NETLMM WG
Internet-Draft
Expires: July 9, 2007

S. Gundavelli
K. Leung
Cisco Systems
V. Devarapalli
Azaire Networks
K. Chowdhury
Starent Networks
January 5, 2007

Proxy Mobile IPv6
draft-sgundave-mip6-proxymip6-01

Status of this Memo

Copyright Notice

Abstract

This specification describes a network-based mobility management protocol. It is called Proxy Mobile IPv6 (PMIPv6) and is based on Mobile IPv6. This protocol is for providing mobility support to any IPv6 host within a restricted and topologically localized portion of

the network and with out requiring the participation of the host in any mobility related signaling.

Table of Contents

1. Introduction

The IP Mobility protocols designed in the IETF so far involve the host in mobility management. There are some deployment scenarios where a network-based mobility management protocol is considered appropriate. The advantages to using a network-based mobility protocol include avoiding tunneling overhead over the air and support for hosts that do not implement any mobility management protocol.

The document describes a network-based mobility management protocol based on Mobile IPv6. it is called Proxy Mobile IPv6 (PMIPv6). One of the most important design considerations behind PMIPv6 has been to re-use as much as possible from the existing mobility protocols.

There are many advantages to develop a protocol based on Mobile IPv6. Mobile IPv6 is a very mature mobility protocol for IPv6. There have been many implementations and inter-operability events where Mobile IPv6 has been tested. There also numerous specifications enhancing Mobile IPv6 that can be re-used. Further, the Proxy MIPv6 solution described in this document allows the same Home Agent to provide mobility to hosts that use Mobile IPv6 and hosts that do not use any mobility management protocol. Proxy Mobile IPv6 provides solution to a real deployment problem.

2. Conventions used in this document

The keywords "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 [4].

The following new terminology and abbreviations are introduced in this document and all other general mobility related terms as defined in Mobile IPv6 specification [2].

Proxy Mobile Agent (PMA)

The proxy mobile agent is a functional element on the access router. This is the entity that makes the mobile node believe it is on its home link, by emulating the home link properties. It registers the location of the mobile node to the home agent and establishes a tunnel for receiving packets sent to the mobile node's home address.

Mobile Node (MN)

This document uses the term mobile node to refer to an IPv6 host. This specification does not require the mobile node to have the Mobile IPv6 client stack.

3. Proxy Mobile IPv6 Protocol Overview

This specification describes a network-based mobility management protocol. It is called Proxy Mobile IPv6 (PMIPv6) and is based on Mobile IPv6. This protocol is for providing mobility support to any IPv6 host, within a restricted and topologically localized portion of the network and with out requiring the participation of the host in any mobility related signaling.

Every mobile node that roams in a Proxy Mobile IPv6 network, would typically be identified by an identifier, such as NAI and that identifier will have an associated policy profile that identifies the mobile's home network prefix, permitted address configuration modes, roaming policy and other parameters that are essential for providing network based mobility service. This information is typically configured in a policy store, such as in AAA infrastructure. All the network entities in the Proxy Mobile IPv6 network will have access to this information.

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

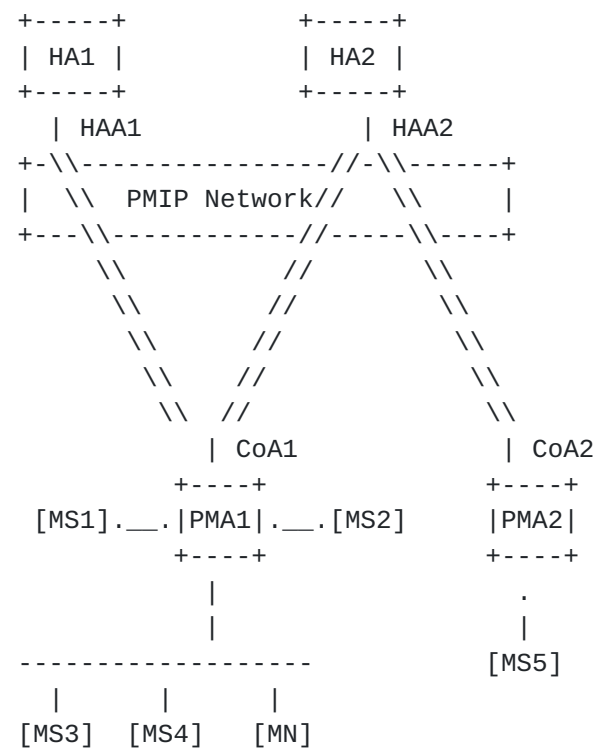


Figure 1: Proxy Mobile IPv6 Domain

The Proxy Mobile IPv6 scheme introduces a new function, the Proxy Mobile Agent (PMA). It is a function that runs on the access router and is the entity that does the mobility related signaling on behalf of the mobile node. From the perspective of the home agent, the proxy mobile agent is a special element in the network that sends Mobile IPv6 signaling messages on behalf of mobile node.

When the mobile node attaches to a link on the access router running proxy mobile agent, the mobile node presents its identity to the network in the form of NAI as part of the access authentication procedure. After a successful authentication, the proxy mobile agent obtains the mobile's profile from the policy store, such as from a AAA infrastructure. It can now emulate the mobile's home network on the access link. The proxy mobile agent sends Router Advertisements to the mobile node advertising its home prefix.

The mobile node on receiving this Router Advertisement will try to configure its interface either using statefull or stateless address configuration modes, based on the permitted configuration modes on that link. In any case, the mobile node will be able to obtain its home address.

For updating the home agent about the current location of the mobile, the proxy mobile agent sends a Binding Update message to the mobile node's home agent. The message will have the mobile node's NAI identifier option. The source address of that message will be the address of the proxy mobile agent on the egress interface. Upon accepting the Binding Update request, the home agent sets up a tunnel to the proxy mobile agent. It also sets up a route to the mobile node's home address over the tunnel and sends Binding Acknowledgment to the proxy mobile agent.

The proxy mobile agent on receiving this Binding Acknowledgment sets up a tunnel to the home agent and adds a default route over the tunnel to the home agent. All traffic from the mobile node gets routed to the mobile node's home agent over the tunnel.

At this point, the mobile node has a valid home address at the point of current attachment, the serving proxy mobile agent and the home agent have proper routing states for handling the traffic sent by the mobile node and also for the incoming traffic to the mobile station.

Home agent being the topological anchor point for the mobile's home prefix, receives any packet from any corresponding node that is sent to the mobile node. Home agent forwards the received packet to the proxy mobile agent through the tunnel. The proxy mobile agent on other end of the tunnel, after receiving the packet removes the tunnel header and forwards the packet on the access link to the mobile station.

The proxy mobile agent acts as a default router on the access link and any packet that the mobile node sends to any corresponding node is received by the proxy mobile agent and it forwards the packet to the home agent through the tunnel. The home agent on the other end of the tunnel, after receiving the packet removes the tunnel header and routes the packet to the destination.

4. Proxy Mobile IPv6 Protocol Security

The signaling messages between the proxy mobile agent and the home agent are protected using IPsec. Per-mobile node security associations are not required between the proxy mobile agent and the home agent to protect the Proxy Binding Update and Proxy Binding Acknowledgment messages.

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

IKEv2 is used to setup security associations between the proxy mobile agent and the home agent to protect the Proxy Binding Update and Proxy Binding Acknowledgment messages. The proxy mobile agent and the home agent can use any of the authentication mechanisms, as specified in IKEv2, for mutual authentication.

Mobile IPv6 specification requires the home agent to prevent a mobile node from creating security associations or creating binding cache entries for another mobile node's home address. In the protocol described in this document, the mobile node is not involved in creating security associations for protecting the signaling messages or sending binding updates. Therefore, this is not a concern. However, the home agent MUST allow only authorized proxy mobile agents to create binding cache entries on behalf of the mobile nodes. The actual mechanism by which the home agent verifies if a proxy mobile agent is authorized to send Proxy Binding Updates on behalf of a mobile node is out of scope for this document. One possible solution is for the home agent to check with the AAA infrastructure if a particular proxy mobile agent is authorized to send Proxy Binding Updates on behalf of a mobile node.

4.1. Peer Authorization Database Entries

The following describes PAD entries on the proxy mobile agent and the home agent. The PAD entries are only example configurations. Note that the PAD is a logical concept and a particular proxy mobile agent or a home agent implementation can implement the PAD in an implementation specific manner. The PAD state may also be distributed across various databases in a specific implementation.

```
proxy mobile agent PAD:
  - IF remote_identity = home_agent_identity_1
       Then authenticate (shared secret/certificate/)
       and authorize CHILD_SA for remote address home_agent_1

home agent PAD:
  - IF remote_identity = pma_11
       Then authenticate (shared secret/certificate/EAP)
       and authorize CHILD_SAs for remote address pma_address_1
```

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

4.2. Security Policy Database Entries

The following describes the security policy entries on the proxy mobile agent and the home agent required to protect the Proxy Mobile IPv6 signaling messages. The SPD entries are only example configurations. A particular proxy mobile agent or a Home Agent implementation could configure different SPD entries as long as they provide the required security.

In the examples shown below, the identity of the proxy mobile agent is assumed to be pma_1, the address of the proxy mobile agent is assumed to be pma_address_1, and the IPv6 address of the Home Agent is assumed to be home_agent_1.

```
mobile node SPD-S:
  - IF local_address = pma_address_1 &
       remote_address = home_agent_1 &
       proto = MH & local_mh_type = BU & remote_mh_type = BAck
    Then use SA ESP transport mode
    Initiate using IDi = pma_1 to address home_agent_1

home agent SPD-S:
  - IF local_address = home_agent_1 &
       remote_address = pma_address_1 &
       proto = MH & local_mh_type = BAck & remote_mh_type = BU
    Then use SA ESP transport mode
```

5. Home Agent Considerations

For supporting the Proxy Mobile IPv6 scheme defined in this document, the Mobile IPv6 home agent entity, defined in [RFC-3775], needs some protocol enhancements. This section describes the required enhancements and the protocol operation on the home agent for supporting this scheme.

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

When the home agent receives a (Proxy) Binding Update message, the source address and the alternate care-of address in the message is the address that is configured on the egress interface of the sending proxy mobile agent and the message is protected by the Security Association of the Proxy Mobile Agent identified with that address. The home agent can distinguish between a Binding Update message received from a proxy mobile agent from a Binding Update message received directly from a mobile node. This distinction is important for using the right security association for validating the Binding Update and this is achieved by relaxing the MUST requirement for having the Home Address Option presence in Destination Options header and by introducing a new flag in the Binding Update message. The home agent as a traditional IPSec peer can use the SPI in the IPSec header [RFC-4306] of the received packet for locating the correct security association and for processing the Binding Update in the context of Proxy Mobile IP scheme.

To allow configuration flexibility, the Proxy Mobile IPv6 scheme allows multiple address configuration models, Per-MN-Prefix and the usual Shared-Prefix addressing model. In the Per-MN-Prefix model, each mobile is allocated a exclusively unique home prefix and the prefix is not hosted on the home link. The home agent in this addressing model is just a topological anchor point and the prefix is physically hosted on the interface of the proxy mobile agent, where the mobile is attached. Thus the home agent is not required to perform any proxy ND operations [RFC-2461] for defending the home address on the home link. The home agent is required to manage a binding cache entry for managing the session state and a routing state for properly routing the packets destined to the mobile node.

5.1. Extensions to Binding Cache Conceptual Data Structure

The home agent maintains a Binding Cache entry for each currently registered mobile node. The Binding Cache is a conceptual data structure, described in Section 9.1 of [RFC3775]. For supporting this specification, the conceptual Binding Cache entry needs to be extended with the following new fields.

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

- A mobile identifier, NAI, for tagging the Binding Cache entry with a global identifier of the mobile. This field is set to the value set in the NAI option [RFC-4285].

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

- o The IPv4 Home Address of the mobile if the mobile is a dual-stack node and if it has obtained a IPv4 home address as part of the IPv4 address configuration.

5.2. Bi-Directional Tunnel Management

The bi-directional tunnel between the home agent and the proxy mobile agent is used for routing the traffic to and from the mobile node. The tunnel hides the topology and enables the mobile node to use an address that is topologically anchored at the home agent. The base Mobile IPv6 specification [RFC-3775], uses the tunneling mechanism for routing traffic to and from the mobile using its home address. However, there are subtle differences in the way Proxy Mobile IPv6 uses the tunneling scheme.

As in Mobile IPv4 [RFC-3344], the tunnel between the home agent and the proxy mobile agent is typically a shared tunnel and MAY be used for routing traffic streams for different mobiles attached to the same proxy mobile agent. This specification modifies the 1:1 relation between the tunnel and a binding cache entry to 1:m relation, reflecting the shared nature of the tunnel.

The source address of the tunnel MUST be the address that is used as the destination address for the Binding Update messages sent by the proxy mobile agent.

The home agent SHOULD use a Tunnel-Life timer for managing the tunnel life time. The timer value should be set to the accepted binding life time and must be updated after each periodic registration. The tunnel should be deleted after the expiry of the timer.

The home agent SHOULD maintain a tunnel-user-count counter for each managed tunnel and this counter should reflect the active mobiles sharing the tunnel. When the tunnel is being used for routing traffic to multiple mobiles attached to the same proxy mobile agent, the home agent MUST set the Tunnel-Life timer value to the highest binding life time across all the binding life time that is granted for all the mobiles sharing that tunnel.

Some implementations MAY choose to statically pre-establish the

tunnels between the home agent and the proxy mobile agent and with out having a need to create or tear down the tunnels dynamically on a need basis.

5.3. Routing Considerations

This section describes how the data traffic to/from the mobile node is handled at the home agent. The following entries explains the routing state at the home agent when supporting 1.) Per-MN-Prefix and 2.) Shared-Prefix addressing models. This section also covers the routing states when supporting IPv4 home address allocation support.

HAA - IPv6 global address that is configured on the home agent's interface and is the address to where the proxy mobile agent sent the binding update. This is one end-point of the tunnel.

CoA - IPv6 global address that is configured on the proxy mobile agent's egress interface and is the registered care-of address in the binding cache entry at the home agent. This is the remote end point of the tunnel.

HoP - The IPv6 home prefix of the mobile.

HoA - The IPv6 home address of the mobile. This is the IPv6 global address that the mobile obtained and configured on the remote MN-AR link from its home prefix (HoP).

HoA_v4 - The IPv4 home address of the mobile. This is the IPv4 address that the mobile obtained, when functioning in the dual-stack mode, and configured on the remote MN-AR link.

```
Per-MN-Prefix Addressing Model:
==============================
   HoP::/64 via tunnel0, next hop CoA

Shared-Prefix Addressing Model:
==============================
   HoA::/128 via tunnel0, next hop CoA

IPv4 Home Address support:
==========================
   HoA_v4/32 via tunnel0, next hop CoA

tunnel0:
========
   Source:      HAA
   Destination: CoA
   Tunnel Transport: IPv6
   Tunnel Payload: IPv4, IPv6
```

The home agent functions as an anchor point for the mobile node's home prefix. When the home agent receives a data packet from a corresponding node, destined for the mobile node's home address, the created routing state will forward the packet to the mobile node through the bi-directional tunnel established between itself and the serving proxy mobile agent. When the mobile is allocated a unique and exclusive home prefix, the home agent will forward all packets sent to that prefix through the tunnel to the proxy mobile agent, as the prefix is hosted on the proxy mobile agent.

All the reverse tunneled packets that the home agent receives from the tunnel, after removing the packet encapsulation will get routed to the destination specified in the inner packet header. These routed packets will have the source address field set to the mobile node's home address.

5.4. Dynamic Home Agent Address Discovery Considerations

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

The Proxy Mobile IPv6 model assumes that the home agent address information is pre-configured in the mobile's profile or it may

obtained through other means and all the network entities can obtain this information. It is important to note that there is little value in using DHAAD for discovering the home agent as the proxy mobile agents at different access routers will not predictably be able to locate the current serving home agent for a mobile. However, if there is only one home agent on the home link, the proxy mobile agent can use Dynamic Home Agent Address Discovery scheme for discovering the home agent address.

When the mobile is configured with a shared Shared-Prefix addressing model, the proxy mobile agent serving the mobile will be able to discover the mobile's home agent by sending the ICMP Home Agent Address Discovery Request message to the Mobile IPv6 Home-Agents anycast address derived from its home prefix. The home agent on the mobile's home link will receive these messages and will be able to reply to this message.

When the mobile is configured with a unique Per-MN-Prefix addressing model, the home agent is a topological anchor point for that prefix and with the prefix being hosted on the link attached to the proxy mobile agent. For the discovery scheme to work, the home agent MUST be able to receive the ICMP discovery packets sent to the anycast address derived from the mobile's home prefix.

5.5. Sequencing Number Considerations

Sequence number is typically used by two communication end points as a means to establish order of the exchanged packets. Mobile IPv6 uses the Sequence Number field in the registrations messages. The home agent and the mobile are required to manage this counter.

In Proxy Mobile IPv6, the Binding Update messages that the home agent receives on behalf of a specific mobile, may not be from the same proxy mobile agent and thus the sequence number value in these messages will have little meaning and the home agent will not be predictably order the messages and thus may end up processing an older message while ignoring the latest binding update message.

In the Proxy Mobile IP model, where the ordering of packets have to established when multiple senders are involved, sequence number scheme in the absence of time context transfers will not work. A global scale such as a time stamp is the right way to ensure order of packets. This document proposes the use of time stamp in all the Binding Update messages sent by proxy mobile agents. By leveraging NTP [RFC-1305] service, all the entities in the Proxy Mobile IP Network will be able to synchronize the clocks and a time stamp field

in the Binding Update message will enable the home agent to predictable identify the latest messages from a list of messages delivered in a out of order fashion.

The Proxy Mobile IP model, defined in this document requires the Binding Update messages sent by the proxy mobile agent to have the time stamp option. The home agent processing a proxy registration MUST ignore the sequence number field and SHOULD use the value from the Time Stamp option to establish ordering of the received Binding Update messages. If the home agent receives a Binding Update message with a invalid time stamp, the registration request MUST be rejected and a Binding Acknowledgement must be sent with the status "Invalid Time Stamp" and with the Time Stamp option.

5.6. IPv4 Home Address Mobility Support

The transition from IPv4 to IPv6 is a long process and during this period of transition, both the protocols will be enabled over the same infrastructure. It is reasonable to assume that the mobile node and the home agent are IPv4 and IPv6 enabled and further it is also reasonable to expect the same mobility infrastructure to provide IPv4 and IPv6 address mobility. The Proxy Mobile IPv6 scheme defined in this document allows the mobile node to obtain a IPv4 address and to roam in the network using the same address.

A mobile node attached to a proxy mobile agent, when it sends a DHCP request, the network will ensure it gets a IPv4 address from its home address prefix. The DHCP Relay Agent on the access router will tag the DHCP request from the mobile node with its home prefix hint and the DHCP server will allocate an address from that prefix. The proxy mobile agent will send this information in the option, IPv4 Home Network Prefix Option as part of the Binding Update message. Upon accepting the registration for the mobile from the proxy mobile agent, the home address will add IPv4 host route over the tunnel to the proxy mobile agent. Any IPv4 packets that the home agent receives from the corresponding node will be routed to the proxy mobile agent over the IPv6/IPv6 tunnel and any IPv4 packets that it receives over the tunnel will be routed after removing the tunnel header.

5.7. Route Optimizations Considerations

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

mobile node owns both the home address and care-of address.

In the Proxy Mobile IPv6 model, the mobile is not involved in any mobility related signaling and also it does not operate in the dual-address mode. Hence, the return routability procedure as defined in RFC-3775 is not applicable for the proxy model. This document does not address the Route Optimization problem and leaves this work item for future enhancements.

This specification further recommends that the home agent MUST drop all HoTI messages received from a home address that has corresponding Binding Cache entry with the proxy registration flag set.

5.8. Mobile Prefix Discovery Considerations

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

In Proxy Mobile IPv6 deployments, the mobile's home prefix information would be typically configured in the mobile's profile and so there is not much need for this dynamic nature of prefix discovery. Thus, this specification does not support Mobile Prefix Discovery.

5.9. Home Agent Operation Summary

After receiving a Proxy Binding Update request from a proxy mobile agent on behalf of a mobile node, the home agent must process the request as defined Section 10, of the base Mobile IPv6 specification [RFC-3775], with one exception that this request is a proxy request and proper authorization checks have to be enforced.

The home agent must use the NAI option present in the mobility header of the Binding Update message for identifying the mobile and for downloading the mobile's policy from the policy store. This policy will contain the mobile's address configuration model, home prefix, home address and other parameters.

The home agent has to verify the policy to ensure the proxy mobile agent that is sending this request has the right to do so, else it MUST reject the request and send a Proxy Binding Acknowledgment with the proper status code.

The home agent MUST ignore the sequence number field in the Binding Update for proxy registrations.

If the received Binding Update does not have a home network prefix option and if there is no Binding Cache entry for that mobile node, the home agent MUST reject the registration with HOME_ADDRESS_REQUIRED status code.

Upon accepting this request, the home agent must create a Binding Cache entry with the home address from the Home Network Prefix Option in the Binding Update and must set up a tunnel to the proxy mobile agent serving the mobile node. This bi-directional tunnel between the home agent and the proxy mobile agent is used for routing the mobile traffic.

For supporting this scheme, the home agent MUST satisfy all the requirements listed in Section 8.4 of [1]. The key differences of this scheme for the Per-MN-Prefix configuration mode, when compared to the base protocol is as follows:

The mobile node is not anchored on any physical interface on the home agent. Thus the home agent is not required to perform any proxy ND operations for defending the home address on the home link. The home agent is required to manage a binding cache entry for managing the session state and a routing state for properly routing the packets destined to the mobile node.

Each mobile node has a home address in a prefix that is created exclusively for that mobile node and no other mobile node will share its home address from this prefix.

The route entry specifying that the mobile node's home prefix is reachable via the tunnel is created as supposed to creating an route entry just for the mobile node's home address.

If multiple mobile stations are currently visiting the same proxy mobile agent, all the binding updates will share the same care-of address and possibly the same tunnel.

6. Proxy Mobile Agent Considerations

The Proxy Mobile IPv6 scheme introduces a new function, the Proxy Mobile Agent (PMA). It is a function that runs on the access router and is the entity that does the mobility related signaling on behalf of the mobile node.

From the perspective of the home agent, the proxy mobile agent is a

special element in the network that sends Mobile IPv6 signaling messages on behalf of a mobile station using its own identity. It is the entity that binds the mobile node's home address to an address on its own access interface.

The Proxy Mobile Agent has the following functional roles. It will emulate the mobile node's home network on the access link, will update the home agent about the current location of the mobile node and sets up a data path for enabling the mobile node to use its home address for communication from the access link.

This specification is independent of the underlying access technology or the link model. The interface between the mobile and the access router can be either:

- Point-to-Point Link
- Shared Link

This specification does not support split links. Also, it is to be noted that from the current deployment perspective, Point-to-Point link model appears to be the most common and required model.

6.1. Address Configuration Models

This specification supports the following address configuration models:

- Per-MN-Prefix Model
- Shared-Prefix Model

In the Per-MN-Prefix model, there is a unique home prefix assigned for each mobile node and that prefix is hosted on the access link. The prefix just follows the mobile. In this addressing model, based on the administrative policy, the mobile node can use either Stateless Address Autoconfiguration or Statefull Address Configuration using DHCP for obtaining the IPv6 address configuration for its interface on the access link. Further, the mobile can also generate interface identifiers with privacy considerations, as specified in [RFC-3041].

In the Shared-Prefix model, the prefix is a shared prefix and the mobile is not the only node using an address from that prefix block. In this addressing model, Stateless Address Autoconfiguration is not supported by this specification. The mobile is allowed to use only

Statefull Address Configuration using DHCP for obtaining the address configuration for its interface on the link.

The configured administrative policy for the mobile dictates the type of addressing model that is supported for a mobile on the access link. The proxy mobile agent on the access router will control this by setting the relevant flags in the Router Advertisement accordingly.

6.2. Access Authentication

Access authentication is outside scope of this document. This specification does not deal with the access link security and further assumes that there are proper authorization models in place for ensuring only authorized nodes with their respective identities are able to access the link.

Access authentication on any wireless access link, ensures a node with a given MAC address and an Identifier such as NAI, is authorized to use the link and the Layer-2 security ensures that. This specification assumes such security mechanisms are in place.

6.3. Home Network Emulation

One of the key functions of the proxy mobile agent is to emulate the mobile's home network on the access link. It has to ensure, the mobile believes it is on its home link. After the access authentication, the proxy mobile agent can obtain the mobile's profile and from that it has to send the Router Advertisements to the mobile advertising its home prefix and other parameters. Further if the mobile uses statefull Address Configuration mode such as DHCP, the proxy mobile agent or the DHCP Relay Agent [RFC-3315], MUST set the link-address field of the DHCP request to the mobile's home network prefix and the DHCP server will allocate an address from that prefix block, as specified in Section 20.1.1 of [RFC-3315].

If the access link is a point-to-point link, the advertisements from the proxy mobile agent on that link are not seen by any other mobile stations. However, if the access link is a shared link, the proxy mobile agent has to ensure that each of the mobile node that is attached to that link receive only their home prefixes as the on-link prefixes. For this to happen, the proxy mobile agent MUST unicast the Router Advertisement to the mobile node. The destination field of the Layer-2 header in the Router Advertisement MUST be the mobile's node's MAC address and however, the destination field in the IPv6 header can be the all-nodes-multicast address.

6.4. Link-Local and Global Address Uniqueness

On a point-to-point link, when the mobile tries to establish a PPP session [RFC-1661] with the access router, the PPP goes through the Network layer Protocol phase and the IPv6 Control Protocol, IPCP6 [RFC-2472] gets triggered. Both the PPP peers negotiate a unique identifier using Interface-Identifier option in IPV6CP and the negotiated identifier is used for generating a unique link-local address on that link. Now, if the mobile moves to a new access router, the PPP session gets torn down and new PPP session with the new access router will be established and the mobile obtains a new link-local address. Now, even if the mobile is DNAv6 capable, as specified in [draft-ietf-dna-protocol-03], the mobile still configures a new link-local address when ever it moves to a new link.

However, if the link between the mobile node and the access router is a shared link and if a DNAv6 capable mobile moves from access network to the other, the mobile may not detect link change due to DNAv6 (how ever this really depends on the wireless technology in use), detecting the same link and there is a remote possibility for the link local address collision on the new link. One of the work around for this issue to the set following flag on the mobile, DNASameLinkDADFlag to TRUE and that will force the mobile to redo DAD operation even when the DNAv6 detected no link change.

For the global address or the home address uniqueness, the home agent will not accept a Binding Update from a mobile, identified by a NAI, for a home address that is already registered for some other mobile station. Further, if the address configuration is based on statefull Address Configuration using DHCP, the DHCP server will ensure the uniqueness.

6.5. IPv4 Home Address Mobility Support

If the mobile node is permitted to roam using a IPv4 home address and if the mobile has a dual-stack, the mobile can send a DHCP request and can obtain the IPv4 address configuration for its interface. As part of this configuration, the mobile node will obtain a IPv4 address, subnet address, subnet mask and default-router address. The relay agent service on the access router will ensure the mobile node is assigned an address from its home prefix, by marking the DHCP request with the prefix hint.

However, the default-router address that is obtained from the DHCP will be that of a router on its home link and the mobile node is on the access link. In order for the mobile node to be able use the default router for routing all IPv4 packets, the proxy mobile agent

on the access link must respond to the ARP requests from the mobile node for the default-router's IPv4 address. Now, if the mobile roams to a new link, the proxy mobile agent on that link must send a gratuitous ARP for the mobile's default-router address.

In IPv6, the nodes on the link use the link-local address of the default router for routing packets and it is not required that the default router needs to have a configured address from the prefix that the node uses. However, in IPv4, the default-router address on the link must be from the same subnet as of the IP address of the node. Since, the proxy mobile agent will not have an address on the mobile's home prefix, it must act as a proxy for the mobile router's IPv4 gateway address.

6.6. Tunnel Management

In the traditional Mobile IPv6 model, there is a separate tunnel from the home agent to every mobile node that has a binding entry. The tunnel end-point of each these tunnels is the respective mobile node's care-of address and that is unique to that mobile node. In the case of Proxy Mobile IPv6, the care-of address or the tunnel end-point is the address of the proxy mobile agent and there could be multiple mobile stations attached to the same proxy mobile agent and hence the tunnel is a shared tunnel serving multiple mobile stations. This is identical to the Mobile IPv4 model [RFC-3344], where a tunnel between the foreign agent and the home agent is shared by many visiting mobile nodes.

The life of the Proxy Mobile IP tunnel should not be based on a single binding cache entry. The tunnel may get created as part of creating a mobility binding for a mobile node and later the same tunnel may be associated with other binding entries. So, the tearing down logic of the tunnel must be based on the number of visitors over that tunnel. Implementations are free to pre-establish tunnels between every home agent and every proxy mobile node in the network and with out creating and destroying the tunnels on a need basis.

6.7. Routing Considerations

This section describes how the data traffic to/from the mobile node is handled at the proxy mobile agent. The following entries explains the routing state at the proxy mobile agent.

HAA - IPv6 global address that is configured on the home agent's interface and is the address to where the proxy mobile agent sent the binding update. This is one end-point of the tunnel.

CoA - IPv6 global address that is configured on the proxy mobile agent's egress interface and is the registered care-of address in the binding cache entry at the home agent. This is the remote end point of the tunnel.

HoP - The IPv6 home prefix of the mobile.

HoA - The IPv6 home address of the mobile. This is the IPv6 global address that the mobile obtained and configured on the remote MN-AR link from its home prefix (HoP).

HoA_v4 - The IPv4 home address of the mobile. This is the IPv4 address that the mobile obtained, when functioning in the dual-stack mode, and configured on the remote MN-AR link.

```
Per-MN-Prefix Addressing Model:
==============================
For all traffic from the source address HoA to
   0::/0 route via tunnel0, next hop HAA

HoA::/64 is on the interface locally connected

Shared-Prefix Addressing Model:
==============================
For all traffic from the source prefix HoA::/64 to
   0::/0 route via tunnel0, next hop HAA

HoA::/128 is on the interface locally connected

IPv4 Home Address support:
=========================
For all IPv4 traffic from the source address HoA_v4 to
   0.0.0.0/0.0.0.0 route via tunnel0, next hop HAA

HoA_v4/32 is on the interface locally connected

tunnel0:
========
   Source:      CoA
   Destination: HAA
   Tunnel Transport: IPv6
```

Tunnel Payload: IPv4, IPv6

When the proxy mobile agent receives any packets from the mobile station to any destination, the packet will be forwarded to the home agent through the bi-directional tunnel established between itself and the mobile's home agent. However, the packets that are sent with link-local source address are not forwarded.

All the packets that the proxy mobile agent receives from the tunnel, after removing the tunnel encapsulation, will get forwarded to the mobile node on the connected interface.

6.8. Interaction with DHCP Relay Agent

If Statefull Address Configuration using DHCP is supported on the access link, the DHCP Relay Agent [RFC-3315] needs to be configured on the access router. When the mobile stations sends a DHCP Request, the relay agent function on the access router must set the link-address field in the DHCP message to the mobile node's home prefix, so as to provide a prefix hint to the DHCP Server. On a point-to-point link, this is just a normal DHCP relay agent configuration. However, on the shared links supporting multiple mobile stations with different home prefixes, there is some interaction required between the relay agent and the proxy mobile agent, for setting the link-address field to the requesting mobile node's home prefix. The proxy mobile agent should also have the ability to learn the DHCP assigned address to the mobile station.

If the mobile is permitted to roam using IPv4 home address, the DHCPv4 relay agent service [RFC-2131] needs to be configured on that link. Further, the giaddr field in the request packet must be set to the mobile node's IPv4 home prefix.

6.9. Coexistence of CMIP & PMIP Nodes

In some operating environments, network operators may want to provision a particular link attached to an access router running proxy mobile agent for supporting nodes using Mobile IP signaling and the nodes that depend on the network for doing the Mobile IP signaling for achieving network mobility. This specification supports links with such mixture of nodes.

Upon obtaining the mobile node's profile after a successful access authentication and after a policy consideration, the proxy mobile agent MUST determine if the network based mobility service should be

offered to that mobile node. If the mobile is entitled for such service, then the network should ensure the mobile believes it is on its home link, as explained in various sections of this document.

If the mobile is not entitled for the network based mobility service, the proxy mobile agent MUST ensure the mobile can obtain an IPv6 care-of address using normal IPv6 address configuration mechanisms. The obtained address should be from a local visitor network prefix. In other words the mobile should be able to operate as a traditional mobile node roaming in a visitor network and with the ability to obtain a care-of address from the local visitor network prefix hosted on that link.

If the stateless address configuration mode is supported on that link, the prefix information option in the router advertisements should contain local visitor network prefix. If statefull address configuration mode is enforced on the link and if DHCP is in used, the mobile should obtain the IPv6 or IPv4 care-of address from the local visitor network prefix.

If the link between the access router and the mobile node is a shared link, the Router Advertisement has to unicasted to the mobile station with the destination address in the layer-2 header set to the mobile's MAC address and the destination address in the IPv6 header set to the all-nodes multicast address.

6.10. Proxy Mobile Agent Operation Summary

After detecting a new mobile node on its access link and after a successful access authentication, the proxy mobile agent using the mobile's identifier will obtain the mobile's profiles from the policy store. The mobile's policy can also be pushed to the proxy mobile agent using context transfer procedure. Context Transfer is out of scope for this current specification. The mobile's profile contains the mobile node's home agent address, home prefix, addressing model, permitted address configuration mechanisms and other parameters that are needed to emulate the mobile's home network on the access network.

The proxy mobile agent constructs a Router Advertisement containing the mobile's home prefix and it will send it to the mobile node. If the link between the mobile node and the access router is a shared link, then the Router Advertisement will be unicasted to the mobile station by setting the destination address in the layer-2 header to the mobile's MAC address and the destination address in the IPv6 header set to the all-nodes multicast address.

The proxy mobile agent sends a Proxy Binding Update to the home agent. The source address of this message will be the configured IPv6 address on the egress interface. The contents of the message include the Mobile Node NAI Option, Home Network Prefix Option, IPv4 Home Address Option and Time Stamp Option. This message will be protected by using IPSec security association created between the proxy mobile agent and home agent.

If the mobile is configured for the Per-MN-Prefix model, the proxy mobile agent will set the Home Network Prefix Option to the mobile's home network that is learnt from the mobile's profile. The home agent sets up a route for the whole prefix and there is no MUST requirement that the mobile's home address is associated in the BCE at the home agent. However, if the proxy mobile agent predictably learns the address that the mobile is using from its home prefix, it is recommended that the Home Network Prefix Option be set with the specific home address, so that the Binding Cache entry on the home agent will have a reachable address for the mobile.

If the mobile is configured for Per-MN-Address model, the proxy mobile agent must set the Home Network Prefix Option to the DHCP assigned address for that mobile. It is possible, the mobile is DNAv6 capable and after attaching to a new link, it never initiates a DHCP request. In that situation, the proxy mobile agent must send the Binding Update with out the Home Network Prefix option and the home agent will send the mobile's home address in Binding Acknowledgement message, if there is a Binding Cache entry for that mobile, else it will reject the Binding Update and the proxy mobile agent must wait till the mobile triggers the DHCP for address configuration.

After receiving a Proxy Binding Acknowledgment with the status code indicating the acceptance of the Binding Acknowledgment, the proxy mobile agent MUST setup a tunnel to the home agent, as explained in the above sections.

If the home agent denies the Proxy Binding Update request, the proxy mobile agent MUST NOT advertise the mobile node's home prefix on the link and there by denying the mobility service to the mobile station.

At any point, if the proxy mobile agent detects that the mobile node has roamed away from its home link, it MUST send a Binding Update to the home agent with the lifetime value of 0 and it must remove the route over the tunnel for that mobile and also delete the tunnel if no other mobile traffic route is setup over that tunnel.

6.11. Conceptual Data Structures

Every proxy mobile agent maintains a Binding Update List for each currently registered visitor. The Binding Update List is a conceptual data structure, described in Section 11.1 [RFC-3775]. For supporting this specification, the conceptual Binding Update List must be extended with the following new fields.

- The Identifier of the mobile node in the form of NAI. This is obtained as part of the Access Authentication procedure. This identifier is required for downloading the mobile node's profile from the policy store.
- A flag specifying whether or not the configured addressing model for the mobile is Per-MN-Prefix model. If the flag is not set, indicates the configured addressing model is a Shared-Prefix model.
- The link-local address of the mobile node on the link. This address is learned through the Source Address of the Router Solicitation messages received from the mobile node on the link.
- The IPv4 home address of the mobile, if IPv4 home address mobility is supported.
- The IPv4 home network prefix length of the mobile, if IPv4 home address mobility is supported.
- The IPv4 default router address of the mobile, if IPv4 home address mobility is supported. This is the address that is configured on the home agent.

7. Mobile Node Considerations

The Proxy Mobile IPv6 scheme, defined in this document, enables a mobile node to achieve network mobility with out requiring its participation in any mobility related signaling. The specification assumes the mobile node is a IPv6 host, and optionally IPv4 capable, if it is operating as a dual-stack node.

Once the mobile enters a Proxy Mobile IPv6 domain and attaches to an access network, the network identifies the mobile as part of the access authentication procedure and ensures the mobile using any of

the address configuration mechanisms permitted by the network for that mobile, will be able to obtain an address and move anywhere in that managed domain. From the perspective of the mobile, the entire Proxy Mobile IPv6 domain appears as a single link, the network ensures the mobile believes it is always on its home link. If the mobile is Mobile IPv6 client, as per [RFC-3775], the mobile will not detect movement and hence it will not trigger the Mobile IPv6 registrations.

7.1. Booting in the Proxy Mobile IPv6 Network

When the mobile node attaches to a link on the access router running proxy mobile agent, it will present its identity to the network in the form of NAI as part of the access authentication procedure. After performing the required access authentication procedures, the network knows the mobile's home prefix, address configuration models and other parameters.

After a successful access authentication, the mobile node will send a Router Solicitation message. The proxy mobile agent on the link will respond to the Router Solicitation message with a Router Advertisement. The Router Advertisement will have the mobile node's home prefix, default router and other address configuration parameters. The address configuration parameters such as Managed Address Configuration, statefull Configuration flag values will be consistent with the home link policy.

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

If the Router Advertisement does not have the Managed Address Configuration flag set, the mobile node can autoconfigure itself by appending its link-layer address (EUI-64 format) to the advertised local home network prefix or it can configure an address per [RFC-3041] specification.

Once the address configuration is complete, the mobile node will always be able to use that IPv6/IPv4 address anywhere with in that managed network where proxy mobile agents are deployed. Further, the mobile node will always get the same Address even after a reboot.

7.2. Roaming in the Proxy Mobile IPv6 Network

After booting in the network and obtaining a IPv6 and possibly IPv4 address as well (if the network supports dual-stack mode), the mobile when it moves from one access network to the other in that Proxy Mobile IP domain, will always detect its home link, home prefix and obtains the same IPv6/IPv4 address, if it uses DHCP for address configuration. However, the mobile always detects a new default-router on the new link advertising its home prefix and with a different link-local address. Any Router Solicitation messages from the mobile node will result in a Router Advertisement advertising its home prefix, default router and other configuration parameters consistent with the home link properties.

7.3. IPv6 Host Protocol Parameters

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

Lower Default Router List Cache Time-out:

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

In the Proxy IPv6 scenario, when the mobile node moves from one link to another, the received Router Advertisement messages advertising the mobile's home prefix on the new access link are from a different link-local address and thus making the mobile believe that there is a new default router on the link. It is important that the mobile node uses the newly learnt default router as supposed to the previous learnt default router. The mobile node must update its default-router list with the new default router entry and must age out the previously default router entry from its cache, just as specified in

Section 6.3.5 of the base IPv6 ND specification [1]. This action is critical for minimizing packet losses during a hand off switch.

On detecting a reachability problem, the mobile node will certainly detect the neighbor or the default router unreachability by performing a Neighbor Unreachability Detection procedure, but it is important that the mobile node times out the previous default router entry at the earliest. If a given IPv6 host implementation has the provision to adjust these flush timers, still conforming to the base IPv6 ND specification, it is desirable to keep the flush-timers to suit the above consideration.

However, if the proxy mobile agent has the ability to with draw the previous router entry, by multicasting a Router Advertisement using the link-local address that of the previous mobility proxy agent and with the Router Lifetime field set to zero, then it is possible to force the flush out of the Previous Default Router entry from the mobile node's cache. This certainly requires the proxy mobile agent to notify its link-local address to the home agent as part of the binding update and the home agent to associate this opaque data with the binding cache entry so that a new proxy mobile agent can learn the link-local address of the previous router and send a Router Advertisement with that link-local address.

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

8. Message Formats

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

8.1. Proxy Binding Update

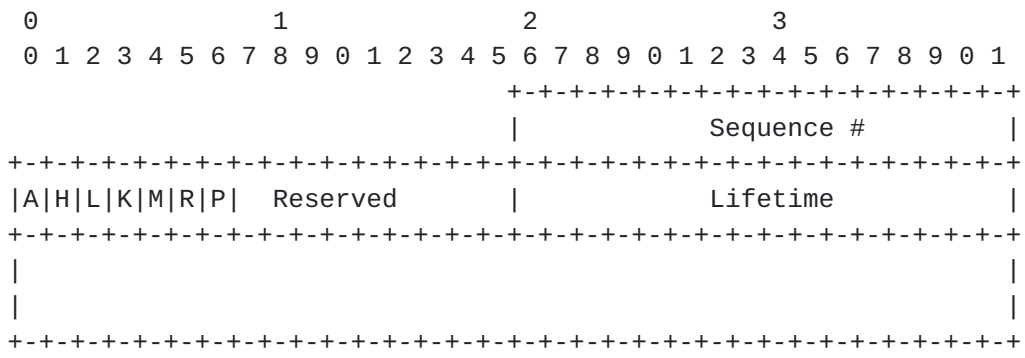


Figure 8: Proxy Binding Update Message

A new flag, the 'P' flag, is added to the Binding Update message [RFC-3775]. The 'P' flag indicates that the registration is a Proxy Registration. When a proxy mobile agent sends a registration to the home agent, the P flag MUST be set to value of 1, to indicate to the home agent that this registration is a proxy registration sent by a proxy mobile agent on behalf of a mobile node.

For descriptions of other fields present in this message, refer to [RFC3775].

A Binding Update message that is sent by proxy mobile agent is also referred to as "Proxy Binding Update".

8.2. Proxy Binding Acknowledgment

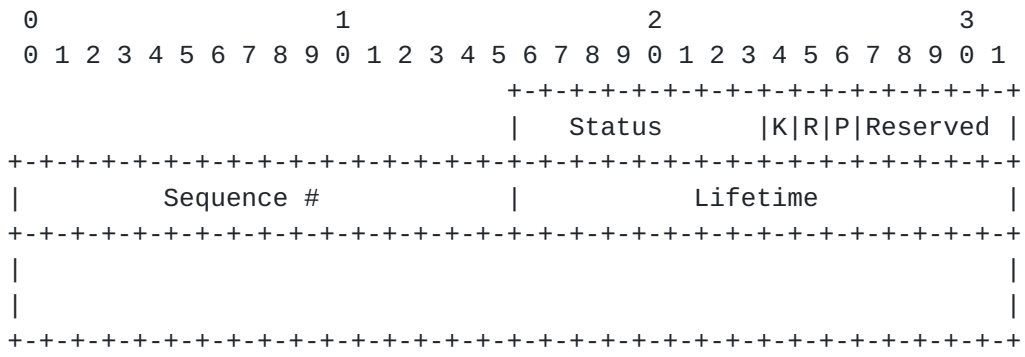


Figure 9: Proxy Binding Acknowledgment Message

Proxy Registration Flag (P)

A new flag, the 'P' flag, is added to the Binding Acknowledgement message [RFC-3775]. The Proxy Registration Flag is set to a value of 1, to indicate that the home agent that processed the Proxy Binding Update supports Proxy Registration. This flag value is set only if the corresponding Proxy Binding Update had the Proxy Registration Flag set.

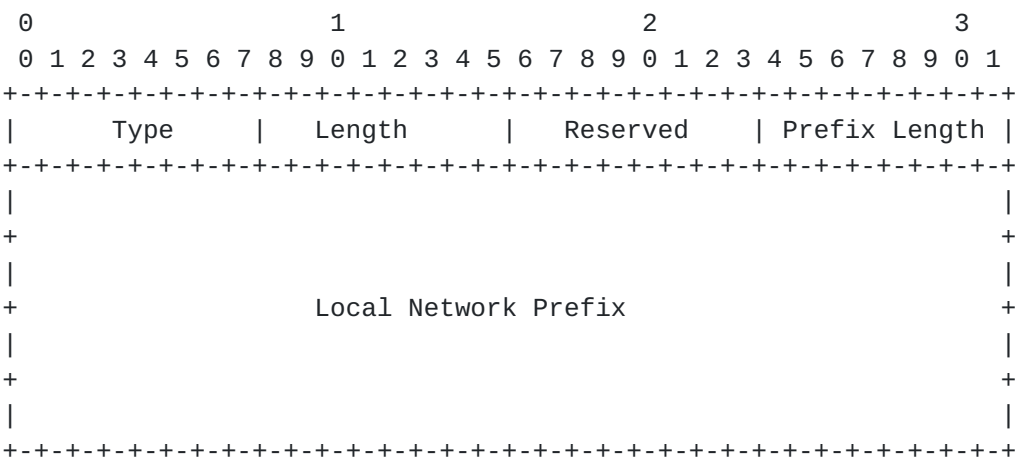
For descriptions of other fields present in this message, refer to [RFC3775].

A Binding Acknowledgment message that is sent by proxy mobile agent is also referred to as "Proxy Binding Acknowledgement".

8.3. Home Network Prefix Option

A new option, Home Network Prefix Option is defined for using it in the Proxy Binding Update and Acknowledgment messages exchanged between the home agent to the proxy mobile agent. This option can be used for exchanging the mobile node's home prefix and home address information.

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



Type
<IANA>

Length

Eight-bit unsigned integer indicating the length in octets of the option, excluding the type and length fields. Set to 18.

Reserved

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

Prefix Length

Eight-bit unsigned integer indicating the prefix length of the IPv6 prefix contained in the option. If the prefix length is set to the value 128, indicates the presence of the mobile's home address.

Home Network Prefix

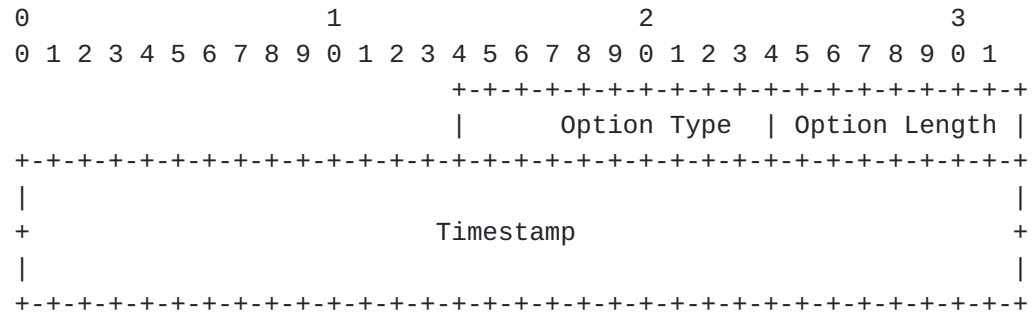
A sixteen-byte field containing the Home Network Prefix

Figure 10: Home Network Prefix Option

8.4. Time Stamp Option

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

all Proxy Binding Update and Acknowledgement messages.



Type
<IANA>

Length

Eight-bit unsigned integer indicating the length in octets of the option, excluding the type and length fields. Set to 18.

Timestamp

64bit time stamp

Figure 11: Time Stamp Option

8.5. Status Codes

Binding Acknowledgment Status Values

The following status code values are defined for using them in the Binding Acknowledgment message when using PMIPv6 protocol.

145: Proxy Registration not supported by the home agent

146: Proxy Registrations from this proxy mobile agent not allowed

147: No home address for this NAI is configured and the Home Network Prefix Option not present in the Binding Update.

148: Invalid Time Stamp Option in the Binding Update

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

The value allocation for this usage needs to be approved by the IANA and must be updated in the IANA registry.

9. IANA Considerations

This document defines a new Mobility Header Option, the Mobile Home Network Prefix Option. This option is described in Section 8.3. The Type value for this option needs to be assigned from the same numbering space as allocated for the other mobility options defined in [RFC-3775].

This document defines a new Mobility Header Option, the Time Stamp Option. This option is described in Section 8.4. The type value for this option needs to be assigned from the same numbering space as allocated for the other mobility options defined in [RFC-3775].

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

10. Security Considerations

The Mobile IPv6 base specification [RFC-3775] requires the signaling messages between the home agent and the mobile node to be secured by the use of IPsec extension headers.

This document introduces a new functional entity, proxy mobile agent, a function that will be implemented in the access routers. This entity is responsible for performing the Mobile IPv6 signaling on behalf of the mobile node, also called as Proxy Mobile IPv6 Signaling.

All signaling messages between the Proxy Mobile Agent and the Home Agent MUST be authenticated by IPsec [RFC-4301]. The use of IPsec to protect Mobile IPv6 signaling messages is described in detail in the HA-MN IPsec specification [RFC-3776]. The signaling messages described in this document just extend Mobile IPv6 messages and just requires some subtle changes to what is described in the HA-MN IPSec

specification.

As described in the base Mobile IPv6 specification [RFC-3775], Section 5.1 both the mobile client (in this case, its the proxy mobile agent) and the home agent MUST support and SHOULD use the Encapsulating Security Payload (ESP) header in transport mode and MUST use a non-NULL payload authentication algorithm to provide data origin authentication, data integrity and optional anti-replay protection.

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

The proxy solution allows one device creating a routing state for some other device at the home agent. It is important that the home agent has proper authorization services in place to ensure a given proxy mobile agent is permitted to be a proxy for a specific mobile node. If proper security checks are not in place, a malicious node may be able to hijack a session or may do a denial-of-service attacks.

11. Acknowledgements

The authors would like to thank Julien Laganier, Alex Petrescu, Brian Haley, Ahmad Muhanna, Mohamed Khalil, Fred Templing, Nishida Katsutoshi, James Kempf, Vidya Narayanan, Henrik Levkowetz, Phil Roberts, Jari Arkko, Ashutosh Dutta, Hesham Soliman and many others for their passionate discussions in the working group mailing list on the topic of Proxy Mobile IPv6 and NETLMM. These discussions stimulated much of the thinking and shaped the draft to the current form. We acknowledge that ! The authors would also like to thank Ole Troan, Akiko Hattori and Perviz Yegani for their input on this document.

12. References

12.1. Normative References

[RFC1305] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, March 1992.

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

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

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

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

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

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

[RFC-3776] Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

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

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

[RFC-4303] Kent, S. "IP Encapsulating Security Protocol (ESP)", RFC 2406, December 2005.

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

[draft-ietf-netlmm-nohost-req-05.txt] Kempf, J., Leung, K., Roberts, P., Nishida, K., Giaretta, G., Liebsch, M., "Goals for Network-based Localized Mobility Management", October 2006.

[draft-ietf-netlmm-nohost-ps-05.txt] Kempf, J., Leung, K., Roberts, P., Nishida, K., Giaretta, G., Liebsch, M., "Problem Statement for

Network-based Localized Mobility Management", September 2006.

[draft-ietf-netlmm-threats-04.txt] Vogt, C., Kempf, J., "Security Threats to Network-Based Localized Mobility Management", September 2006.

12.2. Informative References

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

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

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

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

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

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

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

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

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

Authors' Addresses

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

Email: sgundave@cisco.com

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

Email: kleung@cisco.com

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

Email: vijay.devarapalli@azairenet.com

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury, MA

Email: kchowdhury@starentnetworks.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.