Supported Address Configuration Modes	42
6.5.	Access Authentication & Mobile Node Identification	43
6.6.	Acquiring Mobile Node's Identifier	43
6.7.	Home Network Emulation	44
6.8.	Link-Local and Global Address Uniqueness	45
6.9.	Signaling Considerations	46

6.9.1.	Binding Registrations	46
6.9.2.	Router Solicitation Messages	54
6.9.3.	Default-Router	55
6.9.4.	Retransmissions and Rate Limiting	56
6.9.5.	Path MTU Discovery	56
6.10.	Routing Considerations	57
6.10.1.	Transport Network	58
6.10.2.	Tunneling & Encapsulation Modes	58
6.10.3.	Local Routing	59
6.10.4.	Tunnel Management	59
6.10.5.	Forwarding Rules	59
6.11.	Supporting DHCPv6 based Address Configuration on the Access Link	61
6.12.	Home Network Prefix Renumbering	63
6.13.	Mobile Node Detachment Detection and Resource Cleanup	63
6.14.	Allowing network access to other IPv6 nodes	64
7.	Mobile Node Operation	64
7.1.	Moving into a Proxy Mobile IPv6 Domain	64
7.2.	Roaming in the Proxy Mobile IPv6 Domain	65
8.	Message Formats	66
8.1.	Proxy Binding Update Message	66
8.2.	Proxy Binding Acknowledgement Message	68
8.3.	Home Network Prefix Option	69
8.4.	Handoff Indicator Option	70
8.5.	Access Technology Type Option	71
8.6.	Mobile Node Link-layer Identifier Option	73
8.7.	Link-local Address Option	74
8.8.	Timestamp Option	75
8.9.	Status Values	75
9.	Protocol Configuration Variables	77
9.1.	Local Mobility Anchor - Configuration Variables	77
9.2.	Mobile Access Gateway - Configuration Variables	78
9.3.	Proxy Mobile IPv6 Domain - Configuration Variables	79
10.	IANA Considerations	79
11.	Security Considerations	80
12.	Acknowledgements	81
13.	References	81
13.1.	Normative References	82
13.2.	Informative References	82
Appendix A.	Proxy Mobile IPv6 interactions with AAA Infrastructure	84
Appendix B.	Routing State	84
	Authors' Addresses	85
	Intellectual Property and Copyright Statements	87

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 between a network node and a 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 nodes 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:

- o 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.
- o 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 set up 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 a Proxy Mobile IPv6 domain. It is the topological anchor point for the mobile node's home network prefix(es) and is the entity that manages the mobile node's binding state. The local mobility anchor has the functional capabilities of a home agent as defined in Mobile IPv6 base specification [[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 to and from 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 or router whose mobility is managed by the network. The mobile node may be an IPv4-only node, IPv6-only node or a dual-stack node and 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.

LMA Address (LMAA)

The global 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 global 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 Network Prefix (MN-HNP)

This is the prefix that is assigned to a given interface of a mobile node and is always present in the Router Advertisement messages that the mobile node receives on any of the access links in that Proxy Mobile IPv6 domain. There can also be multiple home network prefixes assigned to a given interface of a mobile node and in which case all of those assigned prefixes will still be managed as part of one mobility session. The mobile node configures its interface with one or more addresses from its home network prefix(es). If the mobile node connects to the Proxy Mobile IPv6 domain through multiple interfaces, simultaneously, each of the attached interfaces will be assigned a unique set of home network prefixes and all the prefixes assigned to a given

interface of a mobile node will be managed under one mobility session. Additionally, in some configurations the assigned prefix can be of 128-bit prefix length. Ex: Home network prefixes P1, P2 assigned to interface I1 will be managed under one mobility session and prefixes P3, P4, P5 assigned to interface I2 of the mobile node will be managed under a different mobility session.

Mobile Node's Home Address (MN-HoA)

MN-HoA is an address from a mobile node's home network prefix. The mobile node will be able to use this address as long as it is attached to the access network that is in the scope of that Proxy Mobile IPv6 domain. If the mobile node uses more than one address from its home network prefix(es), any one of these addresses is referred to as mobile node's home address. Unlike in Mobile IPv6 where the home agent is aware of the home address of the mobile node, in Proxy Mobile IPv6, the mobility entities are only aware of the mobile node's home network prefix(es) and are not always aware of the exact address(es) that the mobile node configured on its interface from its home network prefix(es). However, in some configurations and based on the enabled address configuration modes on the access link, the mobility entities in the network can be certain about the exact address(es) configured by the mobile node.

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 same 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 Network Access Identifier (NAI) [[RFC-4282](#)]

or other identifier such as a Media Access Control (MAC) address.

Mobile Node Link-layer Identifier (MN-LL-Identifier)

An identifier that identifies the attached interface of a mobile node. For those interfaces that have a link-layer identifier, this identifier can be based on that. The link-layer identifier in some cases is generated by the mobile node and conveyed to the mobile access gateway. This identifier of the attached interface must be stable as seen by any of the mobile access gateways in a given Proxy Mobile IPv6 domain. In some other cases, there might not be any link-layer 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 home network prefix(es) assigned to a given interface of a mobile node and its current care-of address (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.

Per-MN-Prefix & Shared-Prefix Models

The term, Per-MN-Prefix model, is used to refer to an addressing model where there is a unique network prefix assigned for each node. The term, Shared-Prefix model, is used to refer to an addressing model where the prefix is shared by more than one node. This specification supports the Per-MN-Prefix model and does not support the Shared-Prefix model.

ALL_ZERO & NON_ZERO

Protocol message fields initialized with value 0 in each byte of the field. Ex: An 8-byte link-layer identifier field with the value set to 0 in each of the 8 bytes, or an IPv6 address with the value 0 in all of the 16 bytes. Conversely, the term NON_ZERO is used to refer to any value other than an ALL_ZERO value.

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 set up 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(es). 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 to and from the access link and for initiating binding registrations to the mobile node's local mobility anchor. The architecture of a Proxy Mobile IPv6 domain is shown in Figure 1.

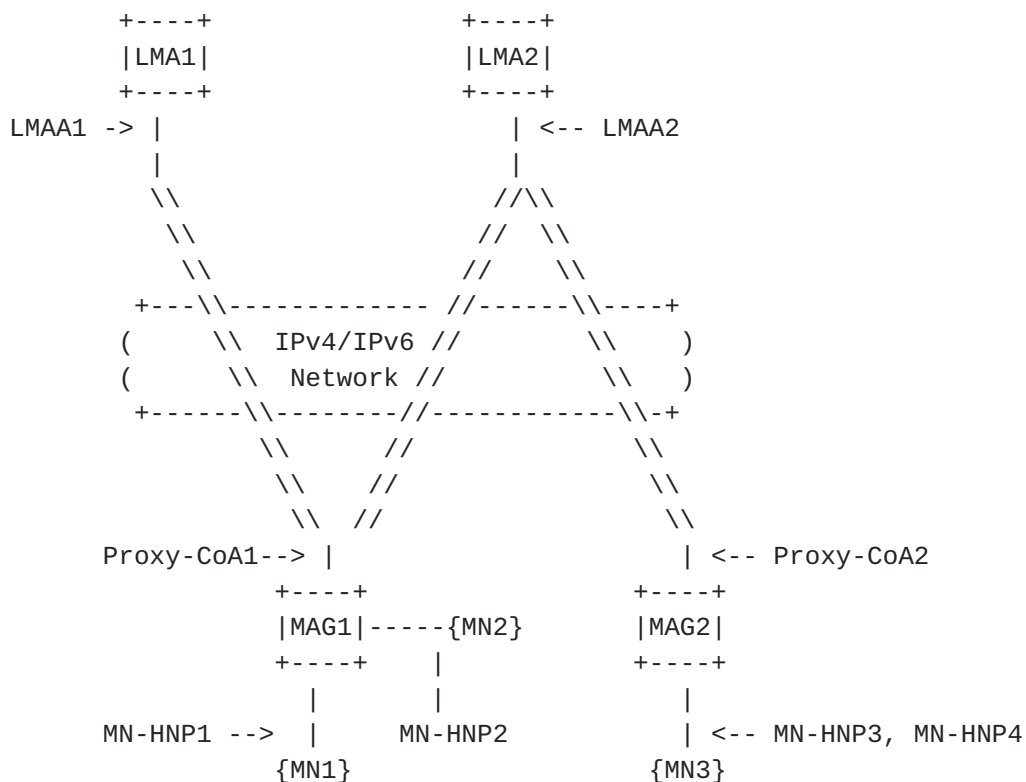


Figure 1: Proxy Mobile IPv6 Domain

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(es), 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 an IPv4-only node, IPv6-only node or a dual IPv4/IPv6 node. 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 this specification only supports IPv6 address mobility and when the transport network is IPv6 network. The support for IPv4 addressing or IPv4 transport network is specified in the companion document [[ID-IPV4-PMIPv6](#)].

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 set of home network prefixes for each of the connected interfaces. The mobile node will be able to configure address(es) on those interfaces from the respective home network prefix(es). However, if the mobile node performs an inter-interface handoff by moving its address configuration from one interface to the other and if the local mobility anchor receives a handoff hint from the serving mobile access gateway about the same, the local mobility anchor will assign the same home network prefix(es) that it previously assigned prior to the handoff. The mobile node will also be able to perform an handoff by changing its point of attachment from one mobile access gateway to a different mobile access gateway using the same interface and will be able to retain the address configuration on the attached interface.

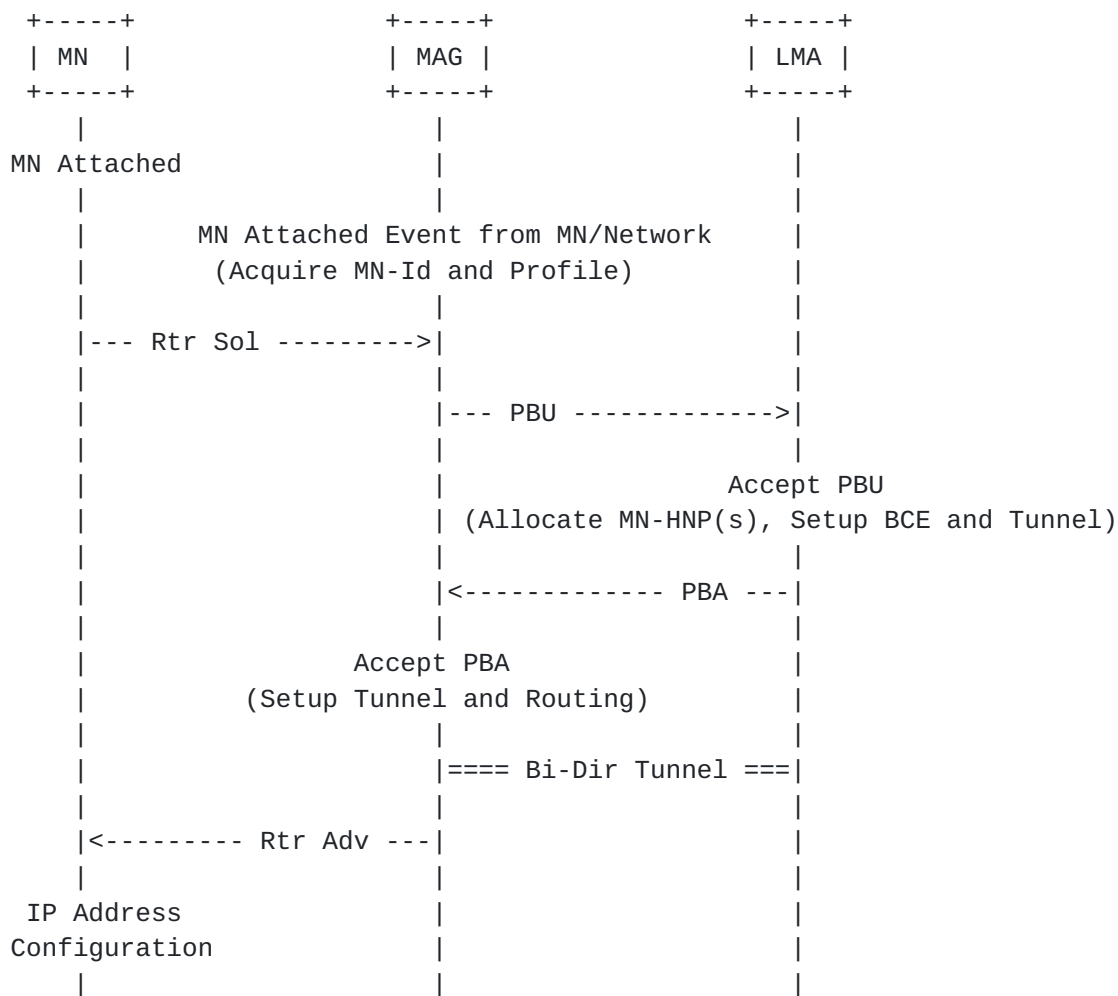


Figure 2: Mobile Node Attachment - Signaling Call Flow

Figure 2 shows the signaling call flow when the mobile node enters the Proxy Mobile IPv6 domain. The Router Solicitation message from the mobile node may arrive at any time after the mobile node's attachment and has no strict ordering relation with the other messages in the call flow.

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(es). It also creates the Binding Cache entry and sets up its endpoint of the bi-directional tunnel to

the mobile access gateway.

The mobile access gateway on receiving the Proxy Binding Acknowledgement message sets up its endpoint of the bi-directional tunnel to the local mobility anchor and also 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(es) as the hosted on-link-prefix(es).

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 one or more addresses from its home network prefixes(es).

Once the address configuration is complete, the mobile node has one or more valid addresses from its home network prefix(es) 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 any one or more of the addresses from its home network prefix(es).

The local mobility anchor, being the topological anchor point for the mobile node's home network prefix(es), receives any packets that are sent to the mobile node by any node in the network. 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. However, in some cases the traffic sent from a correspondent node that is locally connected to the mobile access gateway may not be received by the local mobility anchor and may be routed locally by the mobile access gateway.

The mobile access gateway acts as the 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. However in some cases the traffic sent to a correspondent node that is locally connected to the mobile access gateway may be locally routed by the mobile access gateway.

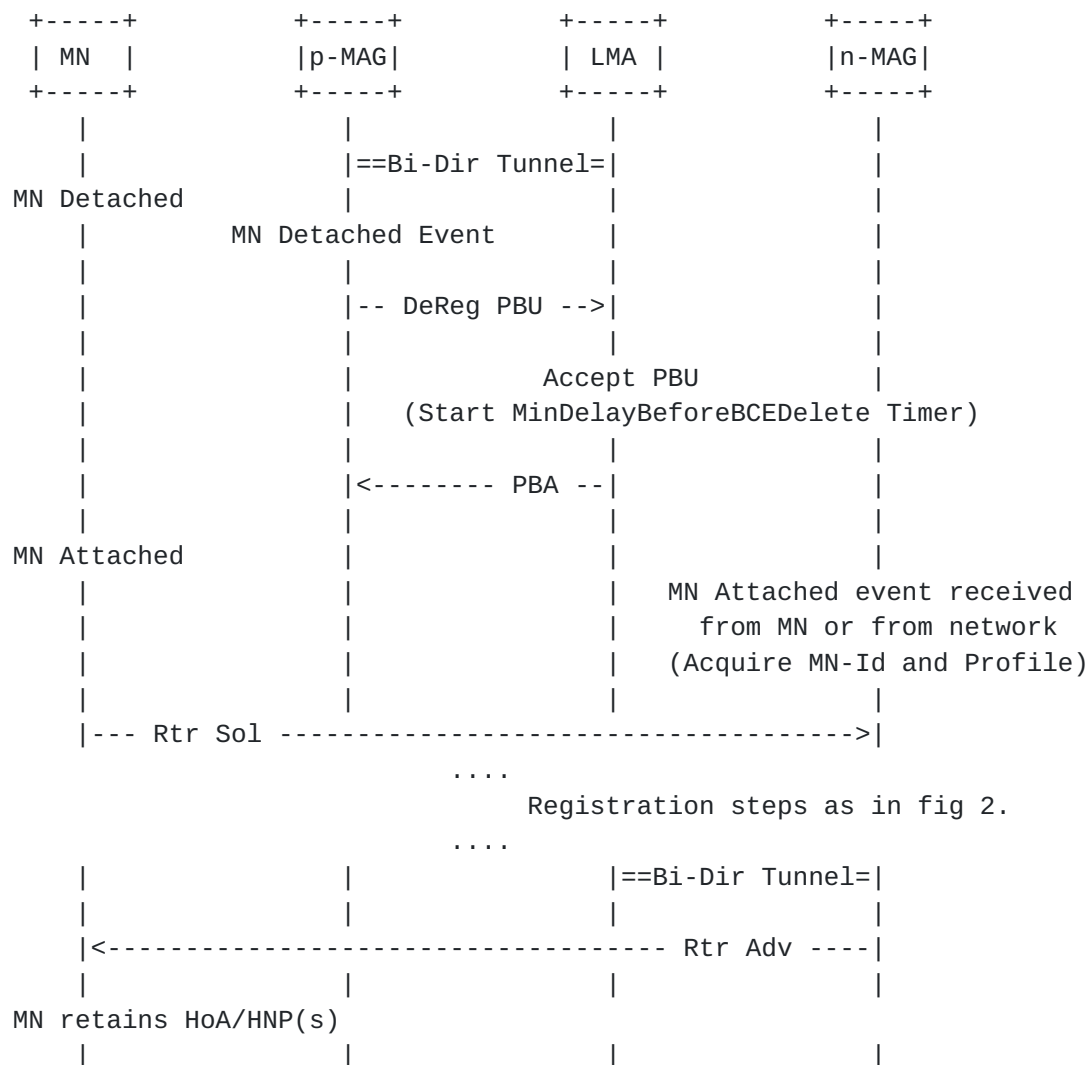


Figure 3: Mobile Node Handoff - Signaling Call Flow

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). This call flow reflects only a specific message ordering, it is possible the registration message from the n-MAG may arrive before the de-registration message from the p-MAG arrives.

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. The local mobility anchor upon receiving this request will identify the corresponding mobility session for which the binding update request was received and once it accepts the request will wait for certain amount of time for allowing the mobile access gateway on the new link to update the binding. However, if it does not receive any binding update request within that given amount of time, it will delete the binding cache entry.

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(es) that were assigned to that mobility session, making it believe it is still on the same link and it will be able to 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]. That is, IPsec is a mandatory to implement security mechanism. However, additional documents may specify alternative mechanisms and the mobility entities can enable a specific mechanism for securing Proxy Mobile IPv6 signaling messages, either based on a static configuration or after a dynamic negotiation using any standard security negotiation protocols. As in Mobile IPv6 [RFC-3775], the use of IPsec for protecting mobile node's data traffic is optional.

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.

IPsec ESP [RFC-4303] in tunnel mode MAY be used to protect the mobile node's tunneled data traffic, if protection of data traffic is required.

IKEv2 [RFC-4306] SHOULD be used to set up 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 [RFC-4306], 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 restrict the creation and manipulation of proxy bindings to specifically authorized mobile access gateways and prefixes. The local mobility anchor MUST be locally configurable to authorize such specific combinations. Additional mechanisms such as a policy store or AAA may be employed, but these are outside the scope of this specification.

Unlike in Mobile IPv6 [[RFC-3775](#)], these signaling messages do not carry either the Home Address destination option or the Type 2 Routing header and hence the policy entries and security association selectors stay the same and require no special IPsec related considerations.

[4.1.1.](#) Peer Authorization Database (PAD) Example 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_address_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 (SPD) Example 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 the Proxy Mobile IPv6 protocol is referred to as a 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 of \[RFC-3775\]](#).

For supporting this specification, the Binding Cache Entry data structure needs to be extended with the following additional fields.

- o A flag indicating whether or not this Binding Cache entry is created due to a proxy registration. This flag is set to value 1 for Binding Cache entries that are proxy registrations and is set to value 0 for all other entries.
- o 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.
- o The link-layer identifier of the mobile node's connected interface on the access link. This identifier can be acquired from the Mobile Node Link-layer Identifier option, present in the received Proxy Binding Update request. If the option was not present in the request, this variable length field MUST be set to two (octets) and MUST be initialized to a value of ALL_ZERO.
- o The link-local address of the mobile access gateway on the point-to-point link shared with the mobile node. This is generated by the local mobility anchor after accepting the initial Proxy Binding Update request.
- o List of IPv6 home network prefixes assigned to the mobile node's connected interface. The home network prefix(es) may have been statically configured in the mobile node's policy profile, or, they may have been dynamically allocated by the local mobility anchor. Each one of these prefix entries will also includes the corresponding prefix length.
- o The tunnel interface identifier (If-Id) of the bi-directional tunnel between the local mobility anchor and the mobile access gateway where the mobile node is currently anchored. This is internal to the local mobility anchor. The tunnel interface identifier is acquired during the tunnel creation.
- o The access technology type, using which the mobile node is currently attached. This is obtained from the Access Technology Type option, present in the Proxy Binding Update request.

- o The 64-bit timestamp value of the most recently accepted Proxy Binding Update request sent for this mobile node. This is the time-of-day on the local mobility anchor, when the message was received. If the Timestamp option is not present in the Proxy Binding Update request (i.e., when the sequence number based scheme is in use), the value MUST be set to ALL_ZERO.

Typically, any one of the mobile node's home network prefixes from its mobility session is the key for locating a Binding Cache entry in all cases except when there has been an handoff of the mobile node's session to a new mobile access gateway and that mobile access gateway is unaware of the home network prefix(es) assigned to that mobility session. In such handoff cases, the Binding Cache entry can be located under the considerations specified in [Section 5.4.1](#).

5.2. Supported Home Network Prefix Models

This specification supports the Per-MN-Prefix model and does not support the Shared-Prefix model. As per the Per-MN-Prefix model, a prefix assigned to a mobile node is for that mobile node's exclusive use and no other node shares an address from that prefix (other than the Subnet-Router anycast address [[RFC-4291](#)] which is used by the mobile access gateway hosting that prefix on that link).

There may be more than one prefix assigned to a given interface of the mobile node and all of those assigned prefixes are unique to that mobile node and all are part of one mobility session. If the mobile node attaches to the Proxy Mobile IPv6 domain through multiple interfaces and simultaneously, each of the attached interfaces will be assigned one or more unique prefixes and all of the assigned prefixes to a given interface will be managed under a different mobility session.

The mobile node's home network prefix(es) assigned to a given interface of a mobile node (part of a mobility session) will be hosted on the access link where the mobile node is attached (using that interface). The local mobility anchor is not required to perform any proxy ND operations [[RFC-4861](#)] for defending the mobile node's home address(es), as the prefixes are not locally hosted on the local mobility anchor. However, from the routing perspective, the home network prefix(es) 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.

5.3.1. Processing Binding Registrations

1. The received Proxy Binding Update message (a Binding Update message with the 'P' flag set to value of 1, format specified in [Section 8.1](#)) **MUST** be authenticated as described in [Section 4](#). 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 message.
2. The local mobility anchor **MUST** observe the rules described in [Section 9.2 of \[RFC-3775\]](#) when processing Mobility Header in the received Proxy Binding Update request.
3. The local mobility anchor **MUST** ignore the check, specified in [Section 10.3.1 of \[RFC-3775\]](#), related to the presence of Home Address destination option in the Proxy Binding Update request.
4. 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 option) and the identifier in the Mobile Node Identifier Option carried in the message **MUST** be set to a zero length identifier.
5. The local mobility anchor **MUST** apply the required policy checks, as explained in [Section 4](#), to verify the sender is a trusted mobile access gateway, authorized to send Proxy Binding Update requests on behalf of this mobile node.
6. If the local mobility anchor determines that the requesting node is not authorized to send Proxy Binding Update requests for the identified mobile node, 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 binding registrations).

7. If the local mobility anchor cannot identify the mobile node based on the identifier present in the Mobile Node Identifier option [[RFC-4283](#)] of Proxy Binding Update request, it MUST reject the request and send a Proxy Binding Acknowledgement message with Status field set to NOT_LMA_FOR_THIS_MOBILE_NODE (Not local mobility anchor for this mobile node).
8. 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).
9. The local mobility anchor MUST apply the considerations specified in [Section 5.5](#), for processing the Sequence Number field and the Timestamp option (if present), in the Proxy Binding Update request.
10. If there is no Home Network Prefix option(s) (with any value) 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 home network prefix option).
11. If the Handoff Indicator 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_HANDOFF_INDICATOR_OPTION (Missing handoff indicator option).
12. 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 access technology type option).
13. Considerations specified in [Section 5.4.1](#) MUST be applied for performing the Binding Cache entry existence test. If those checks specified in [Section 5.4.1](#), result in associating the received Proxy Binding Update request to a new mobility session creation request, considerations from [Section 5.3.2](#) (Initial Binding Registration - New Mobility Session), MUST be applied. If those checks result in associating the request to an existing

mobility session, the following checks determine the next set of processing rules that needs to be applied.

- * If the Handoff Indicator field in the Handoff Indicator option present in the request is set to a value of 5 (Handoff state not changed), considerations from [Section 5.3.3](#) (Binding Lifetime Extension- No handoff) MUST be applied.
 - * If the received Proxy Binding Update request has the lifetime value of zero, considerations from [Section 5.3.5](#) (Binding De-Registration) MUST be applied.
 - * For all other cases, considerations from [Section 5.3.4](#) (Binding Lifetime Extension - After handoff) MUST be applied.
14. When sending the Proxy Binding Acknowledgement message with any Status field value, the message MUST be constructed as specified in [Section 5.3.6](#).

[5.3.2](#). Initial Binding Registration (New Mobility Session)

1. If there is at least one instance of Home Network Prefix option present in the Proxy Binding Update request with the prefix value set to ALL_ZERO, the local mobility anchor MUST allocate one or more home network prefix(es) to the mobile node and assign it to the new mobility session created for the mobile node. The local mobility anchor MUST ensure the allocated prefix(es) is not in use by any other node or mobility session. The decision on how many prefixes to be allocated for the attached interface, can be based on a global policy or a policy specific to that mobile node. However, when stateful address autoconfiguration using DHCPv6 is supported on the link, considerations from [Section 6.11](#) MUST be applied for the prefix assignment.
2. If the local mobility anchor is unable to allocate any 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 there are one or more Home Network Prefix options present in the Proxy Binding Update request (with each of the prefixes set to a NON_ZERO value), the local mobility anchor before accepting that request, MUST ensure each one of those prefixes is owned by the local mobility anchor and further the mobile node is authorized to use these prefixes. If the mobile node is not authorized to use any one or more of those prefixes, 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 for one or more of the requesting home network prefixes).

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 registration.
5. If there is no existing bi-directional tunnel to the mobile access gateway that sent the request, the local mobility anchor MUST establish a bi-directional tunnel to that mobile access gateway. Considerations from [Section 5.6.1](#) MUST be applied for managing the dynamically created bi-directional tunnel.
6. The local mobility anchor MUST create a prefix route(s) over the tunnel to the mobile access gateway for forwarding any traffic received for the mobile node's home network prefix(es) associated with this mobility session. The created tunnel and the routing state MUST result in the forwarding behavior on the local mobility anchor as specified in [Section 5.6.2](#).
7. The local mobility anchor MUST send the Proxy Binding Acknowledgement message with the Status field set to 0 (Proxy Binding Update Accepted). The message MUST be constructed as specified in [Section 5.3.6](#).

[5.3.3](#). Binding Lifetime Extension (No handoff)

1. Upon accepting the Proxy Binding Update request for extending the binding lifetime, received from the same mobile access gateway (if the Proxy-CoA address in the Binding Cache entry is the same as the Proxy-CoA address in the request) that last updated the binding, the local mobility anchor MUST update the Binding Cache entry with the accepted registration values.
2. The local mobility anchor MUST send the Proxy Binding Acknowledgement message with the Status field set to 0 (Proxy Binding Update Accepted). The message MUST be constructed as specified in [Section 5.3.6](#).

5.3.4. Binding Lifetime Extension (After handoff)

1. Upon accepting the Proxy Binding Update request for extending the binding lifetime, received from a new mobile access gateway (if the Proxy-CoA address in the Binding Cache entry does not match the Proxy-CoA address in the request) where the mobile node's session is handed off, the local mobility anchor MUST update the Binding Cache entry with the accepted registration values.
2. The local mobility anchor MUST remove the previously created route(s) for the mobile node's home network prefix(es) associated with this mobility session. Additionally, if there are no other mobile node sessions sharing the dynamically created bi-directional tunnel to the previous mobile access gateway, the tunnel SHOULD be deleted applying considerations from [section 5.6.1](#) (if the tunnel is a dynamically created tunnel and not a fixed pre-established tunnel).
3. If there is no existing bi-directional tunnel to the mobile access gateway that sent the request, the local mobility anchor MUST establish a bi-directional tunnel to that mobile access gateway. Considerations from [Section 5.6.1](#) MUST be applied for managing the dynamically created bi-directional tunnel.
4. The local mobility anchor MUST create prefix route(s) over the tunnel to the mobile access gateway for forwarding any traffic received for the mobile node's home network prefix(es) associated with that mobility session. The created tunnel and routing state MUST result in the forwarding behavior on the local mobility anchor as specified in [Section 5.6.2](#).
5. The local mobility anchor MUST send the Proxy Binding Acknowledgement message with the Status field set to 0 (Proxy Binding Update Accepted). The message MUST be constructed as specified in [Section 5.3.6](#).

5.3.5. Binding De-Registration

1. If the received Proxy Binding Update request with the lifetime value of zero, has a Source Address in the IPv6 header (or the address in the Alternate Care-of Address option, if the option is present) different from what is present in the Proxy-CoA address field in the Binding Cache entry, the local mobility anchor MUST ignore the request.
2. Upon accepting the Proxy Binding Update request with the lifetime value of zero, the local mobility anchor MUST wait for

MinDelayBeforeBCEDelete amount of time, before it deletes the Binding Cache entry. However, it MUST send the Proxy Binding Acknowledgement message with the Status field set to 0 (Proxy Binding Update Accepted). The message MUST be constructed as specified in [Section 5.3.6](#).

- * During this wait period, the local mobility anchor SHOULD drop the mobile node's data traffic.
- * During this wait period, if the local mobility anchor receives a valid Proxy Binding Update request for the same mobility session 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 and additionally the wait period should be ended.
- * By the end of this wait period, if the local mobility anchor did not receive any valid Proxy Binding Update request for this mobility session, then it MUST delete the Binding Cache entry and remove the routing state created for that mobility session.

5.3.6. 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 must be set to value of 1 */
  Mobility Options
    - Mobile Node Identifier Option          (mandatory)
    - Home Network Prefix option(s)         (mandatory)
    - Handoff Indicator option               (mandatory)
    - Access Technology Type option          (mandatory)
    - Timestamp Option                       (optional)
    - Mobile Node Link-layer Identifier option (optional)
    - Link-local Address option              (optional)
```

Figure 6: Proxy Binding Acknowledgement message format

- o 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.
- o 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. When there is no Alternate Care-of Address option present in the request, the destination address is the same as the Proxy-CoA address, otherwise, the address may not be the same as the Proxy-CoA.
- o The Mobile Node Identifier option [[RFC-4283](#)] MUST be present. The identifier field in the option MUST be copied from the Mobile Node Identifier option in the received Proxy Binding Update request. If the option was not present in the request, the identifier in the option MUST be set to a zero length identifier.
- o At least one Home Network Prefix option MUST be present.
 - * If the Status field is set to a value greater than or equal to 128, i.e., if the binding request is rejected, all the Home Network Prefix options that were present in the request (along with their prefix values) MUST be present in the reply. But, if there was no Home Network Prefix option present in the request, then there MUST be only one Home Network Prefix option and with the value in the option set to ALL_ZERO.
 - * For all other cases, there MUST be a Home Network Prefix option for each of the assigned home network prefixes (for that mobility session) and with the prefix value in the option set to the allocated prefix value.
- o The Handoff Indicator option MUST be present. The handoff indicator field in the option MUST be copied from the Handoff Indicator option in the received Proxy Binding Update request. If the option was not present in the request, the value in the option MUST be set to zero.
- o The Access Technology Type option MUST be present. The access technology type field 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, the value in the option MUST be set to zero.
- o The Timestamp option MUST be present only if the same option was present in the received Proxy Binding Update request and MUST NOT be present otherwise. Considerations from [Section 5.5](#) must be applied for constructing the Timestamp option.

- o The Mobile Node Link-layer Identifier option MUST be present only if the same option was present in the received Proxy Binding Update request and MUST NOT be present otherwise. The link-layer identifier value MUST be copied from the Mobile Node Link-layer Identifier option present in the received Proxy Binding Update request.
- o The Link-local Address option MUST be present only if the same option was present in the received Proxy Binding Update request and MUST NOT be present otherwise.
 - * If the received Proxy Binding Update request has the Link-local Address option with any value other than ALL_ZERO, the same value MUST be copied to the Link-local Address field of the Binding Cache entry and it must also be copied to the Link-local Address option in the reply.
 - * If there is no existing Binding Cache entry (i.e., if this is a request for a new mobility session), then the local mobility anchor MUST generate the link-local address that the mobile access gateway can use on the point-to-point link shared with the mobile node and the same must be copied to the Link-local Address field of the Binding Cache entry and it must also be copied to the Link-local Address option in the reply.
 - * For all other cases, the link-local address in the option MUST be copied from the Link-local Address field of the Binding Cache entry.
- o 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.
- o Unlike in Mobile IPv6 [[RFC-3775](#)], the Type 2 Routing header MUST NOT be present in the IPv6 header of the packet.

5.4. Multihoming Support

This specification allows mobile nodes to connect to a Proxy Mobile IPv6 domain through multiple interfaces for simultaneous access. Following are the key aspects of this multihoming support.

- o When a mobile node connects to a Proxy Mobile IPv6 domain through multiple interfaces for simultaneous access, the local mobility anchor MUST allocate a mobility session for each of the attached interfaces. Each of the mobility session should be managed under a separate Binding Cache entry and with its own lifetime.

- o The local mobility anchor MAY allocate more than one home network prefix for a given interface of the mobile node. However, all the prefixes associated with a given interface MUST be managed as part of one mobility session, associated with that interface.
- o The local mobility anchor MUST allow for an handoff between two different interfaces of a mobile node. In such a scenario, all the home network prefix(es) associated with one interface (part of one mobility session) will be associated with a different interface of the mobile node). 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 Proxy Binding Update message and under the considerations specified in this section.

5.4.1. Binding Cache entry lookup considerations

There can be multiple Binding Cache entries for a given mobile node. When doing a lookup for a mobile node's Binding Cache entry for processing a received Proxy Binding Update request message, the local mobility anchor MUST apply the following multihoming considerations (in the below specified order, starting with [Section 5.4.1.1](#)). These rules are chained with the processing rules specified in [Section 5.3](#).

5.4.1.1. Home Network Prefix Option (NON_ZERO Value) present in the request

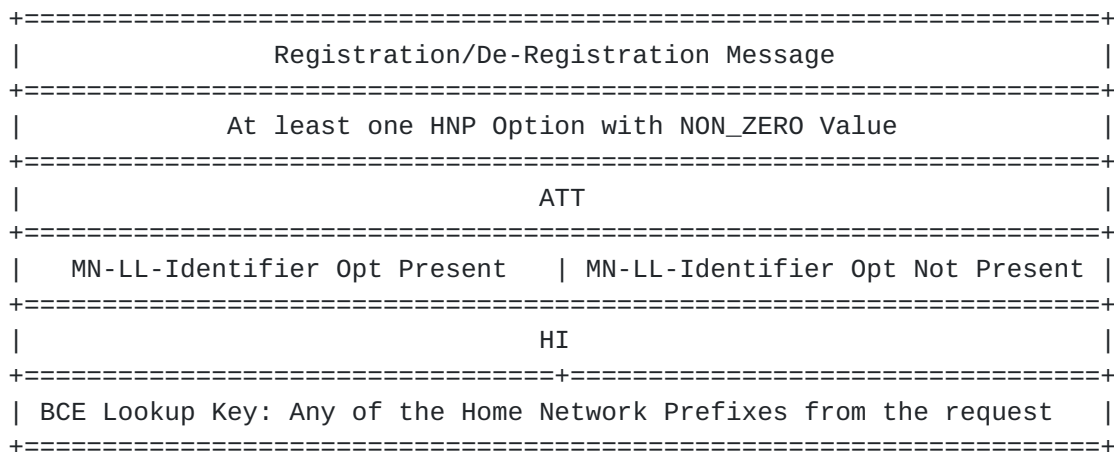


Figure 7: BCE lookup using home network prefix

If there is at least one Home Network Prefix option present in the

request with NON_ZERO prefix value, the following considerations MUST be applied. If there are more than one instances of the Home Network Prefix option, any one of the Home Network Prefix options present in the request (with NON_ZERO prefix value) can be used for locating the Binding Cache entry.

1. The local mobility anchor MUST verify if there is an existing Binding Cache entry with one of its home network prefixes matching the prefix value in one of the Home Network Prefix options of the received Proxy Binding Update request. [BCE(HNP) equals PBU(HNP)]
2. If there does not exist a Binding Cache entry (with one of its home network prefixes in the Binding Cache entry matching the prefix value in one of the Home Network Prefix options of the received Proxy Binding Update request), the request MUST be considered as a request for creating a new mobility session. [BCE(HNP) not equals PBU(HNP)]
3. If there exists a Binding Cache entry (with one of its home network prefixes in the Binding Cache entry matching the prefix value in one of the Home Network Prefix options of the received Proxy Binding Update request) but if the mobile node identifier in the entry does not match the mobile node identifier in the Mobile Node Identifier option of the received Proxy Binding Update request, the local mobility anchor MUST reject the request with the Status field value set to NOT_AUTHORIZED_FOR_HOME_NETWORK_PREFIX (mobile node is not authorized for one or more of the requesting home network prefixes). [BCE(MN-Identifier) not equals PBU(MN-Identifier)]
4. If there exists a Binding Cache entry (matching MN-Identifier and one of its home network prefixes in the Binding Cache entry matching the prefix value in one of the Home Network Prefix options of the received Proxy Binding Update request), but if all the prefixes in the request do not match all the prefixes in the Binding Cache entry, or if they do not match in count, then the local mobility anchor MUST reject the request with the Status field value set to BCE_PBU_PREFIX_SET_DO_NOT_MATCH (all the home network prefixes listed in the BCE do not match all the prefixes in the received PBU). [BCE(HNP1, HNP2, .. HNPn) not equals PBU(HNP1, HNP2, ..HNPn)] OR [BCE(Count(HNP))] not equals PBU(Count(HNP))]
5. If there exists a Binding Cache entry (matching MN-Identifier and all the home network prefixes in the Binding Cache entry matching all the home network prefixes in the received Proxy Binding Update request) and if any one or more of these below stated

conditions match, the request MUST be considered as a request for updating that Binding Cache entry. [BCE(MN-Identifier) equals PBU(MN-Identifier)] AND [BCE(HNP1, HNP2, .. HNPN) equals PBU(HNP1, HNP2, ..HNPN)]

- * If the Handoff Indicator field in the Handoff Indicator option present in the request is set to a value of 2 (Handoff between two different interfaces of the mobile node). [PBU(HI) equals 2]
- * If there is no Mobile Node Link-layer Identifier option present in the request, the link-layer identifier value in the Binding Cache entry is set to ALL_ZERO, the access technology type field in the Access Technology Type option present in the request matches the access technology type in the Binding Cache entry and if the Handoff Indicator field in the Handoff Indicator option present in the request is set to a value of 3 (Handoff between mobile access gateways for the same interface).
- * If the Proxy-CoA address in the Binding Cache entry matches the source address of the request (or the address in the alternate Care-of Address option, if the option is present) and if the access technology type field in the Access Technology Type option present in the request matches the access technology type in the Binding Cache entry. [BCE(Proxy-CoA, ATT) equals PBU(Proxy-CoA, ATT)].

6. For all other cases, the message MUST be considered as a request for creating a new mobility session.

5.4.1.2. Mobile Node Link-layer Identifier Option present in the request

```

+=====+
|           Registration/De-Registration Message           |
+=====+
|           HNP option with ALL_ZERO Value                 |
+=====+
|                               ATT                          |
+=====+
| MN-LL-Identifier Option Present (NON_ZERO Value)         |
+=====+
|                               HI                           |
+=====+
| BCE Lookup Keys: (MN-Identifier + ATT + MN-LL-Identifier) |

```


+=====+

Figure 8: BCE Lookup using Link-layer Identifier

1. The local mobility anchor MUST verify if there is an existing Binding Cache entry, with the mobile node identifier matching the identifier in the received Mobile Node Identifier option, access technology type matching the value in the received Access Technology Type option and the link-layer identifier value matching the identifier in the received Mobile Node Link-layer Identifier option. [BCE(MN-Identifier, ATT, MN-LL-Identifier) equals PBU(MN-Identifier, ATT, MN-LL-Identifier)]
2. If there exists a Binding Cache entry (matching MN-Identifier, ATT and MN-LL-Identifier), the request MUST be considered as a request for updating that Binding Cache entry.
3. If there does not exist a Binding Cache entry (matching MN-Identifier, ATT and MN-LL-Identifier) and the Handoff Indicator field in the Handoff Indicator option present in the request is set to a value of 2 (Handoff between two different interfaces of the mobile node). The local mobility anchor MUST apply the following additional considerations. [PBU(HI) equals 2]
 - * The local mobility anchor MUST verify if there exists one and only one Binding Cache entry with the mobile node identifier matching the identifier in the Mobile Node Identifier option present in the request and for any link-layer identifier value. If there exists only one such entry (matching the MN-Identifier), the request MUST be considered as a request for updating that Binding Cache entry. [BCE(MN-Identifier) equals PBU(MN-Identifier)]
4. If there does not exist a Binding Cache entry (matching MN-Identifier, ATT and MN-LL-Identifier) and if the Handoff Indicator field in the Handoff Indicator option present in the request is set to a value of 4 (Handoff state unknown), the local mobility anchor MUST apply the following additional considerations.
 - * The local mobility anchor MUST verify if there exists one and only one Binding Cache entry with the mobile node identifier matching the identifier in the Mobile Node Identifier option present in the request and for any link-layer identifier value. If there exists only one such entry (matching the MN-Identifier), the local mobility anchor SHOULD wait till the

existing Binding Cache entry is de-registered by the previously serving mobile access gateway, before the request can be considered as a request for updating that Binding Cache entry. However, if there is no de-registration message that is received within MaxDelayBeforeNewBCEAssign amount of time, the local mobility anchor upon accepting the request MUST consider the request as a request for creating a new mobility session. The local mobility anchor MAY also choose to create a new mobility session and without waiting for a de-registration message and this should be configurable on the local mobility anchor.

5. For all other cases, the message MUST be considered as a request for creating a new mobility session.

5.4.1.3. Mobile Node Link-layer Identifier Option not present in the request

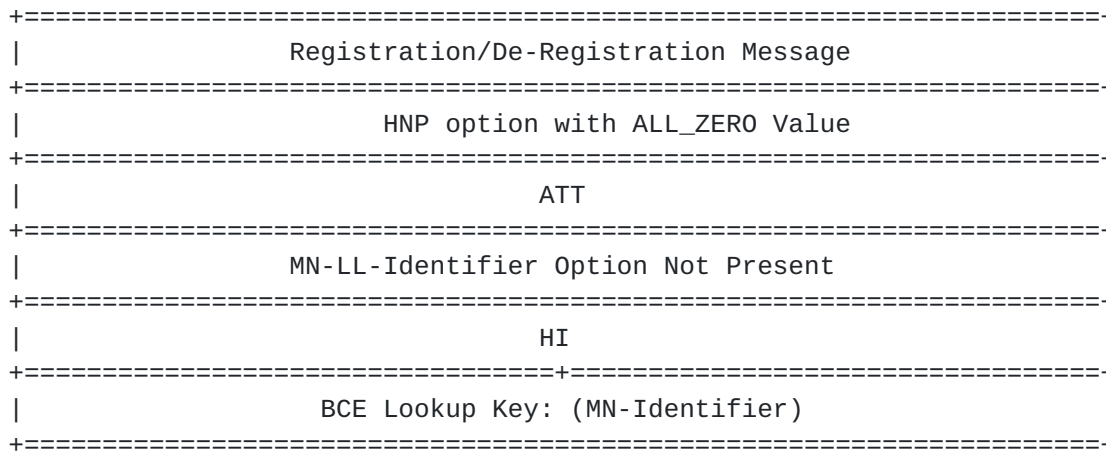


Figure 9: BCE Lookup using Mobile Node Identifier

1. The local mobility anchor MUST verify if there exists one and only one Binding Cache entry with the mobile node identifier matching the identifier in the Mobile Node Identifier option present in the request.
2. If there exists only one such entry (matching the MN-Identifier) and the Handoff Indicator field in the Handoff Indicator option present in the request is set to a value of 2 (Handoff between two different interfaces of the mobile node) or set to a value of

- 3 (Handoff between mobile access gateways for the same interface), then the request MUST be considered as a request for updating that Binding Cache entry. [PBU(HI) equals 2] or [PBU(HI) equals 3]
3. If there exists only one such entry (matching the MN-Identifier) and the Handoff Indicator field in the Handoff Indicator option present in the request is set to a value of 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 the request can be considered as a request for updating that Binding Cache entry. However, if there is no de-registration message that is received within MaxDelayBeforeNewBCEAssign amount of time, the local mobility anchor upon accepting the request MUST consider the request as a request for creating a new mobility session. The local mobility anchor MAY also choose to create a new mobility session and without waiting for a de-registration message and this should be configurable on the local mobility anchor.
 4. For all other cases, the message MUST be considered as a request for creating a new mobility session.

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, but delivered out of order, resulting in incorrectly updating the mobile node's Binding Cache entry and creating a routing state for tunneling the mobile node's traffic to the previously serving gateway.

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.

If the mechanism used for clock synchronization in the Proxy Mobile IPv6 domain cannot assure a clock drift between the two mobile access gateways (between which the mobile node did a handoff), which is not less than half the total time it took for the mobile node to roam between the two mobile access gateways and the time it took for the serving mobile access gateway to detect the node on its access link and construct the Proxy Binding Update message, then this solution will not predictably work in all cases and hence SHOULD NOT be used.

As an alternative to the Timestamp based approach, the specification also allows the use of Sequence Number based scheme, as specified in [[RFC-3775](#)]. However, for this scheme to work, the serving mobile access gateway in a Proxy Mobile IPv6 domain MUST have the ability to obtain the last sequence number that was sent in a binding registration message. The sequence number MUST be maintained on a per mobile node basis and MUST be available to the serving mobile access gateway. 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 made available to the serving mobile access gateway prior to sending the binding registration messages is outside the scope of this document."

Using the Timestamps based approach:

1. A local mobility anchor implementation MUST support the 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 the 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 8.8](#)).
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 (within TimestampValidityWindow amount of time difference) 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. However, if the flag MobileNodeGeneratedTimestampInUse is set to value of 1, this check MUST NOT be performed.
7. If the timestamp value in the received Proxy Binding Update is valid (validity as specified in the above considerations) or if the flag MobileNodeGeneratedTimestampInUse is set to value of 1, 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 the Sequence Number based approach:

1. If the Timestamp option is not present in the received Proxy Binding Update request, the local mobility anchor MUST fall back 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 the Sequence Number based scheme, as specified in [[RFC-3775](#)].
3. The Sequence Number based approach can be used only when there is some mechanism (such as context transfer procedure between mobile access gateways) that allows the serving mobile access gateway to obtain the last sequence number that was sent in a binding registration message for updating a given mobile node's binding.

[5.6.](#) Routing Considerations

[5.6.1.](#) Bi-Directional Tunnel Management

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. A tunnel hides the topology and enables a mobile node to use address(es) from its home network prefix(es) from any access link in that Proxy Mobile IPv6 domain. A tunnel may be created dynamically when needed and removed when not needed. However, implementations

MAY choose to use static pre-established tunnels instead of dynamically creating and tearing them down on a need basis. The following considerations MUST be applied when using dynamic tunnels.

- o A bi-directional tunnel MUST be established between the local mobility anchor and the mobile access gateway with IPv6-in-IPv6 encapsulation, as described in [[RFC-2473](#)]. The tunnel end points are the Proxy-CoA and LMAA. When using IPv4 transport, the end points of the tunnel are the IPv4-LMAA and IPv4-Proxy-CoA, as specified in [[ID-IPv4-PMIPv6](#)].
- o 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 can be set to the accepted binding lifetime and can 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.
- o The tunnel SHOULD be deleted when either the tunnel lifetime expires or when there are no mobile nodes sharing the tunnel.

5.6.2. Forwarding Considerations

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

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

Forwarding Packets to the Mobile Node:

- o On receiving a packet from a correspondent node with the destination address matching a mobile node's home network prefix(es), the local mobility anchor MUST forward the packet through the bi-directional tunnel set up for that mobile node.
- o The format of the tunneled packet is shown below. Considerations from [[RFC-2473](#)] MUST be applied for IPv6 encapsulation. 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 10: Tunnelled Packet from LMA to MAG

- o The format of the tunnelled packet is shown below, when payload protection using IPsec is enabled for the mobile node's data traffic. 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 */
  ESP Header in tunnel mode             /* ESP Header */
    IPv6 header (src= CN, dst= MN-HoA ) /* Packet Header */
      Upper layer protocols             /* Packet Content*/

```

Figure 11: Tunnelled Packet from LMA to MAG with Payload Protection

Forwarding Packets Sent by the Mobile Node:

- o All the reverse tunnelled packets that the local mobility anchor received 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. Considerations from [[RFC-2473](#)] MUST be applied for IPv6 decapsulation.

5.7. Local Mobility Anchor Address Discovery

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

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(es), as the prefix(es) 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

This specification does not support mobile prefix discovery. The mobile prefix discovery mechanism as specified in [\[RFC-3775\]](#) is not applicable to Proxy Mobile IPv6.

5.9. Route Optimization 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 address(es) from its home network prefix(es) 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 [\[RFC-3775\]](#) 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 to and from the 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:

- o 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.
- o Emulation of the mobile node's home link on the access link by sending Router Advertisement messages containing the mobile node's home network prefix(es), each prefix carried using the Prefix Information option [[RFC-4861](#)].
- o Responsible for setting up the data path for enabling the mobile node to configure one or more addresses from its home network prefix(es) and use it from the attached 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 of \[RFC-3775\]](#).

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

- o 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.
- o The link-layer identifier of the mobile node's connected interface. This 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 link-layer identifier conveyed by the mobile node; however, the specific details on how that is conveyed is out of scope for this specification. If this identifier is not available, this variable length field MUST be set to two (octets) and MUST be initialized to a value of ALL_ZERO.
- o List of IPv6 home network prefixes assigned to the mobile node's connected interface. The home network prefix(es) may have been

statically configured in the mobile node's policy profile, or, may have been dynamically allocated by the local mobility anchor. Each of these prefix entries will also includes the corresponding prefix length.

- o The Link-local address of the mobile access gateway on the access link shared with the mobile node.
- o 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.
- o The interface identifier (If-Id) of the point-to-point link between the mobile node and the mobile access gateway. This is internal to the mobile access gateway and is used to associate the Proxy Mobile IPv6 tunnel to the access link where the mobile node is attached.
- o The tunnel 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:

- o The mobile node's identifier (MN-Identifier)
- o The IPv6 address of the local mobility anchor (LMAA)

The following are the optional fields of the policy profile:

- o The mobile node's IPv6 home network prefix(es) assigned to the mobile node's connected interface
- o The mobile node's IPv6 home network Prefix lifetime. This lifetime will be same for all the hosted prefixes on the link, as they all are part of one mobility session.
- o Supported address configuration procedures (Stateful, Stateless or both) for the mobile node 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 emulates point-to-point delivery between the mobile node and the mobile access gateway for all the protocol traffic.

It is also necessary to be able to identify mobile nodes attaching to the link. Requirements relating to this are covered in [Section 6.6](#).

Finally, while this specification can operate without link layer indications of node attachment and detachment to the link, the existence of such indications either on the network or mobile node side improves the resulting performance.

6.4. Supported Address Configuration Modes

A mobile node in the Proxy Mobile IPv6 domain can configure one or more global IPv6 addresses on its interface (using Stateless, Stateful or manual address autoconfiguration procedures) from the hosted prefix(es) on that link. 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 access link, the mobile node can generate one or more IPv6 addresses from the hosted prefix(es) by standard IPv6 mechanisms such as Stateless

Autoconfiguration [[RFC-4862](#)] or Privacy extensions [[RFC-4941](#)].

When stateful address autoconfiguration is supported on the link, the mobile node can obtain the address configuration from the DHCPv6 server located in the Proxy Mobile IPv6 domain, by standard DHCPv6 mechanisms, as specified in [[RFC-3315](#)]. The obtained address(es) will be from its home network prefix(es). [Section 6.11](#) specifies the details on how this configuration can be achieved.

Additionally, other address configuration mechanisms specific to the access link between the mobile node and the mobile access gateway may also be used for delivering the address configuration to the mobile node. This specification does not modify the behavior of any of the standard IPv6 address configuration mechanisms.

[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 the 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 and unique across the Proxy Mobile IPv6 domain. The mobility entities in the Proxy Mobile IPv6 domain MUST be able to use this identifier in the signaling messages and unambiguously identify a given mobile node. Following are some of the considerations related to this MN-Identifier.

- o The MN-Identifier is typically obtained as part of the access authentication or from a notified network attachment event. In cases where the user identifier authenticated during access authentication uniquely identifies a mobile node, the MN-Identifier MAY be the same as the user identifier. However, the user identifier MUST NOT be used if it identifies a user account that can be used from more than one mobile node operating in the same Proxy Mobile IPv6 domain.

- o In some cases, the obtained identifier as part of the access authentication can be a temporary identifier and further that temporary identifier may be different at each re-authentication. However, the mobile access gateway MUST be able to use this temporary identifier and obtain the mobile node's stable identifier from the policy store. For instance, in AAA-based systems the RADIUS attribute, Chargeable-User-Identifier [RFC-4372] may be used, as long as it uniquely identifies a mobile node, and not a user account that can be used with multiple mobile nodes.
- o In some cases and for privacy reasons, 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.
- o The mobile access gateway MUST be able to identify the mobile node by its MN-Identifier and it MUST be able to associate this identity to the point-to-point link shared with the mobile node.

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 Advertisement messages advertising the mobile node's home network prefix(es) carried using the Prefix Information option(s) [[RFC-4861](#)] and with 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(es) details from the received Proxy Binding Acknowledgement message or it may obtain them 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(es) only after successfully completing the binding registration with the mobile node's local mobility anchor.

When advertising the home network prefix(es) in the Router Advertisement messages, the mobile access gateway MAY set the prefix

lifetime value for the advertised prefix(es) 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 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 address(es). 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 its existing addresses, which may potentially lead to address collisions after the mobile node's handoff to a new link.

The issue of address collision is not relevant to the mobile node's global address(es). Since the assigned home network prefix(es) are for the mobile node's exclusive usage, no other node shares an address (other than Subnet-Router anycast address which is configured by the mobile access gateway) from the prefix(es) and so the uniqueness for the mobile node's global address is assured on the access link.

The issue of address collision is however relevant to the mobile node's link-local addresses since the mobile access gateway and the mobile node will have link-local addresses configured from the same link-local prefix (FE80::/64). This leaves a room for link-local address collision between the two neighbors (i.e., the mobile node and the mobile access gateway) on that access link. For solving this problem, this specification requires that the link-local address that the mobile access gateway configures on the point-to-point link shared with a given mobile node be generated by the local mobility anchor and be stored in the mobile node's Binding Cache entry. This address will not change for the duration of that mobile node's session and can be provided to the serving mobile access gateway at every mobile node's handoff, as part of the Proxy Mobile IPv6 signaling messages. The specific method by which the local mobility anchor generates the link-local address is out of scope for this specification.

Optionally, implementations MAY choose to configure a fixed link-local address across all the access links in a Proxy Mobile IPv6 domain and without a need for carrying this address from the local

mobility anchor to the mobile access gateway in the Proxy Mobile IPv6 signaling messages.

6.9. Signaling Considerations

6.9.1. Binding Registrations

6.9.1.1. 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.
2. The Proxy Binding Update message MUST include the Mobile Node Identifier option [[RFC-4283](#)], carrying the MN-Identifier for identifying the mobile node.
3. The Home Network Prefix option(s) MUST be present in the Proxy Binding Update message. If the mobile access gateway learns the mobile node's home network prefix(es) either from its policy store or from other means, the mobile access gateway MAY choose to request the local mobility anchor to allocate the requested prefix(es) by including a Home Network Prefix option for each of those requested prefixes. The mobile access gateway MAY also choose to include just one Home Network Prefix option with the prefix value of ALL_ZERO, for requesting the local mobility anchor to do the prefix assignment. However, when including a Home Network Prefix option with the prefix value of ALL_ZERO, then there MUST be only one instance of the Home Network prefix option in the request.
4. The Handoff Indicator option MUST be present in the Proxy Binding Update message. The Handoff Indicator field in the Handoff Indicator option MUST be set to a value indicating the handoff hint.
 - * The Handoff Indicator field MUST be set to value 1 (Attachment over a new interface), if the mobile access gateway determines (under the Handoff Indicator considerations specified in this section) that the mobile node's current attachment to the network over this interface is not as a result of a handoff of an existing mobility session (over the same interface or through a different interface), but as a result of an attachment over a new interface. This essentially serves as a request to the local

mobility anchor to create a new 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.

- * The Handoff Indicator field MUST be set to value 2 (Handoff between two different interfaces of the mobile node), if the mobile access gateway definitively knows the mobile node's current attachment is due to a handoff of an existing mobility session, between two different interfaces of the mobile node.
 - * The Handoff Indicator field 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 an existing mobility session between two mobile access gateways and for the same interface of the mobile node.
 - * The Handoff Indicator field MUST be set to value 4 (Handoff state unknown), if the mobile access gateway cannot determine if the mobile node's current attachment is due to a handoff of an existing mobility session.
5. The mobile access gateway MUST apply the below considerations when choosing the value for the Handoff Indicator field.
- * The mobile access gateway can choose to use the value 2 (Handoff between two different interfaces of the mobile node), only when it knows that the mobile node has on purpose switched from one interface to another, and the previous interface is going to be disabled. It may know this due to a number of factors. For instance, most cellular networks have controlled handovers where the network knows that the host is moving from one attachment to another. In this situation the link layer mechanism can inform the mobility functions that this is indeed a movement, not a new attachment.
 - * Some link layers have link-layer identifiers that can be used to distinguish (a) the movement of a particular interface to a new attachment from (b) the attachment of a new interface from the same host. Option value 3 (Handoff between mobile access gateways for the same interface) is appropriate in case a and value of 1 (Attachment over a new interface) in case b.
 - * The mobile access gateway MUST NOT set the option value to 2 (Handoff between two different interfaces of the mobile node) or 3 (Handoff between mobile access gateways for the same

interface) if it can not be determined that the mobile node can move the address between the interfaces involved in the handover or that it is the same interface that has moved. Otherwise Proxy Mobile IPv6-unaware hosts that have multiple physical interfaces to the same domain may suffer unexpected failures.

- * Where no support from the link layer exists, the host and the network would need to inform each other about the intended movement. The Proxy Mobile IPv6 protocol does not specify this and simply requires that knowledge about movements can be derived either from the link-layer or from somewhere else. The method by which this is accomplished is outside the scope of this specification.
6. Either the Timestamp option or a valid sequence number maintained on a per mobile node basis (if the Sequence Number based scheme is in use) MUST be present. When Timestamp option is added to the message, the mobile access gateway SHOULD also set the Sequence Number field to a value of a monotonically increasing counter (not to be confused with the per mobile node sequence number specified in [[RFC-3775](#)]). The local mobility anchor will ignore this field when there is a Timestamp option present in the request, but will return the same value in the Proxy Binding Acknowledgement message. This will be useful for matching the reply to the request message.
 7. The Mobile Node Link-layer Identifier option carrying the link-layer identifier of the currently attached interface MUST be present in the Proxy Binding Update message, if the mobile access gateway is aware of the same. If the link-layer identifier of the currently attached interface is not known or if the identifier value is ALL_ZERO, this option MUST NOT be present.
 8. The Access Technology Type option MUST be present in the Proxy Binding Update message. The access technology type field in the option SHOULD be set to the type of access technology using which the mobile node is currently attached to the mobile access gateway.
 9. The Link-local Address option MAY be present in the Proxy Binding Update message. Considerations from [Section 6.8](#) MUST be applied when using the link-local address option.
- * When querying the local mobility anchor for the link-local address that it should use on the point-to-point link shared with the mobile node, this option MUST be set to ALL_ZERO.

This essentially serves as a request to the local mobility anchor to provide the link-local address that it can use on the access link shared with the mobile node.

- * When uploading the link-local address to the local mobility anchor, the value in the option MUST be set to the link-local address that is configured on the point-to-point link shared with the mobile node. This is allowed only during an initial mobile node's attachment.

10. The Proxy Binding Update message MUST be constructed as specified in [Section 6.9.1.5](#).
11. If there is no existing Binding Update List entry for that mobile node, the mobile access gateway MUST create a Binding Update List entry for the mobile node upon sending the Proxy Binding Update request.

[6.9.1.2](#). Receiving Binding Registration Reply

On receiving a Proxy Binding Acknowledgement message (format specified in [Section 8.2](#)) from the local mobility anchor, the mobile access gateway MUST process the message as specified below.

1. The received Proxy Binding Acknowledgement message (a Binding Acknowledgement message with the 'P' flag set to value of 1) MUST be authenticated as described in [Section 4](#). 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 message.
2. The mobile access gateway MUST observe the rules described in [Section 9.2 of \[RFC-3775\]](#) when processing Mobility Headers in the received Proxy Binding Acknowledgement message.
3. The mobile access gateway MUST apply the considerations specified in [Section 5.5](#) for processing the Sequence Number field and the Timestamp option (if present), in the message.
4. The mobile access gateway MUST ignore any checks, specified in [[RFC-3775](#)] related to the presence of a Type 2 Routing header in the Proxy Binding Acknowledgement message.
5. The mobile access gateway MAY use the mobile node identifier present in the Mobile Node Identifier option for matching the

response to the request messages that it sent recently. However, if there is more than one request message in its request queue for the same mobile node, the sequence number field can be used for identifying the exact message from those messages. There are other ways to achieve this and implementations are free to adopt the best approach that suits their implementation. Additionally, if the received Proxy Binding Acknowledgement message does not match any of the Proxy Binding Update messages that it sent recently, the message MUST be ignored.

6. If the received Proxy Binding Acknowledgement message has any one or more of the following options, Handoff Indicator option, Access Technology Type option, Mobile Node Link-layer Identifier option, Mobile Node Identifier option, carrying option values that are different from the option values present in the corresponding request (Proxy Binding Update) message, the message MUST be ignored as the local mobility anchor is expected to echo back all these listed options and with the same option values in the reply message. Further, the mobile access gateway MUST NOT retransmit the Proxy Binding Update message till an administrative action is taken.
7. 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 deny the mobility service to that mobile node.
8. If the received Proxy Binding Acknowledgement message has the Status field value set to TIMESTAMP_LOWER_THAN_PREV_ACCEPTED (Timestamp value lower than previously accepted value), the mobile access gateway SHOULD try to register again to reassert the mobile node's presence on its access link. The mobile access gateway is not specifically required to synchronize its clock upon receiving this error code.
9. If the received Proxy Binding Acknowledgement message has the Status field value set to TIMESTAMP_MISMATCH (Invalid timestamp value), 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.

10. If the received Proxy Binding Acknowledgement message has the Status field value set to NOT_AUTHORIZED_FOR_HOME_NETWORK_PREFIX (The mobile node is not authorized for one or more of the requesting home network prefix(es)), the mobile access gateway SHOULD NOT request for the same prefix(es) again, but can only request the local mobility anchor to do the assignment of prefix(es) by including only one Home Network Prefix option with the prefix value set to ALL_ZERO.
11. 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(es) in the Router Advertisement messages sent on that access link and MUST deny the mobility service to the mobile node by not forwarding any packets received from the mobile node using an address from the home network prefix(es). It MAY also tear down the point-to-point link shared with the mobile node.
12. If the received Proxy Binding Acknowledgement message has the Status field value set to 0 (Proxy Binding Update accepted), the mobile access gateway MUST establish a bi-directional tunnel to the local mobility anchor (if there is no existing bi-directional tunnel to that local mobility anchor). Considerations from [Section 5.6.1](#) MUST be applied for managing the dynamically created bi-directional tunnel.
13. The mobile access gateway MUST set up the route for forwarding the packets received from the mobile node using address(es) from its home network prefix(es) through the bi-directional set up for that mobile node. The created tunnel and the routing state MUST result in the forwarding behavior on the mobile access gateway as specified in [Section 6.10.5](#).
14. The mobile access gateway MUST also update the Binding Update List entry for reflecting the accepted binding registration values. It MUST also advertise the mobile node's home network prefix(es) as the hosted on-link prefixes, by including them in the Router Advertisement messages that it sends on that access link.
15. If the received Proxy Binding Acknowledgement message has the address in the Link-local Address option set to a NON_ZERO value, the mobile access gateway MUST configure that link-local address on that point-to-point link and MUST NOT configure any other link-local address on that point-to-point link. This will avoid any link-local address collisions with the mobile node on that access link.

6.9.1.3. Extending Binding Lifetime

1. For extending the lifetime of a currently registered mobile node (i.e., after a successful initial binding registration from the same mobile access gateway), the mobile access gateway can send a Proxy Binding Update message to the local mobility anchor with a new lifetime value. This re-registration message MUST be constructed with the same set of options as the initial binding registration message, under the considerations specified in [Section 6.9.1.1](#). However the following exceptions apply.
2. There MUST be a Home Network Prefix option for each of the assigned home network prefixes assigned for that mobility session and with the prefix value in the option set to that respective prefix value.
3. The Handoff Indicator field in the Handoff Indicator option MUST be set to a value of 5 (Handoff state not changed - Re-Registration).

6.9.1.4. Mobile Node Detachment and Binding De-Registration

1. If at any point the mobile access gateway detects that the mobile node has moved away from its access link, or if it decides to terminate the mobile node's mobility session, it SHOULD send a Proxy Binding Update message to the local mobility anchor with the lifetime value set to zero. This de-registration message MUST be constructed with the same set of options as the initial binding registration message, under the considerations specified in [Section 6.9.1.1](#). However, the following exceptions apply.
2. There MUST be a Home Network Prefix option for each of the assigned home network prefix(es) assigned for that mobility session and with the prefix value in the option set to the respective prefix value.
3. The Handoff Indicator field in the Handoff Indicator option MUST be set to a value of 4 (Handoff state unknown).

Either upon receipt of a Proxy Binding Acknowledgement message from the local mobility anchor or after INITIAL_BINDACK_TIMEOUT [[RFC-3775](#)] timeout waiting for the reply, the mobile access gateway MUST do the following:

1. It MUST remove the Binding Update List entry for the mobile node from its Binding Update List.

2. It MUST remove the created routing state for tunneling the mobile node's traffic.
3. If there is a dynamically created tunnel to the mobile node's local mobility anchor and if there are not other mobile nodes for which the tunnel is being used, then the tunnel MUST be deleted.
4. It MUST tear down the point-to-point link shared with the mobile node. This action will force the mobile node to remove any IPv6 address configuration on the interface connected to this point-to-point link.

6.9.1.5. Constructing the Proxy Binding Update Message

- o 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 MUST be set to value 1 */
  Mobility Options
    - Mobile Node Identifier option          (mandatory)
    - Home Network Prefix option(s)         (mandatory)
    - Handoff Indicator option               (mandatory)
    - Access Technology Type option         (mandatory)
    - Timestamp option                      (optional)
    - Mobile Node Link-layer Identifier option (optional)
    - Link-local Address option              (optional)
```

Figure 12: Proxy Binding Update message format

- o The Source Address field in the IPv6 header of the message MUST be set to the global address configured on the egress interface of the mobile access gateway. When there is no Alternate Care-of Address option present in the request, this address will be considered as the Proxy-CoA address for this binding registration request. However, when there is Alternate Care-of Address option present in the request, this address will not be considered as the Proxy-CoA address, but the address in the alternate Care-of Address option will be considered as the Proxy-CoA address.
- o The Destination Address field in the IPv6 header of the message MUST be set to the local mobility anchor address.

- o The Mobile Node Identifier option [[RFC-4283](#)] MUST be present.
- o At least one Home Network Prefix option MUST be present.
- o The Handoff Indicator option MUST be present.
- o The Access Technology Type option MUST be present.
- o The Timestamp option MAY be present.
- o The Mobile Node Link-layer Identifier option MAY be present.
- o The Link-local Address option MAY be present.
- o 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.
- o Unlike in Mobile IPv6 [[RFC-3775](#)], the Home Address option [RFC-3775] MUST NOT be present in the IPv6 Destination Options extension header of the Proxy Binding Update message.

6.9.2. Router Solicitation Messages

A mobile node may send a Router Solicitation message on the access link shared with the mobile access gateway. The Router Solicitation message that the mobile node sends is as specified in [[RFC-4861](#)]. The mobile access gateway on receiving the Router Solicitation message or before sending a Router Advertisement message MUST apply the following considerations.

1. The mobile access gateway on receiving the Router Solicitation message SHOULD send a Router Advertisement message containing the mobile node's home network prefix(es) as the on-link prefix(es). However, before sending the Router Advertisement message containing the mobile node's home network prefix(es), 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 reason, the mobile access gateway MUST NOT advertise the mobile node's home network prefix(es) in the Router Advertisement messages that it sends on the access link. However, it MAY choose to advertise a local visited network prefix(es) to enable the mobile node for regular IPv6 access.

3. The mobile access gateway SHOULD add the MTU option, as specified in [\[RFC-4861\]](#), to the Router Advertisement messages that it sends on the access link. This will ensure the mobile node on the link uses the advertised MTU value. The MTU value SHOULD reflect the tunnel MTU for the bi-directional tunnel between the mobile access gateway and the local mobility anchor. Considerations from [Section 6.9.5](#) SHOULD be applied for determining the tunnel MTU value.

[6.9.3.](#) Default-Router

In Proxy Mobile IPv6, the mobile access gateway is the IPv6 default-router for the mobile node on the access link, as it is the entity that sends the Router Advertisements on the access link. However, as the mobile node moves from one access link to another, the serving mobile access gateway on those respective links will send the Router Advertisement messages. If these Router Advertisements are sent using a different link-local address or a different link-layer address, the mobile node will always detect a new default-router after every handoff. For solving this problem, this specification requires all the mobile access gateways in the Proxy Mobile IPv6 domain to use the same link-local and link-layer address on any of the access links where ever the mobile node attaches. These addresses can be fixed addresses across the entire Proxy Mobile IPv6 domain and all the mobile access gateways can use these globally fixed address on any of the point-to-point links. Additionally, this specification allows the local mobility anchor to generate the link-local address and provide it to the mobile access gateway as part of the signaling messages.

However, both of these approaches (a link-local address generated by the local mobility anchor or when using a globally fixed link-local address) have implications on the deployment of SEcure Neighbor Discovery (SEND) [\[RFC-3971\]](#). In SEND, routers have certificates and public key pairs, and their Router Advertisements are signed with the private keys of these key pairs. When a number of different routers use the same addresses, the routers either all have to be able to construct these signatures for the same key pair, or the used key pair and the router's cryptographic identity must change after a movement. Both approaches are problematic. Sharing of private key information across a number of nodes would be inappropriate. And changing even the cryptographic identity of the router goes against the general idea of the Proxy Mobile IPv6 being as invisible to the hosts as possible.

There is, however, ongoing work at the IETF to revise the SEND specifications. It is suggested that these revisions also address the above problem. Other revisions are needed to deal with other

problematic cases (such as Neighbor Discovery proxies) before widespread deployment of SEND.

6.9.4. Retransmissions and Rate Limiting

The mobile access gateway is responsible for retransmissions and rate limiting the binding registration requests that it sends to the local mobility anchor. The Retransmission and the Rate Limiting rules are as specified in [RFC-3775]. However, the following considerations MUST be applied.

1. When the mobile access gateway sends a Proxy Binding Update request, it should use the constant, INITIAL_BINDACK_TIMEOUT [RFC-3775], for configuring the retransmission timer, as specified in Section 11.8 [RFC-3775]. However, the mobile access gateway is not required to use a longer retransmission interval of InitialBindackTimeoutFirstReg as specified in [RFC-3775] for the initial binding registration request.
2. If the mobile access gateway fails to receive a valid matching response for a registration or re-registration message 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 of [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 the Timestamp based scheme is in use, the retransmitted Proxy Binding Update messages MUST use the latest timestamp. If the 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].

6.9.5. Path MTU Discovery

For getting optimal throughput, it is required that the routed packets between the local mobility anchor and the mobile access gateway are sent in the largest size and without fragmentation. If the mobility entities are aware of the Path MTU (PMTU) between

themselves, it can be used for determining the Tunnel Path MTU and also for advertising this value as the link MTU on the access link shared with the mobile node. The following are some of the considerations related to Path MTU discovery.

- o The local mobility anchor and mobile access gateway MAY use the Path MTU Discovery mechanisms as specified in [RFC-1981] and [RFC-4821]. for determining the Path MTU (PMTU) for the path between themselves.
- o The local mobility anchor and the mobile access gateway MAY use any standard application probes for determining the PMTU. The specifics details related to the type of traffic that can be used for the PMTU discovery is outside the scope of this document.
- o If there is an administratively configured PMTU value for the path between the local mobility anchor and the mobile access gateway, the dynamic discovery of PMTU is not required.
- o The IPv6 tunnel MTU for the established tunnel between the local mobility anchor and the mobile access gateway can be computed based on this Path MTU value, as specified in [Section 6.7](#) of [RFC-2473].
- o The mobile access gateway SHOULD use this determined tunnel Path MTU value (for the tunnel established with the mobile node's local mobility anchor) as the MTU value in the MTU option that it sends in the Router Advertisements on the access link shared with the mobile node.

[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 interfaces.

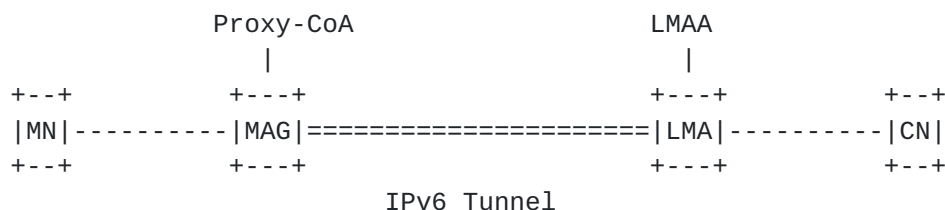


Figure 13: Proxy Mobile IPv6 Tunnel

6.10.1. Transport Network

As per this specification, the transport network between the local mobility anchor and the mobile access gateway is an IPv6 network. The companion document [[ID-IPV4-PMIP6](#)] specifies the required extensions for negotiating IPv4 transport and the corresponding encapsulation mode.

6.10.2. Tunneling & Encapsulation Modes

An IPv6 address that a mobile node uses from its home network prefix(es) 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 [[RFC-2473](#)], between the home agent and the mobile node and this specification extends the use of the same tunneling mechanism for use between the local mobility anchor and the mobile access gateway.

On most operating systems, a tunnel is 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 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 a global address on its egress interface (Proxy-CoA) and the destination address field set to the global address of the local mobility anchor (LMAA).

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

- o IPv6-In-IPv6 - IPv6 datagram encapsulated in an IPv6 packet [[RFC-2473](#)].

The companion document [[ID-IPV4-PMIP6](#)] specifies other encapsulation modes for supporting IPv4 transport.

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

PMIP6].

- o IPv6-In-IPv4-UDP - IPv6 datagram encapsulation in an IPv4 UDP packet. This mode is specified in [[ID-IPV4-PMIP6](#)].
- o IPv6-In-IPv4-UDP-TLV - IPv6 datagram encapsulation in an IPv4 UDP packet with a TLV header. This mode is specified in [[ID-IPV4-PMIP6](#)].

[6.10.3.](#) 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 flag EnableMAGLocalRouting MAY be used for controlling this behavior. 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.

[6.10.4.](#) 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.

[6.10.5.](#) Forwarding Rules

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

- o 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. Considerations from [RFC-2473] MUST be applied for IPv6 decapsulation. 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 [[RFC-2473](#)] MUST be applied.

- o 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 flag 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:

- o 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.
- o On receiving a packet from a mobile node connected to its access link for a destination that is locally connected, the mobile access gateway MUST check the flag 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 MUST route the packet directly to the destination.
- o On receiving a packet from a 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.
- o The format of the tunneled packet is shown below. Considerations from [[RFC-2473](#)] MUST be applied for IPv6 encapsulation. 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 14: Tunneled Packet from MAG to LMA

- o The format of the tunneled packet is shown below, when payload protection using IPsec is enabled for the mobile node's data traffic. However, when using IPv4 transport, the format of the packet is as described in [\[ID-IPV4-PMIP6\]](#).

```

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

```

Figure 15: Tunneled Packet from MAG to LMA with Payload Protection

[6.11.](#) Supporting DHCPv6 based Address Configuration on the Access Link

This section explains how Stateful Address Configuration using DHCPv6 support can be enabled in a Proxy Mobile IPv6 domain. It also identifies the required configuration in DHCP and mobility infrastructures for supporting this address configuration mode and also identifies the protocol interactions between these two systems.

- o For supporting Stateful Address Configuration using DHCP, the DHCP relay agent [\[RFC-3315\]](#) service MUST be configured on all the mobile access gateways in the Proxy Mobile IPv6 domain. Further, as specified in [Section 20 of \[RFC-3315\]](#), the DHCP 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 as required in a given deployment.
- o The DHCP infrastructure needs to be configured with different IPv6 prefix groups, each group MUST represent a link in that Proxy Mobile IPv6 domain on which those respective prefixes are hosted. In essence the DHCP infrastructure is aware of all the links in that domain along with the associated IPv6 prefixes with each one of those links. This configuration requirement is identical to the fixed infrastructure configuration except with the key difference that these links are mobile in nature, a link along with its prefixes associated with a given mobile node and a mobile access gateway pair at a point of time may be associated with a different mobile access gateway and mobile node pair at a later point of time. However, from the perspective of the DHCP server, this aspect of prefix mobility will not be visible to it.

- o The local mobility anchor needs to have the same awareness with respect to the links along with the associated prefixes in a Proxy Mobile IPv6 domain. When a local mobility anchor assigns prefix(es) to a mobile node, it MUST assign all the prefixes associated with a given link and all of those assigned prefixes will remain as the home network prefixes for that mobile node through out the life of that mobility session. The serving mobile access gateway that hosts these prefixes is physically connected to that link and can function as the DHCP relay agent. This common understanding between DHCP and mobility entities about all the links in the domain along with the associated prefixes, provides the required coordination for allowing mobility entities to perform prefix assignment dynamically to a mobile node and still allowing DHCP infrastructure to perform address assignment for that mobile node only from its home network prefixes.
- o When a mobile node sends a DHCP request message, the DHCP relay agent function on the mobile access gateway will set the link-address field in the DHCP message to an address in the mobile node's home network prefix (any one of the mobile node's home network prefixes assigned to that mobile node's attached interface). The address can be generated as per [\[RFC-4862\]](#) by combining that mobile node's home network prefix and its own interface identifier on that access link shared with the mobile node, so as to provide a hint to the DHCP Server for the link identification. The DHCP server on receiving the request from the mobile node, will allocate addresses from all the prefixes associated with that link (identified using the link-address field of the request).
- o Once the mobile node obtains address(es) and moves to a different link and sends a DHCP request (at any time) for extending the DHCP lease, the DHCP relay agent on the new link will set the prefix hint in the DHCP message to one of the mobile node's home network prefixes. The DHCP server will identify the client from the Client-DUID option and will identify the link from the link-address option present in the request and will allocate the same address(es) as before.
- o The DHCP based address configuration is not recommended for deployments where the local mobility anchor and the mobile access gateway 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 request messages from a given mobile node anchored on any of the access links in that domain, will always be handled by the same DHCP server or by a server from the same group of coordinated DHCP servers serving that domain.

- o The DHCP infrastructure should be configured to offer low address lease reclaiming the address even after the local mobility anchor deletes the mobile node's binding cache entry. It is recommended that the configured lease time be lower than the accepted binding lifetime for any mobility binding.

6.12. Home Network Prefix Renumbering

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

- o Link-layer event specific to the access technology
- o PPP Session termination event on point-to-point link types

- o IPv6 Neighbor Unreachability Detection event from IPv6 stack
- o 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 a scenario the normal IPv6 considerations apply. If IPv6 access is enabled, the mobile node **SHOULD** be able to obtain IPv6 address(es) using the normal IPv6 address configuration procedures. The obtained address(es) must be from a local visitor network prefix(es). This essentially ensures that the mobile access gateway functions as a normal access router to a mobile node attached to its access link and without 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

When 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 set up 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 a Router Solicitation message [[RFC-4861](#)]. The mobile access gateway on the access link will respond to the Router Solicitation message with a Router Advertisement message. The Router Advertisement message will carry the mobile node's home network prefix(es), 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 completes the signaling with the mobile node's local mobility anchor, the mobile access gateway may not know the mobile node's home network prefix(es) and may not be able to emulate the mobile node's home link on the access link. In such a scenario, the mobile node may notice a delay before it receives a Router Advertisement message. This will also affect mobile nodes that would be capable of handling their own mobility, or mobile nodes that do not need to maintain the same IP address through movements.

If the received Router Advertisement message 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 can obtain one or more addresses and from its home network prefix(es).

If the received Router Advertisement message does not have the Managed Address Configuration flag set and if the mobile node is allowed to use autoconfigured address(es), the mobile node will be able to obtain IPv6 address(es) and from each of its home network prefixes using any of the standard IPv6 address configuration mechanisms permitted for that mode.

If the mobile node is IPv4 enabled and if the network permits, it will be able to obtain the IPv4 address configuration as specified in the companion document [[ID-IPV4-PMIPv6](#)].

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

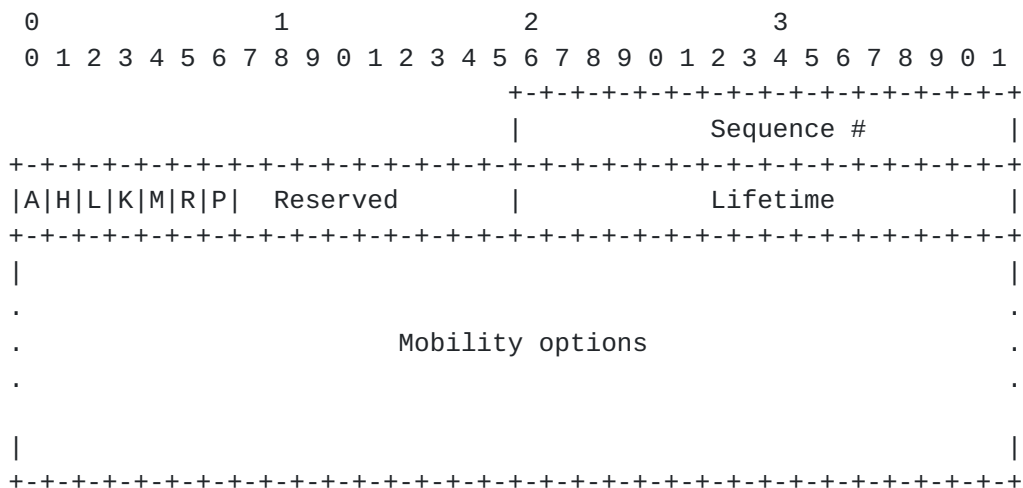
After obtaining the address configuration in the Proxy Mobile IPv6 domain, as the mobile node moves and changes its point of attachment from one mobile access gateway to the other, it can still continue to use the same address configuration. As long as the attached access

link is in the scope of that Proxy Mobile IPv6 domain, the mobile node will always detect the same default-router advertising the mobile node's home network prefix(es) on each connected link. If the mobile node has address configuration that it obtained using DHCPv6, it will be able to retain the address configuration and extend the lease lifetime.

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 of \[RFC-3775\]](#). 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. These options can be present in the message in any order. There can be one or more instances of the Home Network Prefix options present in the message. However, there cannot be more than one instance of any of the other options.

Mobile Node Identifier option

Home Network Prefix option

Handoff Indicator option

Access Technology Type option

Timestamp option

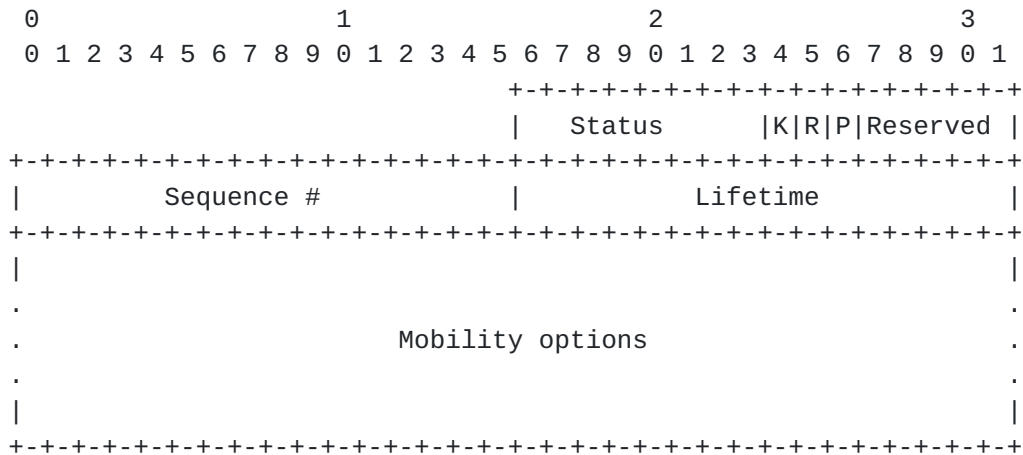
Mobile Node Link-layer Identifier option

Link-local Address option

Additionally, there can one or more instances of the Vendor-Specific Mobility option [[RFC-5094](#)].

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

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) flag as specified in [RFC-3963].

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 to value of 1 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 of \[RFC-3775\]](#). 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. These options can be present in the message in any order. There can be one or more instances of the Home Network Prefix options present in the message. However, there cannot be more than one instance of any of the other options.

Mobile Node Identifier option

Home Network Prefix option

Handoff Indicator option

Access Technology Type option

Timestamp option

Mobile Node Link-layer Identifier option

Link-local Address option

Additionally, there can one or more instances of the Vendor-Specific Mobility option [[RFC-5094](#)].

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 8.9](#) defines the Status values that can be used in Proxy Binding Acknowledgement message.

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

[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. There can be multiple Home Network Prefix options present in the message.

The Home Network Prefix Option has an alignment requirement of $8n+4$. Its format is as follows:

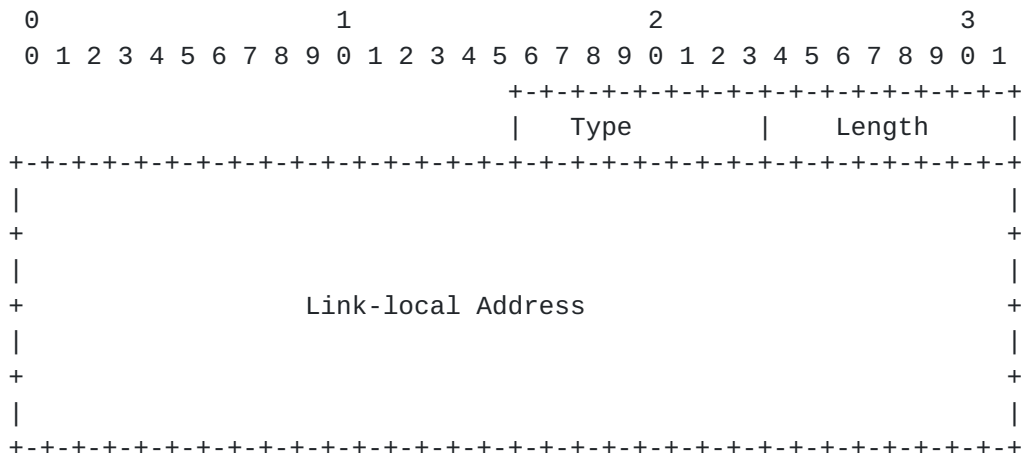
The content and format of this field (including byte and bit ordering) is as specified in [Section 4.6 of \[RFC-4861\]](#) for carrying Link-Layer Address. On certain access links, where the link-layer address is not used or cannot be determined,

this option cannot be used.

8.7. 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 link-local address of the mobile access gateway.

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.

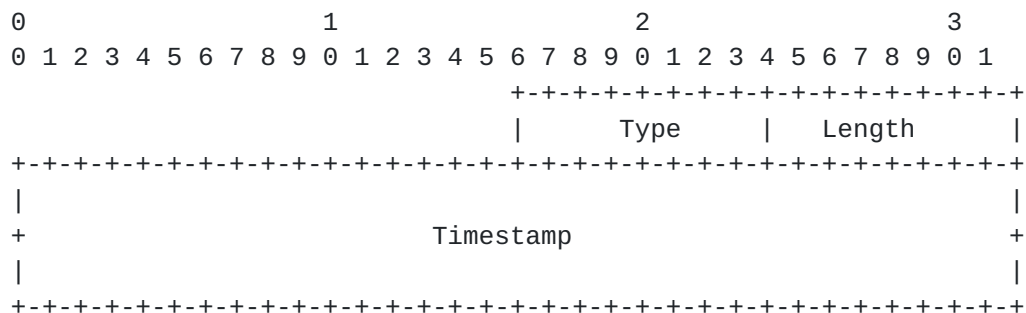
Link-local Address

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

8.8. 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.

8.9. 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 of \[RFC-3775\]](#).

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: IANA

Proxy registration not enabled for the mobile node

NOT_LMA_FOR_THIS_MOBILE_NODE: IANA

Not local mobility anchor for this mobile node

MAG_NOT_AUTHORIZED_FOR_PROXY_REG: IANA

The mobile access gateway is not authorized to send proxy binding registrations

NOT_AUTHORIZED_FOR_HOME_NETWORK_PREFIX: IANA

The mobile node is not authorized for one or more of the requesting home network prefixes.

TIMESTAMP_MISMATCH: IANA

Invalid timestamp value (the clocks are out of sync)

TIMESTAMP_LOWER_THAN_PREV_ACCEPTED: IANA

The timestamp value is lower than the previously accepted value

MISSING_HOME_NETWORK_PREFIX_OPTION: IANA

Missing home network prefix option

BCE_PBU_PREFIX_SET_DO_NOT_MATCH: IANA

All the home network prefixes listed in the BCE do not match all the prefixes in the received PBU

MISSING_MN_IDENTIFIER_OPTION: IANA

Missing mobile node identifier option

MISSING_HANDOFF_INDICATOR_OPTION: IANA

Missing handoff indicator option

MISSING_ACCESS_TECH_TYPE_OPTION: IANA

Missing access technology type option

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

[9.](#) Protocol Configuration Variables

[9.1.](#) Local Mobility Anchor - Configuration Variables

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

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.

MaxDelayBeforeNewBCEAssign

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.

TimestampValidityWindow

This variable specifies the maximum amount of time difference in milliseconds between the timestamp in the received Proxy Binding Update message and the current time-of-day on the local mobility anchor, that is allowed by the local mobility anchor for the received message to be considered valid.

The default value for this variable is 300 milliseconds. This variable must be adjusted to suit the deployments.

9.2. Mobile Access Gateway - Configuration Variables

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

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 value of 0, 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 value of 1, 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.

9.3. Proxy Mobile IPv6 Domain - Configuration Variables

All the mobile entities (local mobility anchors and mobile access gateways in a Proxy Mobile IPv6 domain MUST allow the following variables to be configured by the system management. The configured values for these protocol variables MUST survive server reboots and service restarts. These variables MUST be globally fixed for a given Proxy Mobile IPv6 domain resulting in the same values being enforced on all the mobility entities in that domain.

MobileNodeGeneratedTimestampInUse

This flag indicates whether or not the mobile node generated timestamp mechanism is in use in that Proxy Mobile IPv6 domain. When the value for this flag is set to 1, the local mobility anchors and mobile access gateways in that Proxy Mobile IPv6 domain MUST apply the mobile node generated timestamp considerations.

The default value for this flag is set to value of 0, indicating that the mobile node generated timestamp mechanism is not in use in that Proxy Mobile IPv6 domain.

10. IANA Considerations

This document defines six new Mobility Header options, the Home Network Prefix option, Handoff Indicator option, Access Technology Type option, Mobile Node Link-layer Identifier option, Link-local Address option and Timestamp option. These options are described in [Section 8](#). 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 Handoff Indicator option defined in [Section 8.4](#) of this document

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

The Access Technology Type option defined in [Section 8.5](#) of this document introduces a new Access Technology type (ATT) numbering space, where the values from 0 to 5 have been reserved by this document. Approval of new Access Technology type values are to be made through IANA Expert Review.

This document also defines new Binding Acknowledgement status values as described in [Section 8.9](#). 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 Jari Arkko, Julien Laganier, Christian Vogt, Dave Thaler, Pasi Eronen, Pete McCann, Brian Haley, Ahmad Muhanna, JinHyeock Choi and Elwyn Davies 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 Giarretta, Henrik Levkowetz, Hesham Soliman, James Kempf, Jean-Michel Combes, Jun Awano, John Zhao, Jong-Hyouk Lee, Jonne Soininen, Jouni Korhonen, Kalin Getov, Kilian Weniger, Lars Eggert, Magnus Westerlund, Marco Liebsch, Mohamed Khalil, Nishida Katsutoshi, Phil Roberts, Ralph Droms, Ryuji Wakikawa, Sangjin Jeong, Suresh Krishnan, Uri Blumenthal, 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 and we acknowledge that !

The authors would also like to thank Ole Troan, Akiko Hattori, Parviz Yegani, Mark Grayson, Michael Hammer, Vojislav Vucetic, Jay Iyer, Tim Stammers, Bernie Volz and Josh Littlefield 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-4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", [RFC 4282](#), December 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-4291] Hinden, R., Deering, S., "IP Version 6 Addressing Architecture", [RFC 4291](#), February 2006.
- [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-1981] McCann, J., Deering, S., and J. Mogul, "Path MTU Discovery for IP version 6", [RFC 1981](#), August 1996.
- [RFC-2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", [RFC 2865](#), June 2000.

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

[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 4330](#), October 1996.

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

[RFC-4821] Mathis, M. and Heffner, J., "Packetization Layer Path MTU Discovery", [RFC 4821](#), March 2007.

[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-5094] Devarapalli, V., Leung, K. and Patel, A., "Mobile IPv6 Vendor Specific Option", [RFC 5094](#), December 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] Narayanan, S., et al "Detecting Network Attachment in IPv6 Networks (DNAV6)", [draft-ietf-dna-protocol-07.txt](#), February 2008.

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(es) on a per-interface basis, permitted address configuration modes, roaming policy and other parameters that are essential for providing network-based mobility management service. This information is typically configured in AAA. In some cases, the home network prefix(es) may be dynamically assigned to the mobile node's interface, after its initial attachment to the Proxy Mobile IPv6 domain over that interface and may not be configured in the mobile node's policy profile.

The network entities in the proxy Mobile IPv6 domain, while serving a mobile node will have access to the mobile node's policy profile and these entities can query this information using RADIUS [[RFC-2865](#)] or DIAMETER [[RFC-3588](#)] protocols.

Appendix B. Routing State

The following section explains the routing state created 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,	_ANY_DESTINATION_	Tunnel0
(IPv6 Prefix or	-----	
Input Interface)	Locally Connected	Tunnel0
+-----+		
MAC_Address_MN2,	_ANY_DESTINATION_	Tunnel1
+ (IPv6 Prefix or	-----	
Input Interface	Locally Connected	direct
+-----+		

Figure 24: Example - Policy based Route Table

+=====+			
Interface	Source Address	Destination Address	Encapsulation
+=====+			
Tunnel0	Proxy-CoA	LMAA1	IPv6-in-IPv6
+-----+			
Tunnel1	Proxy-CoA	LMAA2	IPv6-in-IPv6
+-----+			

Figure 25: Example - Tunnel Interface Table

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
Wichorus
3590 North First Street
San Jose, CA 95134
USA

Email: vijay@wichorus.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

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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

