NETLMM Working Group R. Wakikawa
(Editor)
Internet-Draft Keio
University
Intended status: Standards Track S.
Gundavelli
Expires: November 23, 2008
Cisco

May 22,
2008

IPv4 Support for Proxy Mobile IPv6
draft-ietf-netlmm-pmip6-ipv4-support-03.txt

Status of this Memo

Copyright Notice

Abstract

This document specifies extensions to Proxy Mobile IPv6 protocol for supporting IPv4 protocol. The scope of this IPv4 support includes the support for the mobile node's IPv4 home address mobility and for allowing the mobility entities in the Proxy Mobile IPv6 domain to exchange signaling messages over an IPv4 transport.

Table of Contents

1. Overview

The transition from IPv4 to IPv6 is a long process and during this period of transition, both the protocols will be enabled over the same network infrastructure. Thus, it is reasonable to assume that a mobile node in a Proxy Mobile IPv6 domain may operate in an IPv4-only IPv6-only or in dual-stack mode and additionally the network between the mobile access gateway and a local mobility anchor may be an IPv4 or an IPv6 network. It is also reasonable to expect the same mobility infrastructure in a Proxy Mobile IPv6 domain to provide mobility to the mobile nodes operating in IPv4, IPv6 or in dual mode and when the network between the local mobility anchor and the mobile access gateway is an IPv4 or an IPv6 network. The motivation and scope of IPv4 support in Mobile IPv6 is summarized in [RFC-4977] and all those requirements apply to Proxy Mobile IPv6 protocol as well.

The Proxy Mobile IPv6 protocol[ID-PMIP6] specifies a mechanism for providing IPv6 home address mobility support to a mobile node in a Proxy Mobile IPv6 domain and when there is an IPv6 transport network separating the entities involved in the mobility management. The extensions defined in this document are for extending IPv4 support to the Proxy Mobile IPv6 protocol [ID-PMIP6].

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

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

- IPv4 Transport Network Support: The mobility entities in the Proxy Mobile IPv6 domain will be able to exchange Proxy Mobile IPv6 signaling messages over an IPv4 transport and further the local mobility anchor or the mobile access gateway may be using IPv4 private addresses and with NAT [RFC-3022] translation devices separating them.

The DSMIPv6 specification [ID-DSMIP6], defines IPv4 home address mobility and IPv4 transport support to the Mobile IPv6 protocol [RFC-3775]. The solution specified in this document leverages some of the options related to IPv4 support and some processing logic for

extending IPv4 support to Proxy Mobile IPv6 protocol. These two features, the IPv4 Home Address Mobility support and IPv4 transport support features, are independent of each other and deployments can choose to enable any one or both of these features.

Figure 1 illustrates a Proxy Mobile IPv6 domain supporting IPv4 home address mobility and IPv4 transport support features. The mobile nodes MN1, MN2 and MN3 can be operating in IPv4-only, IPv6-only or dual-stack mode, and the transport network between the local mobility anchor and the mobile access gateway may be an IPv6 network or an IPv4 network. Further, when the transport network is IPv4, either the local mobility anchor or the mobile access gateway, or both can be behind a NAT [RFC-3022] translation device and configured with an IPv4 private address.

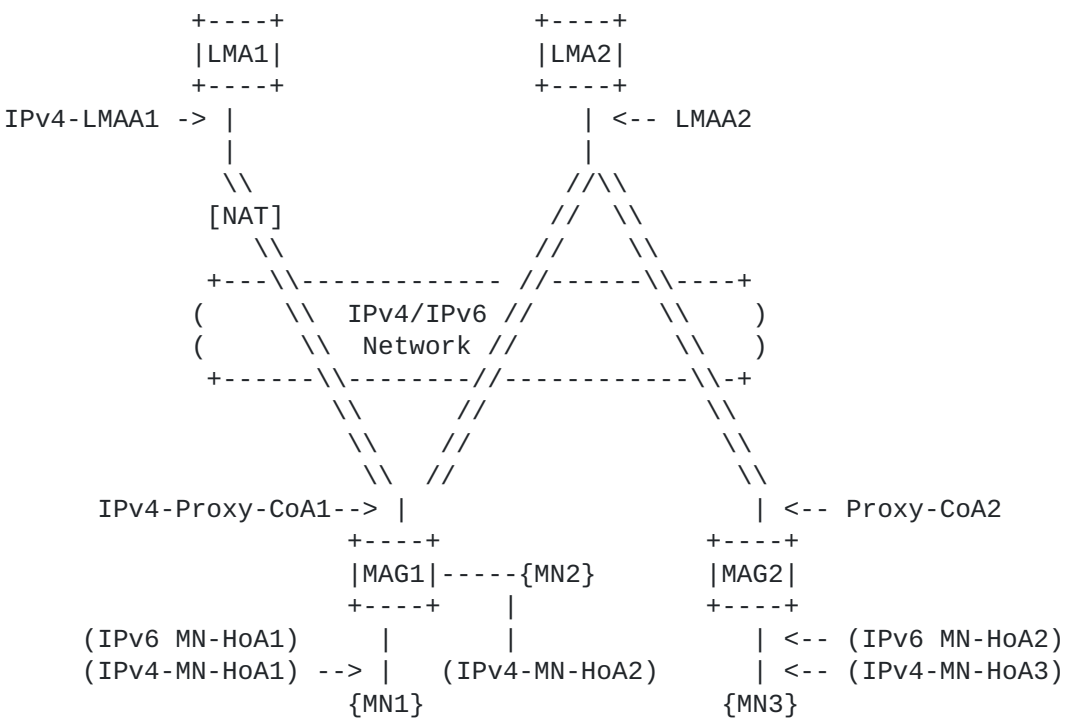


Figure 1: IPv4 support for Proxy Mobile IPv6

1.1. Stated Assumptions

o This specification requires that the local mobility anchor and the mobile access gateway are both IPv6 capable and IPv6 enabled. Irrespective of the type of transport network (IPv4 or IPv6) separating these two entities (i.e., if the entities are reachable using an IPv4 or IPv6 transport address), the mobility signaling is always based on Proxy Mobile IPv6.

- For supporting IPv4/IPv6 home address mobility, the transport network between the local mobility anchor and the mobile access gateway can be an IPv6 network or an IPv4 network. However, for supporting IPv4 transport network feature, as implied, IPv4 transport network is required.

- The mobile node can be operating in IPv4-only, IPv6-only or in dual mode. If enabled, the mobile node should be able to obtain IPv4-only, IPv6-only or both IPv4 and IPv6 address(es) on its interface. However, the respective protocol(s) support must be enabled on the access link between the mobile node and the mobile access gateway.

- There can be support for multiple IPv4 home network prefixes for the mobile node's attached interface. The mobile node should be able to obtain one or more IPv4 addresses from one or all of its IPv4 home network prefixes. Based on the type of link, it may be able to acquire its IPv4 address configuration using DHCP, IPCP, IKEv2 or through other standard address configuration mechanisms.

- The mobile node's IPv4 home network prefix is a shared prefix (unlike its IPv6 home network prefix, which is a shared prefix). There can be more than one mobile node sharing address(es) from the same IPv4 home network prefix.

- The mobile access gateway is always the IPv4 default-router for the mobile node on its access link. It will always be able to receive traffic sent to the mobile node's IPv4 default-router address.

2. Conventions & Terminology

2.1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC-2119].

2.2. Terminology

All the mobility related terms used in this document are to be interpreted as defined in Mobile IPv6 specification [RFC-3775] and Proxy Mobile IPv6 specification [ID-PMIP6]. In addition the document introduces the following terms.

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

The IPv4 address that is configured on the interface of the mobile access gateway and is the transport endpoint of the tunnel between a local mobility anchor and a mobile access gateway. This address will be used as the source address for the signaling messages sent by the mobile access gateway to the local mobility anchor and will be the registered Care-of address in the mobile node's Binding Cache entry. However, when the configured address is a private IPv4 address and with a NAT device in the path to the local mobility anchor, the care-of address as seen by the local mobility anchor will be the address allocated by the NAT device for that flow.

IPv4 Local Mobility Anchor Address (IPv4-LMAA)

The IPv4 address that is configured on the interface of a local mobility anchor and is the transport endpoint of the tunnel between the local mobility anchor and the mobile access gateway. This is the address to where the mobile access gateway sends the Proxy Binding Update messages when using IPv4 transport. If the local mobility anchor is configured to be behind a NAT device, this address will not be directly configured on the local mobility anchor, but a corresponding mapped private address will be configured on the local mobility anchor.

Mobile Node's IPv4 Home Network Prefix (IPv4-MN-HNP)

This is the IPv4 prefix from which the mobile node obtains its

home address(es). This IPv4 home network prefix is topologically anchored at the mobile node's local mobility anchor. The mobile node configures its interface with address(es) from this prefix.

3. IPv4 Home Address Mobility Support

An IPv4 enabled mobile node when it attaches to the Proxy Mobile IPv6 domain, the network will ensure the mobile node will be able to obtain an IPv4 address (IPv4-MN-HoA) from its home network prefix for the interface attached to the access network in that Proxy Mobile IPv6 domain. Using the extensions defined in this specification, the mobile access gateway on the access network will exchange the signaling messages with the mobile node's local mobility anchor and will setup the required routing state for that home address.

If the mobile node connects to the Proxy Mobile IPv6 domain, through multiple interfaces and simultaneously through different access networks, each of the connected interfaces will obtain an address from a unique IPv4 home network prefix. In such configuration, there will be multiple Binding Cache entries on the local mobility anchor for that mobile node and with one entry for each connected interface, as specified in Section 5.4 [ID-PMIP6].

The support for IPv4 addressing is orthogonal to the IPv6 addressing support. Unlike as specified in [ID-DSMIP6], the mobile node is not required to have an IPv6 home address for obtaining IPv4 home address mobility. A mobile node attached to an access link in a Proxy Mobile IPv6 domain will be able to obtain just an IPv4 address configuration or both IPv4 and IPv6 address configurations on the connected interface. The mobile nodes' policy profile will determine if the mobile node is entitled for both the protocols or a single protocol and based on what is enabled, only those protocols will be enabled on the access link. Further, when the mobile node after obtaining the IPv4 or IPv4/IPv6 address configuration on the access link, performs an inter-technology handoff, the network will ensure the mobile node will be able to use the same IPv4/IPv6 address configuration on the new interface. [RYUJI The IPv4 home address MUST be the global IPv4 address. A private IPv4 address assignment as an IPv4 home address is prohibited. There is no gurantee to assign the IPv4 private home address which is different from the private address configured at a mobile access gateway.]

3.1. IPv4 Home Address Assignment

A mobile node on attaching to an access link connected to a mobile access gateway, and if the network allows the mobile node for IPv4 home address mobility service, the mobile node using any of the IPv4

address configuration procedures, such as DHCP [RFC-2131], IPCP or IKEv2 that are supported on that access link, will be able to obtain required information for its IPv4 home address configuration. The required information includes the IPv4 home address, the IPv4 home network prefix, IPv4 home network prefix length and the IPv4 default

router address.

When a mobile node is configured with a static IPv4 home address, the IPv4 home address information SHOULD be stored in the mobile node's policy profile. The mobile access gateway where the mobile node attached obtains the static IPv4 home address from the policy profile. The mobile access gateway MUST use either the obtained IPv4 home address or the obtained IPv4 home subnet address to initialize the IPv4 Home Address and Pref fields in the IPv4 Home Address option [ID-DSMIP6]. This option is carried by a proxy binding update described in [ID-PMIP6].

On the other hand, if DHCP is used for the IPv4 home address allocation as specified in [RFC-2131], a DHCP server and/or a DHCP relay agent on the link will ensure the mobile node is assigned an IPv4 address from its home network subnet. All the IPv4 home addresses assigned to mobile nodes must be reachable via local mobility anchor so that local mobility anchor intercepts packets meant for an IPv4 home address and tunnels them to the mobile node via corresponding mobile access gateway. There are several configurations where the DHCP entities are located in a Proxy Mobile IPv6 domain. This document recommends following two configurations. The other configurations are explained in Appendix A.

1. DHCP server is co-located with each mobile access gateway

2. DHCP server is co-located with a local mobility anchor and a DHCP relay is co-located with each mobile access gateway

Figure 2 shows the operational sequence of the home address assignment when a DHCP server is co-located with each mobile access gateway. In this scenario, a DHCP server which is also a mobile access gateway interacts with a DHCP client on a mobile node. All mobile access gateways SHOULD support minimal functionality of a DHCP server in order to send DHCP offer and acknowledgment messages to the mobile node in reply to the DHCP discovery and request messages. While the mobile access gateway is seen as a DHCP server from a mobile node, it actually obtains the IPv4 home address for each mobile node from the local mobility anchor during proxy binding procedure (set 0.0.0.0 in the the IPv4 Home Address field of the IPv4 home address option as described in [ID-DSMIP6]). After MAG receiving the assigned IPv4 address from LMA, it assigns the address to the requesting mobile node. Note that the mobile access gateway MUST return its own IP address in the 'server identifier' option when

sending DHCP messages to the mobile node. Thus, whenever the mobile node changes the attached mobile access gateway, this server identifier must be updated. The detail can be found in Section 3.2.2. The second scenario does not have this server

identifier change when a mobile node changes its mobile access gateway. Any information carried in DHCP options such as addresses of domain name server, time server, lpr server, etc. MUST be configured in all the DHCP server located at mobile access gateways if necessary.

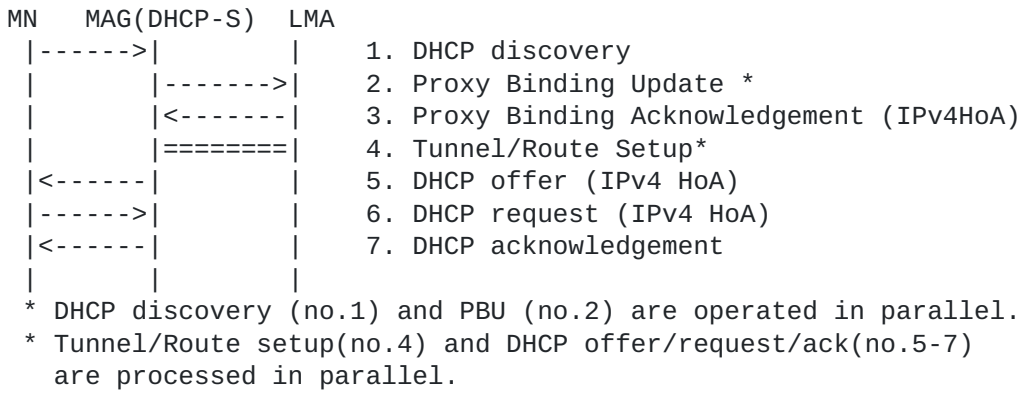


Figure 2: An example when LMA assigns an IPv4 home address

In the second scenario, a DHCP relay is co-located at each mobile access gateway and a DHCP server is co-located at a local mobility anchor. A mobile access gateway sends a proxy binding update and retrieves an IPv4 home address for the mobile node from the local mobility anchor as described in the first scenario. When the mobile access gateway relays DHCP messages to the DHCP server, it includes the assigned IPv4 home address information in the DHCP messages as a hint. The DHCP server SHOULD assign the address stored in the hint to the mobile node. Figure 3 are the sequence of IPv4 home address assignment using DHCP Relay. The DHCP discovery message is sent by a mobile node at any time, but the DHCP relay SHOULD NOT relay the DHCP discovery message before it learns the IPv4 home address hint during the proxy binding registration. As shown in Figure 3, the DHCP messages MAY be sent across an administrative boundaries. The operators MUST ensure to secure these messages. More remarks can be found in Section 6. The DHCP server identifier remains the same all the time, because the server is uniquely located at the local mobility anchor.

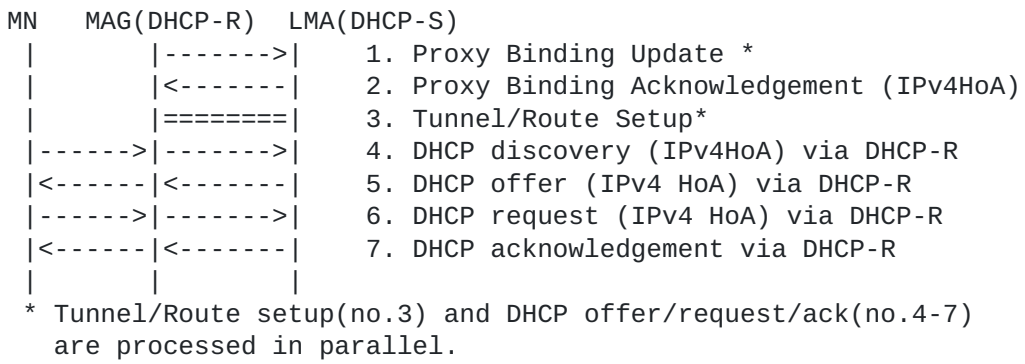


Figure 3: The use of DHCP relay

3.2. Mobile Access Gateway Considerations

3.2.1. Extensions to Binding Update List Entry

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

- The IPv4 home address of the attached mobile node. This is acquired from the mobile node's local mobility anchor through the received Proxy Binding Acknowledgment message. The IPv4 home address parameter also includes the corresponding subnet mask.

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

3.2.2. Signaling Considerations

All the considerations from Section 6.9 of [ID-PMIP6] apply here. However, the following additional considerations MUST be applied.

Mobile Node Attachment and Initial Binding Registration:

- 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 IPv4 home address mobility service needs to be offered to the mobile node [RYUJI by checking the policy profile], it MUST send a Proxy Binding Update message for the IPv4 home address to the local mobility anchor. The message MUST include the IPv4 Home Address option, defined in section 3.1.1 of [ID-DSMIP6]. The mobile access gateway MAY also

include the IPv6 Home Network Prefix option in the same message for requesting IPv6 home address support in addition to IPv4 home address support for the mobile node. [RYUJI The mobile access gateway contain either an IPv4 Home Address Option or a Home Network Prefix option, or both, depending on the mobile node's type.]

- If the mobile access gateway learns the mobile node's IPv4 home network prefix or the IPv4 home address either from its policy store or from the DHCP messages exchanged between the mobile node and the DHCP server, the mobile access gateway can specify the same in the IPv4 Home Address option for requesting the local mobility anchor to allocate that address or to allocate an address from the specified home network prefix. If the specified value is 0.0.0.0, then the local mobility anchor will consider this as a request for dynamic address allocation.

- The mobile access gateway on the access link where mobile node is attached, will register this address with the local mobility anchor using the IPv4 Home Address option, defined in Section 3.1.1 of [ID-DSMIP6]. The IPv4 Home Address option is sent with a proxy binding update message. The format of the proxy binding update is slightly different from the one of [ID-DSMIP6]. In [ID-DSMIP6], the source address of IPv6 header must be a home address of the mobile terminal. However, since Proxy Mobile IPv6 supports also IPv4-only nodes, IPv6 home address is not always available on the terminal. In addition to this, the originator of this proxy binding update is not the mobile terminal, but the mobile access gateway. The mobile access gateway cannot send the proxy binding update with the mobile node's home address because of security reasons (IPsec and ingress filtering). Therefore, in this specification, the mobile access gateway's care-of address (Proxy-CoA) is used in the IPv6 source address field.

- The proxy binding update MUST be protected by IPsec ESP.

Receiving Binding Acknowledgement Message:

- If the received Proxy Binding Acknowledgement message has neither an IPv4 Address Acknowledgement option or a Home Network Prefix option present, the mobile access gateway MUST ignore the Proxy Binding Acknowledgement and MUST NOT enable routing for the mobile node's IPv4 Home Address or IPv6 home address traffic. However,

if there is an IPv4 Home Address Acknowledgment option present in the reply, the option MUST be processed as per the rules specified in Dual Stack Mobile IPv6 specification [ID-DSMIP6].

- If the received Proxy Binding Acknowledgement message has the Status field value in the IPv4 Address Acknowledgement Option set to a value that indicates that the request was rejected by the local mobility anchor, the mobile access gateway MUST NOT enable IPv4 support for the mobile node. However, if there is an IPv6 Home Network Prefix option in the Proxy Binding Acknowledgement message and the Status field in the message is set to a value 0 (Proxy Binding Update accepted), the mobile access gateway MUST enable IPv6 support for the mobile node.

- If the received Proxy Binding Acknowledgement message has the Status field value set to 0 (Proxy Binding Update accepted), the mobile access gateway MUST update a Binding Update List entry and must setup a tunnel to the local mobility anchor and must also add a default route over the tunnel for all the mobile node's IPv4 traffic. The encapsulation mode for the bi-directional tunnel set to IPv4-In-IPv6 mode. The considerations from Section 6.10 [ID-PMIP6] apply.

Extending Binding Lifetime:

- For extending the binding lifetime of a currently registered mobile node , the mobile access gateway MUST send a Proxy Binding Update message to the local mobility anchor with a non zero lifetime value. The message MUST contain the IPv4 Home Address option with the value set to the currently registered IPv4 home address value. Additionally, if there is a registered IPv6 home network prefix for the mobile node for the connected interface on that access link, both the options, Home Network Prefix option and the IPv4 Home Address option MUST be present and with the values set to the respective registered values.

Mobile Node Detachment and Binding De-Registration:

- As specified in Section 6.9.1 [ID-PMIP6], at any point in time, when the mobile access gateway detects that the mobile node has moved away from its access link, it SHOULD send a Proxy Binding Update message to the local mobility anchor with the lifetime value set to zero. The message MUST contain the IPv4 Home Address option with the value set to the currently registered IPv4 home address value. Additionally, if there is a registered IPv6 home network prefix for the mobile node for the connected interface on that access link, both the options, Home Network Prefix option and the IPv4 Home Address option MUST be present and with the values set to the respective registered values.

Constructing the Proxy Binding Update Message:

The mobile access gateway when sending the Proxy Binding Update request to the local mobility anchor for requesting IPv4 home address mobility support MUST construct the message with the following considerations.

- The message MUST be constructed as specified in Section 6.9 of [ID-PMIP6]. However, when sending the messages over IPv4 transport, additional considerations from Section 4.0 MUST be applied.

- The IPv4 Home Address option [ID-DSMIP6] MUST be present. The address value MAY be set 0.0.0.0 or to a specific value.

DHCP Messages from the mobile node:

The operations of DHCP are almost same for both scenarios listed in Section 3.1. There is one special operation for address renewing operation when a mobile access gateway is the DHCP server.

- When a mobile node attached to an access link and attempts to obtain an IPv4 address configuration, using DHCP or other procedures, it will get an IPv4 address as an IPv4 home address from its home subnet as discussed in Section 3.1. The mobile access gateway on the access link where mobile node is attached, will register the IPv4 home address with the local mobility anchor using the IPv4 Home Address option, defined in Section 3.1.1 of [ID-DSMIP6]. The IPv4 Home Address option is sent with a proxy binding update.

- When a mobile node attempts to obtain an IPv4 home address by using DHCP, the mobile access gateway SHOULD complete the proxy binding registration before starting any DHCP operation. This is necessary for the mobile access gateway to obtain all the information required for DHCP operation from the local mobility anchor.

- The mobile access gateway SHOULD send a proxy binding update with 0.0.0.0 in the the IPv4 Home Address field of the IPv4 home address option [ID-DSMIP6] and retrieve the assigned IPv4 home address from the local mobility anchor. The IPv4 home address assigned by the local mobility anchor is offered to the mobile node by DHCP.

- When a mobile node changes its attached mobile access gateway, the new mobile access gateway MUST sends a proxy binding update with

the IPv4 home address option. If the new mobile access gateway know the assigned IPv4 home address, for example by context transfer mechanism or policy profile, it SHOULD include the address in the IPv4 Home Address field. Otherwise, it uses 0.0.0.0 and obtains the assigned IPv4 home address of the mobile node from the local mobility anchor, again.

- Except for the mobile node's bootstrap, DHCP runs independently to the proxy binding registration, for instance, for renewing the assigned IPv4 home address. It is not necessary to run DHCP whenever a mobile node changes its attached mobile access gateway.
  A DHCP client renew the address according to the address lifetime, etc. However, whenever a mobile node renews the IPv4 home address by DHCP (DHCP RENEWING STATE [RFC-2131]), the mobile access gateway SHOULD send a proxy binding update to the local mobility anchor regardless of the mobile node's assigned address changes.

- When a mobile node gets IPv4 home address from Local Mobility Anchor through DHCP interaction with mobile access gateway that supports DHCP server functionality, the DHCP client in the mobile node recognizes mobile access gateway's IP address as DHCP server's IP address. Thus, the DHCP client unicasts DHCP renew to the mobile access gateway, when the DHCP client goes into the DHCP RENEWING state [RFC-2131]. However, when the mobile node handovers to a new mobile access gateway, the mobile node does not know the link change and the DHCP client would unicast DHCP request to the previous mobile access gateway whose IP address was acquired from DHCP offer. The DHCP client in the mobile node needs to reconfigure its local configuration parameters. The mobile access gateway SHOULD discard any DHCP request message that does not belong to the mobile access gateway itself, so that the mobile node should go into the DHCP REBINDING state and broadcast DHCP discovery message without server identifier.

3.3. Local Mobility Anchor Considerations

3.3.1. Extensions to Binding Cache Entry

For supporting this feature, the conceptual Binding Cache entry data structure needs to be extended with the following additional parameter, as specified in [ID-DSMIP6] specification and is presented here for convenience.

- The IPv4 home address of the registered mobile node. The IPv4 home address value may have been statically configured in the mobile node's policy profile, it MAY have been assigned by a DHCP server, or it MAY have been dynamically allocated by the local mobility anchor.

3.3.2. Signaling Considerations

All the considerations explained in Section 5.3 [ID-PMIP6] apply here. For supporting IPv4 home address mobility feature, the following additional considerations MUST be applied.

Processing Binding Registrations:

- If there is an IPv4 Home Address option present in the request, but if there is no Home Network Prefix option present in the request, the local mobility anchor MUST NOT reject the request as specified in [ID-PMIP6]. At least one of these two options MUST be present. However, if both the options are not present, the local mobility anchor MUST reject the request and send a Proxy Binding Acknowledgement message with Status field set to MISSING_HOME_NETWORK_PREFIX_OPTION (Missing mobile node's home network prefix option).

- The local mobility anchor MUST use the identifier from the Mobile Node Identifier Option [RFC-4283] present in the Proxy Binding Update request and MUST apply multihoming considerations specified in Section 5.4 [ID-PMIP6] and from this section for performing the Binding Cache entry existence test.

- If there is no existing Binding Cache entry that matches the request, the local mobility anchor MUST consider this request as an initial binding registration request. If the entry exists, the local mobility anchor MUST consider this request as a binding re-registration request.

- The proxy care-of address MUST be retrieved from the source address field of the proxy binding update message.

- If the IPv4 Home Address option present in the Proxy Binding Update request has the value of 0.0.0.0, the local mobility anchor MUST allocate an IPv4 home address for the mobile node and send a Proxy Binding Acknowledgement message and including the IPv4 Address Acknowledgement option, defined in Section 3.2.1 of [ID-DSMIP6], containing the allocated address value. The specific details on how the local mobility anchor allocates the home address is outside the scope of this document. The local mobility anchor MUST ensure the allocated prefix is not in use by any other mobile node.

- If the local mobility anchor is unable to allocate an IPv4 home

address for the mobile node, it MUST reject the request and send a
Proxy Binding Acknowledgement message with Status field set to 130

(Insufficient resources).

- Upon accepting the request, the local mobility anchor MUST create a Binding Cache entry for the mobile node. It must set the fields in the Binding Cache entry to the accepted values for that binding. It MUST also establish a bi-directional tunnel to the mobile access gateway, as described in [RFC-2473]. Considerations from Section 5.6 [ID-PMIP6] MUST be applied. The local mobility anchor MUST add an IPv4 host route for that allocated IPv4 home address over the tunnel to the mobile access gateway.

Multihoming Considerations:

- The multihoming considerations specified in Section 5.4 [ID-PMIP6] allows the local mobility anchor to perform the Binding Cache entry existence test for identifying the mobility session, by using the mobile node identifier, interface identifier and the Home Network Prefix values. When using an IPv4 home address value, instead of the IPv6 home network prefix for matching the Binding Cache entry, all those considerations equally apply for the IPv4 home address as well.

- If there is an Home Network Prefix option present in the Proxy Binding Update request and with a NON_ZERO value, the local mobility anchor MUST use this parameter in combination with the mobile node identifier and interface identifier for matching the Binding Cache entry, just as specified in Section 5.4 [ID-PMIP6]. For all other cases, the local mobility anchor MUST use the IPv4 home address parameter in combination with the mobile node identifier and interface identifier for matching the Binding Cache entry, as specified in Section 5.4 [ID-PMIP6].

Constructing the Proxy Binding Acknowledgement Message:

- The local mobility anchor when sending the Proxy Binding Acknowledgement message to the mobile access gateway MUST construct the message as specified in Proxy Mobile IPv6 base specification [ID-PMIP6]. However, the following considerations MUST be applied.

- The IPv4 Address Acknowledgement option MUST be present in the Proxy Binding Acknowledgement message.

  1. If the Status field is set to a value greater than or equal to 128, i.e., if the binding request is rejected, then the IPv4

home address value in the IPv4 Address Acknowledgement option

MUST be set to ALL_ZERO value.

2. For all other cases, the IPv4 home address value in the IPv4 Address Acknowledgement option MUST be set to the allocated IPv4 home address value for that mobility session.

3.3.3. Routing Considerations

Forwarding Considerations for the mobile node's IPv4 home address traffic.

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

- When the local mobility anchor is serving a mobile node, it MUST be able to receive packets that are sent to the mobile node's IPv4 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 IPv4 home network prefix or for an aggregated prefix with a larger scope. This essentially enables IPv4 routers in that network to detect the local mobility anchor as the last-hop router for that IPv4 prefix.

Forwarding Packets to the Mobile Node:

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

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

Figure 4: Tunneled Packets from LMA to MAG

Forwarding Packets Sent by the Mobile Node:

- All the reverse tunneled packets that the local mobility anchor receives from the mobile access gateway, after removing the tunnel

header MUST be routed to the destination specified in the inner IPv4 packet header. These routed packets will have the source

address field set to the mobile node's IPv4 home address.

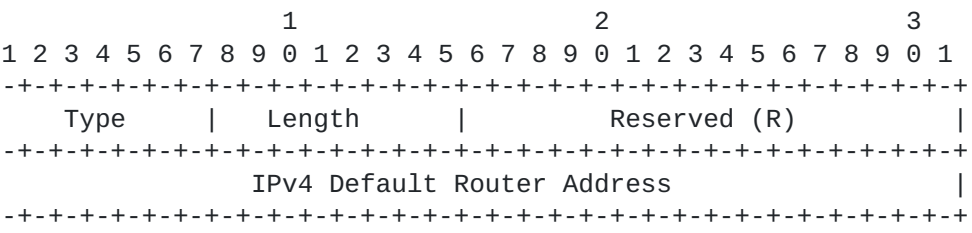
3.4. Mobility Options

For supporting IPv4 home address mobility feature, this specification defines the following new option.

3.4.1. IPv4 Default Router Address Option

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

The IPv4 Default Router Address option has an alignment requirement of 4n. Its format is as follows:



Type

<IANA>

Length

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

Reserved (R)

This 8-bit field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

IPv4 Default Router Address

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

Figure 5: IPv4 Default Router Address Option

4. IPv4 Transport Support

The Proxy Mobile IPv6 specification [ID-PMIP6] requires the network between the local mobility anchor and the mobile access gateway to be an IPv6 network and the signaling messages exchanged between the local mobility anchor and the mobile access gateway to be over an IPv6 transport. The extensions defined in this section allow the exchange of signaling messages over an IPv4 transport when the local mobility anchor and the mobile access gateway are separated by an IPv4 network and are reachable using an IPv4 address.

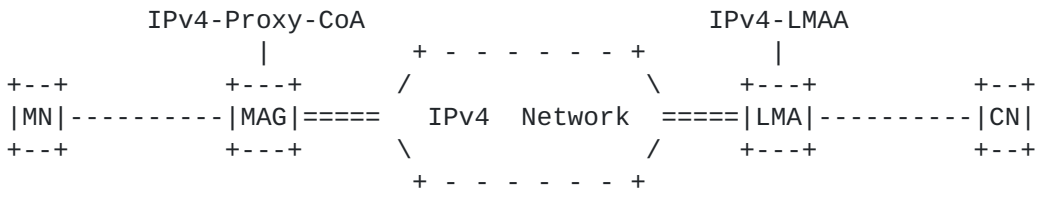


Figure 6: IPv4 Transport Network

When the network between the local mobility anchor and the mobile access gateway is an IPv4 network, i.e., when both these mobility entities are configured and reachable using an IPv4 address, the mobile access gateway serving a mobile node can potentially register its IPv4 address with the local mobility anchor, as the care-of address in the mobile node's Binding Cache entry and can negotiate and IPv4 transport tunnel for tunneling the mobile node's data traffic.

The Dual Stack Mobile IPv6 specification [ID-DSMIP6] defines protocol extensions to Mobile IPv6 protocol for allowing a mobile node to roam into an IPv4 network and registers an IPv4 care-of address with the home agent. The same mechanism is leveraged for extending IPv4 transport support to Proxy Mobile IPv6 protocol. The mobility options for requesting IPv4 transport support, the processing logic and the on-path NAT detection logic is just as described in [ID-DSMIP6]. The following are the key properties of this feature.

- The local mobility anchor and the mobile access gateway are both configured and reachable using an IPv4 address.

- The configured address on the mobile access gateway can be an IPv4 private address and when it is behind a NAT translation device and the mechanism specified in Dual Stack Mobile IPv6 specification

[ID-DSMIP6] is again leveraged for NAT detection and traversal.

- The Proxy Mobile IPv6 signaling messages exchanged between the local mobility anchor and the mobile access gateway for negotiating the IPv4 transport will be encapsulated and carried as IPv4 packets. However, these signaling messages are fundamentally IPv6 messages with the mobility header and the semantics as specified in base Proxy Mobile IPv6 specification [ID-PMIP6], but carried as payload in IPv4 packets. Additionally, the mobility options defined in Dual Stack Mobile IPv6 specification [ID-DSMIP6] are used for negotiating IPv4 transport support and with a specific encapsulation mode.

- The IPv4 tunnel established between the local mobility anchor and the mobile access gateway (with any of the supported encapsulation modes over IPv4 transport) is used for carrying the mobile node's IPv4 and IPv6 traffic. The mobile node can be an IPv6, IPv4 or a dual IPv4/IPv6 node and the IPv4 transport support specified in this section is agnostic to the type of address mobility enabled for the mobile node.

4.1. NAT Support

When the transport network between the local mobility anchor and the mobile access gateway is an IPv4 network, the mobile access gateway MUST send Proxy Binding Update message encapsulated in the IPv4-UDP packet. On receiving this Proxy Binding Update packet encapsulated in an IPv4-UDP packet, the local mobility anchor if it detects a NAT on the path, will send the Proxy Binding Acknowledgment message with the NAT Detection Option. The presence of this option in the Proxy Binding Acknowledgment is an indication to the mobile access gateway about the presence of NAT in the path. On detecting the NAT in the path, both the local mobility anchor and the mobile access gateway MUST set the encapsulation mode of the tunnel to IPv4-UDP-based encapsulation. The specific details around the NAT detection and the related logic is described in in DSMIPv6 specification [ID-DSMIP6].

There are discussions on how to incorporate the NAT detection mechanism of IKE with DSMIPv6 in the MEXT Working Groups. This documentation will follow the conclusion of their discussions.

[RYUJI Private addresses MUST NOT be configured at both mobile access gateways and a local mobility anchor in the same Proxy Mobile IPv6 domain. At least one of Proxy Mobile IPv6's tunnel end points MUST have a global address. Otherwise, the packets might not be exchanged in the tunnel due to NAT.]

[RYUJI When a mobile access gateway is configured with an IPv4 private address, it MUST NOT operate the local routing (described in Section 6.10.3 of [ID-PMIP6]) for packets destined to an IPv4 address

assigned to a correspondent node. The address translation MUST happen before the packets are arrived at the correspondent node. To ensure this, the packets MUST be sent to the local mobility anchor and routed back to the correspondent node.]

4.2. Mobile Access Gateway Considerations

4.2.1. Extensions to Binding Update List Entry

For supporting this feature, the conceptual Binding Update List entry data structure needs to be extended with the following additional parameters, as specified in [ID-DSMIP6] specification and is reviewed here for convenience.

- The IPv4 address registered with the local mobility anchor as the mobile node's care-of address.

4.2.2. Signaling Considerations

All the considerations as explained in Section 6.11 of the base Proxy Mobile IPv6 specification apply here.

Network Configurations for IPv4 Transport Signaling Support:

- If IPv4 transport support is enabled in order to place a mobile access gateway at IPv4 only network, the mobile access gateway MUST have an IPv4 address at the visiting network. In addition to that, the mobile access gateway MUST obtain an IPv6 address configured for the Proxy Mobile IPv6 operation. Even if the mobile access gateway does not have connectivity to the IPv6 network, it MUST configure with an IPv6 address for sending the proxy binding registration to the local mobility anchor.

Processing Binding Registrations:

- As explained in the DSMIPv6 specification, the mobile access gateway can encapsulate a Proxy Binding Update message and carry it in IPv4 and UDP packet. The processing logic for handling the NAT detection at the mobile node is applicable to the mobile access gateway as described in Section 4.1.

- An example of proxy binding update sent by mobile access gateway is shown in Figure 7. The source address of the inner IPv6 header MUST set to the IPv6 address assigned to the mobile access gateway

and the destination address MUST be the local mobility anchor's IPv6 address (LMAA). This is slightly different from [ID-DSMIP6]

. The reason is already mentioned in Section 3.2.2.

- The source address of the outer packet MUST be the IPv4-Proxy-CoA and the destination MUST be the local mobility anchor's IPv4 address (IPv4-LMAA).

- The IPv4-Proxy-CoA MUST be set in the IPv4 Care-of Address option defined in section 3.1.2 of [ID-DSMIP6].

- For the NAT handling, the UDP-based encapsulation MUST be always used for the proxy binding update. The UDP port number is defined in [ID-DSMIP6].

- If the mobile access gateway requested to use the TLV header for the UDP encapsulation, it MUST insert a TLV header after the UDP header and MUST set T flag in the proxy binding update message. The format of the TLV header is defined in section 4.1 of [ID-DSMIP6].

- The proxy binding update MUST be protected by IPsec ESP. The security association for IPv4 addresses of the mobile access gateway and local mobility anchor are pre-established.

Constructing the Proxy Binding Update Message:

- For requesting IPv4 transport support, the mobile access gateway when sending the Proxy Binding Update request to the local mobility anchor from an IPv4 networks MUST construct the message as specified below.

```
IPv4 header (src=IPv4-Proxy-CoA, dst=IPv4-LMAA)
   UDP header
      IPv6 header (src=Proxy-CoA, dst=LMAA)
         Mobility header
            -BU (P flag is set. F/T flags are optional)
                Mobility Options
                   - The IPv4 Care-of Address option(Mandatory)
                   -
                   - All the options as required by [ID-PMIP6]
                   - or as required by any extension documents
                   -
```

Figure 7: Proxy Binding Update Message Format for IPv4 Transport Support

o

o The IPv4 Care-of Address option [ID-DSMIP6] MUST be present. The address value MUST be set to mobile access gateway's IPv4 address.

o All the other fields and the options MUST be constructed, as specified in [ID-PMIP6].

Receiving Binding Registration Reply:

o After receiving a Proxy Binding Acknowledgment message encapsulated in an IPv4 packet, the mobile access gateway MUST verify the Proxy Binding Acknowledgment according to the Section 4.3 of Dual Stack Mobile IPv6 specification [ID-DSMIP6].

o If the Status field indicates Success, the mobile access gateway MUST setup a tunnel to the local mobility anchor and add a default route over the tunnel for all the mobile node's traffic.

o If the NAT is available and the NAT detection option is presented in the Proxy Binding Acknowledgment, the mobile access gateway MUST use the UDP tunnel to traverse the NAT for mobile node's traffic and MUST send a proxy binding update every refresh time specified in the NAT detection option. The detailed operation can be found in Dual Stack Mobile IPv6 specification [ID-DSMIP6].

o If the Status field in the proxy binding acknowledgment indicates the rejection of the binding registration, the mobile access gateway MUST NOT enable IPv4 transport for the mobile node's traffic.

Forwarding Packets to Local Mobility Anchor

o On receiving any packets from the mobile node's IPv6 home address and/or IPv4 home address, the mobile access gateway tunnels the packets to local mobility anchor as shown in Figure 8. If the mobile access gateway and the local mobility anchor agreed to use the TLV header for the UDP tunnel during the binding registration, the TLV header MUST be presented after the UDP header as shown in Figure 9.

```
IPv4 header (src=IPv4-Proxy-CoA, dst=IPv4-LMAA)
    [UDP header] /*Only if NAT is detected*/
        union { /*following either v6 or v4 header */
            IPv4 header (src=MN's IPv4-HoA, dst=IPv4 CN)
            IPv6 header (src=MN's IPv6-HoA, dst=IPv6 CN)
        }
                Upper layer protocols /*TCP,UDP,SCTP*/
```

Figure 8: Tunneled Packets from MAG to LMA

```
IPv4 header (src=IPv4-Proxy-CoA, dst=IPv4-LMAA)
    UDP header
        TLV header
        union {
            IPv4 header (src=MN's IPv4-HoA, dst=IPv4 CN)
            IPv6 header (src=MN's IPv6-HoA, dst=IPv6 CN)
            IPsec
            GRE
        }
                Upper layer protocols /*TCP,UDP,SCTP*/
```

Figure 9: Tunneled Packets from MAG to LMA using the TLV header

4.3. Local Mobility Anchor Considerations

4.3.1. Extensions to Binding Cache Entry

For supporting this feature, the conceptual Binding Cache entry data structure needs to be extended with the following additional parameter as specified in [ID-DSMIP6] specification and are reviewed here for convenience.

- The IPv4 Care-of address of the attached mobile node. In this specification, it can be translated to IPv4 Care-of address of the mobile access gateway to which a mobile node is attached.

4.3.2. Signaling Considerations

When a mobile node is attached to a mobile access gateway that is reachable only through an IPv4 transport network, the local mobility anchor must establish an IPv4 tunnel for routing the mobile node's IPv4 and IPv6 home address traffic. The DSMIPv6 specification provides the semantics on how the IPv4 tunnel needs to be negotiated and the detection logic of the NAT devices. This specification

leverages the NAT Detection Option, defined in the Dual Stack Mobile IPv6 specification for the use in Binding Acknowledgment message and extends it to Proxy Binding Acknowledgment messages. The operational steps are defined below.

Processing Binding Registrations:

- After accepting the registration from the mobile access gateway locating at the IPv4 only network, the local mobility anchor MUST setup a tunnel to the mobile access gateway. The tunnel is established between the v4-LMAA and the IPv4-Proxy-CoA of the mobile access gateway.

- If the NAT is available, the local mobility anchor MUST use UDP encapsulation for the tunnel.

- If the T flag is set in the proxy binding update message and the TLV header is presented, the specified tunnel type must be used.

- The local mobility anchor also setup a host routes for the IPv4 home address and the IPv6 home address of the mobile node over the tunnel to the mobile access gateway. Any traffic that the local mobility anchor receives from a correspondent node will be tunneled to the mobile access gateway over the bi-directional tunnel and then routed accordingly after removing the tunnel headers. The encapsulation modes for the bi-directional tunnel are as specified in Section 5.3 of Proxy Mobile IPv6 specification [ID-PMIP6] and as in this specification.

- Upon receiving a Proxy Binding Update message encapsulated in an IPv4 packet, the local mobility anchor MUST send the Proxy Binding Acknowledgment to the mobile access gateway's IPv4-Proxy-CoA by using IPv4 encapsulation.

- If the NAT is detected, the NAT detection option MUST be used in the Proxy Binding Acknowledgment. How to detect NAT is described in Section 4.1 of [ID-DSMIP6] and Section 4.1.

Constructing the Proxy Binding Acknowledgement Message:

- The proxy binding acknowledgment MUST be protected by IPsec ESP. The security association for IPv4 addresses of the mobile access gateway and local mobility anchor are pre-established.

- For the IPv4 transport support, no special mobility options are required. Only when NAT is detected, the NAT detection option

MUST be present. The local mobility anchor MUST construct the proxy binding Acknowledgement as specified in [ID-PMIP6].

- An example of proxy binding acknowledgment sent by local mobility anchor is shown below. The same illustration for Mobile IPv6 can be found in Section 4.1 of [ID-DSMIP6].

```
IPv4 header (src=IPv4-LMAA, dst=IPv4-Proxy-CoA)
    UDP header
    [TLV-header] /* optional, if T flag is set */
     IPv6 header (src=LMAA, dst=Proxy-CoA)
        Mobility header
            -BA /* P flag/T flag(option) */
           Mobility Options
              - Home Network Prefix Option
              - IPv4 Address Acknowledgement option
              - Timestamp option (optional)
              - Mobile Node Identifier Option
              - Access Technology Type option
(Mandatory)
              - Mobile Node Interface Identifier option
                (Optional)

              - NAT Detection Option (Optional)
```

Figure 10: Proxy Binding Acknowledgment in IPv4 network

Forwarding Packets to Mobile Access Gateway

- When sending any packets meant to a mobile node's IPv4 home address or IPv6 home address, the local mobility anchor tunnels the packet to mobile access gateway as shown in Figure 11.

```
IPv4 header (src=IPv4-LMAA, dst=IPv4-Proxy-CoA)
    [UDP header] /*Only if NAT is detected*/
        union { /*following either v6 or v4 header */
            IPv4 header (src=IPv4-CN, dst=IPv4-HoA)
            IPv6 header (src=IPv6-CN, dst=IPv6-HoA)
        }
                Upper layer protocols /*TCP,UDP,SCTP*/
```

Figure 11: Tunneled Packets from LMA to MAG

- If the mobile access gateway and the local mobility anchor agreed to use the TLV header for the UDP tunnel during the binding registration, the TLV header MUST be presented after the UDP header as shown in Figure 12.

```
IPv4 header (src=IPv4-Proxy-CoA, dst=IPv4-LMAA)
    UDP header
        TLV header
        union {
            IPv4 header (src=IPv4-CN, dst=IPv4-HoA)
            IPv6 header (src=IPv6-CN, dst=IPv6-HoA)
            IPsec
            GRE
        }
                Upper layer protocols /*TCP,UDP,SCTP*/
```

Figure 12: Tunneled Packets from LMA to MAG using the TLV header

4.4. Tunnel Management

As specified in the Proxy Mobile IPv6 specification, the bi-directional tunnel between the local mobility anchor and the mobile access gateway, is a shared tunnel and all the considerations from Section 6.6 of Proxy Mobile IPv6 [ID-PMIP6] apply for IPv4 transport as well.

5. IANA Considerations

This document does not require IANA Action.

6. Security Considerations

The security mechanisms specified for Proxy Mobile IPv6 protocol are used when using the extensions defined in this document.

When supporting IPv4 address assignment from a DHCP server, all the IPv4 home addresses managed in the DHCP server must be reachable via local mobility anchor so that local mobility anchor intercepts packets meant for an IPv4 home address and tunnels them to the mobile node via corresponding mobile access gateway. Moreover, all the DHCP messages between a DHCP relay and the DHCP server SHOULD be securely exchanged.

After receiving a Proxy Binding Update message with an IPv4 Home Address Option, the local mobility anchor MUST be able to verify that the mobile node is authorized to use that address before setting up forwarding for that host route.

When supporting dynamic IPv4 address assignment by DHCP and also from local mobility anchor, it should be ensured both the entities are configured with different address pools, so as to avoid both entities do not allocate the same address to different mobile nodes.

This specification describes the use of IPv4 transport network between the local mobility anchor and the mobile access gateway. All the signaling messages exchanged between the mobile access gateway and the local mobility anchor over the IPv4 transport MUST be protected using IPsec, just as the messages must be protected when using IPv6 transport and as specified in the Section 4.0, of the Proxy Mobile IPv6 specification [ID-PMIP6].

7. Contributors

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

Kuntal Chowdhury

kchowdhury@starentnetworks.com

Vijay Devarapalli

vijay.devarapalli@azairenet.com

Sangjin Jeong

sjjeong@etri.re.kr

Basavaraj Patil

basavaraj.patil@nsn.com

Myungki Shin

myungki.shin@gmail.com

8. Acknowledgments

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

9. References

9.1. Normative References

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

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

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

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

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

[ID-DSMIP6] Soliman, H. et al, "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)", draft-ietf-mip6-nemo-v4traversal-05.txt ,July 2007.

[ID-PMIP6] Gundavelli, S., et.al, "Proxy Mobile IPv6", draft-ietf-netlmm-proxymip6-16.txt, November 2007.

9.2. Informative References

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

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

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

Appendix A. DHCP usages for IPv4 home address assignment

There are several other configurations of DHCP entities [RFC-2131] in a Proxy Mobile IPv6 domain other than the two configurations listed in Section 3.1. Although this specification recommends the two configurations described in Section 3.1, operators should select the best configuration according to their deployments scenario. The mobile node behavior for all scenarios does not change. We do not have major interoperability concerns between multiple scenarios. A mobile access gateway and local mobility anchor make sure that which scenario is used in the same Proxy Mobile IPv6 domain based on deployment requirements. The optional DHCP configurations for IPv4 home address assignment are described below.

- DHCP relay is co-located with each mobile access gateway and DHCP server is solely located in the Proxy Mobile IPv6 domain.

- DHCP relay is co-located with both each mobile access gateway and a local mobility anchor. DHCP server is solely located behind the local mobility anchor in the Proxy Mobile IPv6 domain.

The operations are same as described in Section 3.1. Before relaying any DHCP messages, a mobile access gateway SHOULD complete the proxy binding registration so that it learns the assigned address to provide the IPv4 home address hint to the DHCP server. However, when DHCP relays are located at both a mobile access gateway and a local mobility anchor, the DHCP relay at the local mobility anchor can simply insert the address hint retrieved from its local address management pool in the DHCP messages. Thus, the IPv4 home address option [ID-DSMIP6] can be omitted from the Proxy Binding Update and Acknowledgement messages.

Authors' Addresses

Ryuji Wakikawa
Keio University
Department of Environmental Information, Keio University.
5322 Endo
Fujisawa, Kanagawa 252-8520
Japan

Email: ryuji@sfc.wide.ad.jp

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

Email: sgundave@cisco.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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