NETLMM Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 15, 2009

R. Wakikawa
Toyota ITC
S. Gundavelli
Cisco

July 14, 2008

IPv4 Support for Proxy Mobile IPv6
draft-ietf-netlmm-pmip6-ipv4-support-04.txt

Status of this Memo

Copyright Notice

Abstract

This document specifies extensions to Proxy Mobile IPv6 protocol for adding IPv4 protocol support. The scope of IPv4 protocol support is two-fold: 1) For extending IPv4 home address mobility support to the mobile node. 2) For allowing the mobility entities in the Proxy Mobile IPv6 domain to exchange signaling messages over an IPv4 transport network.

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 the 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.

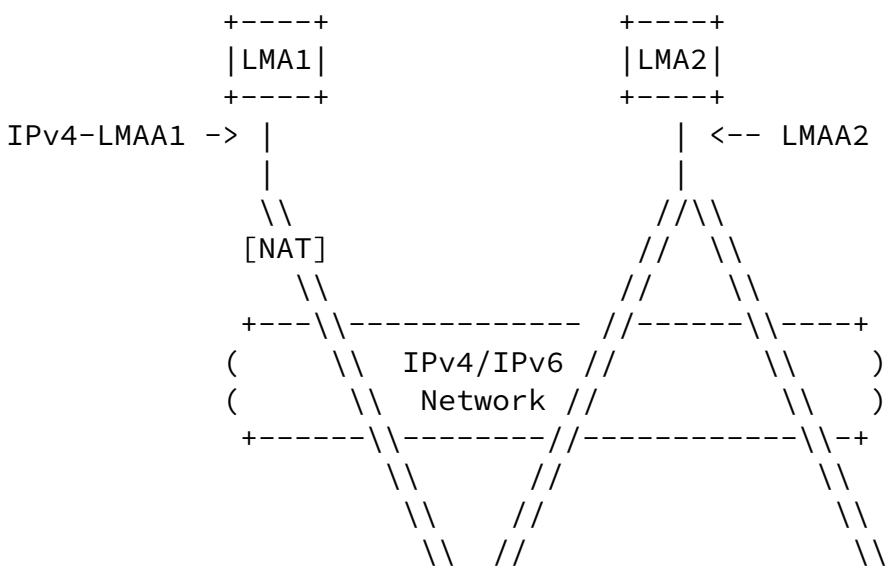
The Proxy Mobile IPv6 protocol [RFC-5213] specifies a mechanism for providing IPv6 home address mobility support to a mobile node in a Proxy Mobile IPv6 domain. The protocol requires IPv6 transport network between the mobility entities. The extensions defined in this document extends IPv4 support to the Proxy Mobile IPv6 protocol [RFC-5213].

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 mobile access gateway may be using an IPv4 private address and with NAT [RFC-3022] translation devices on the path to the local mobility anchor.

These two features, the IPv4 Home Address Mobility support and the IPv4 transport support features, are independent of each other and deployments may choose to enable any one or both of these features as required.



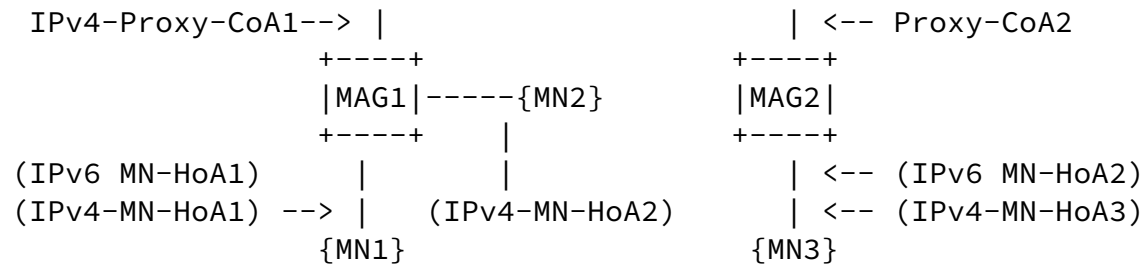


Figure 1: IPv4 support for Proxy Mobile IPv6

1.1. Stated Assumptions

Following are the configuration requirements from the mobility entities in the Proxy Mobile IPv6 domain for supporting the extensions defined in this document.

- The local mobility anchor and the mobile access gateway are both IPv4 and IPv6 enabled. Irrespective of the type of transport network (IPv4 or IPv6) separating these two entities, the mobility signaling is always based on Proxy Mobile IPv6 [RFC-5213].

- The mobile node can be operating in IPv4-only, IPv6-only or in dual mode. Based on what is enabled for a mobile node, it should be able to obtain IPv4-only, IPv6-only or both IPv4 and IPv6 address(es) for its interface and further achieve mobility support for those addresses.

- For enabling IPv4 home address mobility support to a mobile node, it is not required that the IPv6 home address mobility support needs to enabled. However, the respective protocol(s) support must be enabled on the access link between the mobile node and the

mobile access gateway.

- The mobile node can obtain one or more IPv4 addresses for its attached interface. Based on the type of link, it may be able to acquire its IPv4 address configuration using DHCP [RFC-2131], IPCP [RFC-1332], IKEv2 [RFC-4306], static configuration or through other standard IPv4 address configuration mechanisms.

- The mobile node's IPv4 home subnet is typically a shared address space. Its is not for the exclusive use of any one mobile node. There can be more than one mobile node sharing different addresses from the same IPv4 subnet.

- The mobile access gateway is the IPv4 default-router for the mobile node on its access link. It will be in the forwarding path for the mobile node's data traffic.

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 the Mobile IPv6 specification [RFC-3775] and Proxy Mobile IPv6 specification [RFC-5213]. In addition this document introduces the following terms.

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

The IPv4 address that is configured on the egress-interface of the mobile access gateway. When using IPv4 transport, this address will be the registered care-of address in the mobile node's Binding Cache entry and will also be the transport-endpoint of the tunnel between the local mobility anchor and a mobile access gateway. However, if 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 egress-interface of the local mobility anchor. When using IPv4 transport, the mobile access gateway sends the Proxy Binding Update messages to this address and will be the transport-endpoint of the tunnel between the local mobility anchor and the mobile access gateway.

Mobile Node's IPv4 Home Address (IPv4-MN-HoA)

This is the IPv4 home address assigned to the mobile node's attached interface. This IPv4 home address is topologically anchored at the local mobility anchor. The mobile node configures this address on its attached interface. There can be more than one IPv4 home addresses assigned to the mobile node's attached interface. Further, if the mobile node connects to the Proxy Mobile IPv6 domain through multiple interfaces and for simultaneous access, each of the attached interfaces will be assigned a unique set of IPv4 home addresses and all the IPv4 addresses that are assigned to a given interface of a mobile node

will be managed under one mobility session.

Encapsulation Modes

This document uses the following terms when referring to the different encapsulation modes.

IPv4-over-IPv6

IPv4 packet carried as a payload of an IPv6 packet

IPv4-over-IPv4

IPv4 packet carried as a payload of an IPv4 packet

IPv4-over-IPv4-UDP

IPv4 packet carried as a payload in an UDP header of an IPv4 packet

IPv4-over-IPv4-UDP-TLV

IPv4 packet carried as a payload in an IPv4 packet with UDP and TLV headers

3. IPv4 Home Address Mobility Support

The IPv4 home address mobility support essentially enables a mobile node in a Proxy Mobile IPv6 domain to obtain IPv4 home address configuration for its attached interface and be able to retain that address configuration even after changing its point of attachment in that Proxy Mobile IPv6 domain. This section describes the protocol operation and the required extensions to Proxy Mobile IPv6 protocol for supporting IPv4 home address mobility support.

When an IPv4-enabled or a dual-stack enabled mobile node attaches to the Proxy Mobile IPv6 domain, the mobile access gateway on the access network where the mobile node is attached will identify the mobile node and will initiate the Proxy Mobile IPv6 signaling with the mobile node's local mobility anchor. The mobile access gateway will follow the signaling considerations specified in Section 3.2 for requesting IPv4 home address support. Upon the completion of the signaling the local mobility anchor and the mobile access gateway will have the required states for allowing the mobile node to use its IPv4 home address(es) from the current point of attachment.

The mobile node on the access link using any of the standard IPv4 address configuration mechanisms supported on that access link, such as IPCP [RFC-1332], IKEv2 [RFC-4306] or using DHCP [RFC-2131], will be able to obtain one or more IPv4 home addresses (IPv4-MN-HoA) for the attached interface. Although the address configuration protocol mechanisms for delivering the address configuration to the mobile node is independent of the Proxy Mobile IPv6 protocol operation, however there needs to be some interactions between these two protocol flows. Section 3.4 identifies these interactions for supporting DHCP based address configuration.

The support for IPv4 home address mobility is not dependent on the IPv6 home address support. The mobile node is not required to have an IPv6 home address for obtaining IPv4 home address mobility. A mobile node will be able to obtain just IPv4 address configuration or both IPv4 and IPv6 address configuration on its attached interface. The mobile node's 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, if the mobile node after obtaining the address configuration on its interface performs an handoff, either by changing its point of attachment over the same interface or to a different interface, the network will ensure the mobile node will be able to use the same IPv4 address configuration after the handoff.

Additionally, 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 one or more IPv4 home addresses from different subnets. In such scenario, there will be multiple Binding Cache entries for the mobile node on the local mobility anchor. All the address (IPv4/ IPv6) assigned to a given interface will be managed as part of one mobility session, as specified in Section 5.4 of [RFC-5213].

3.1. Local Mobility Anchor Considerations

3.1.1. Extensions to Binding Cache Entry

For supporting this feature, the conceptual Binding Cache entry data structure maintained by the local mobility anchor needs to be extended with the following additional parameters.

- List of IPv4 home addresses assigned to the mobile node's interface registered by the mobile access gateway. Each of these IPv4 home address entries also include the corresponding prefix length.

- The IPv4 default-router address assigned to the mobile node.

3.1.2. Signaling Considerations

3.1.2.1. Processing Proxy Binding Updates

The processing rules specified in Section 5.3 of [RFC-5213] are applied for processing the received Proxy Binding Update message. However, if the received Proxy Binding Update message has one or more IPv4 Home Address options, the following additional considerations

MUST be applied.

- If there is an IPv4 Home Address option present in the received Proxy Binding Update message, 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 Section 5.3.1 of [RFC-5213]. At least one instance of any of these two options MUST be present. However, if not a single instance of any of these 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).

- For performing the Binding Cache entry existence test, the following considerations MUST be applied:

  * If there is at least one Home Network Prefix option with a NON_ZERO prefix value, or, if there is no IPv4 Home Address option with a NON_ZERO IPv4 address, considerations from Section 5.4 of [RFC-5213] MUST be applied.

  * If there is at least one IPv4 Home Address option present in the request with a NON_ZERO IPv4 address value, considerations from Section 3.2.2.7 MUST be applied.

- If there is no existing Binding Cache entry that can be associated with the request, the local mobility anchor MUST consider this request as an initial binding registration request and considerations from Section 3.2.2.2 MUST be applied.

- If there exists a Binding Cache entry that can be associated with the request, the local mobility anchor MUST apply considerations from Section 5.3.1 of [RFC-5213], (point 13), to determine if the request is re-registration request or a de-registration request and the respective considerations from below MUST be applied.

3.1.2.2. Initial Binding Registration (New Mobility Session)

- If there is at least one IPv4 Home Address option present in the Proxy Binding Update message with the IPv4 address value set to

ALL_ZERO, the local mobility anchor MUST allocate one or more IPv4 home addresses to the mobile node and associate them to the new mobility session created for that mobile node. The decision on how many IPv4 home addresses to be allocated can be based on a domain-wide policy or a policy specific to that mobile node.

- If there are one or more IPv4 Home Address options present in the received Proxy Binding Update message (with the IPv4 address field in the option set to a NON_ZERO value), the local mobility anchor before accepting the request, MUST ensure the address is owned by the local mobility anchor and further the mobile node is authorized to use that address. If the mobile node is not authorized for a specific address, the local mobility anchor MUST reject the request and send a Proxy Binding Acknowledgement message with Status field set to NOT_AUTHORIZED_FOR_IPV4_HOME_ADDRESS (mobile node not authorized for the requesting IPv4 Home Address). It MUST also set the status field value in the corresponding IPv4 Address Acknowledgement option [ID-DSMIP6] to 129 (Administratively prohibited).

- If the local mobility anchor is unable to allocate an IPv4 address due to lack of resources, it MUST reject the request and send a

Proxy Binding Acknowledgement message with Status field set to 130 (Insufficient resources). It MUST also set the status field value in the corresponding IPv4 Address Acknowledgement option [ID-DSMIP6], to 128 (Failure, reason unspecified).

- Upon accepting the request, the local mobility anchor MUST create a Binding Cache entry for this mobility session. However, if the request also contains one or more Home Network Prefix options, there should still be only one Binding Cache entry that should be created for this mobility session. The created Binding Cache entry MUST be used for managing both IPv4 and IPv6 home address bindings. The fields in the Binding Cache entry MUST be updated with the accepted values for that binding.

- The local mobility anchor MUST establish a bi-directional tunnel to the mobile access gateway and with the encapsulation mode as negotiated. When using IPv6 transport, the encapsulation mode is IPv4 over IPv6.

- The local mobility anchor MUST create IPv4 host route(s) for tunneling the packets received for any of the mobile node's home address(es) associated with this mobility session.

- The local mobility anchor MUST send the Proxy Binding Acknowledgement message with the Status field set to 0 (Proxy Binding Update Accepted). The message MUST be constructed as specified in Section 3.1.2.6.

3.1.2.3. Binding Lifetime Extension (No handoff)

All the consideration from Section 5.3.2 of [RFC-5213] MUST be applied.

3.1.2.4. Binding Lifetime Extension (After handoff)

- The local mobility anchor MUST remove the previously created host route(s), towards the mobile access gateway where the mobile node was anchored prior to the handoff.

- The local mobility anchor MUST create a host route(s) for tunneling the packets received for any of the mobile node's home address(es) associated with this mobility session.

- The required forwarding state identified in Section 5.3.6 of [RFC-5213] is for IPv6 payload traffic. Those considerations apply for IPv4 payload traffic as well. However, if IPv4 transport is in use, considerations from Section 4.0 MUST be applied.

3.1.2.5. Binding De-Registration

All the consideration from Section 5.3.5 of [RFC-5213] MUST be applied. Additionally, for removing the routing state as part of the Binding Cache entry deletion, any IPv4 host route(s) added for this mobility session MUST be removed.

3.1.2.6. 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 Section 5.3.6 of [RFC-5213]. Additionally, the following considerations MUST be applied.

- Section 5.3.6 of [RFC-5213] requires the local mobility anchor to include at least one instance of Home Network Prefix option in the Proxy Binding Acknowledgement message that it sends to the mobile access gateway. However, if the received Proxy Binding Update message has only the IPv4 Home Address option and did not contain the Home Network Prefix option(s), then the local mobility anchor MUST NOT include the Home Network Prefix option in the reply.

- The IPv4 Address Acknowledgement option(s) 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 Proxy Binding Update is rejected, then there MUST be an IPv4 Address Acknowledgement option for each of the IPv4 Home Address options present in the request and with the address value and the prefix length in the option set to the values present in the corresponding request option. The status field value in the option must be set to the specific error code.

  2. For all other cases, there MUST be an IPv4 Address Acknowledgement option for each of the assigned IPv4 home addresses assigned for that mobility session and with the value in the option set to the allocated address value. The prefix length in the option MUST be set to the prefix length of the allocated address. The status field value in the option must be set to 0 (Success).

- The IPv4 Default-Router Address option MUST be present, if the Status field value in the Proxy Binding Acknowledgement message is set to 0 (Proxy Binding Update Accepted). Otherwise, the option MUST NOT be present. If the option is present, the default-router address in the option MUST be set to the mobile node's default-router address.

3.1.2.7. Binding Cache Entry Lookup Considerations

The Binding Cache entry lookup considerations specified in Section 5.4.1.1 of [RFC-5213] is for using the Home Network Prefix as the key

parameter for identifying the Binding Cache entry. When using an IPv4 address with a NON_ZERO value, the exact same considerations specified in Section 5.4.1.1 of [RFC-5213] MUST be applied, with the exception of using an IPv4 home address in place of an IPv6 home network prefix.

3.1.3. Routing Considerations for the Local Mobility Anchor

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

- When the local mobility anchor is serving a mobile node, it MUST be able to receive packets that are sent to any of the mobile node's IPv4 addresses. 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 address or for its home subnet. This essentially enables IPv4 routers in that network to detect the local mobility anchor as the last-hop router for that subnet.

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 when payload protection is not enabled:

```
  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 2: 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.

3.2. Mobile Access Gateway Considerations

3.2.1. Extensions to Binding Update List Entry

For supporting the IPv4 home address mobility feature, the conceptual Binding Update List entry data structure needs to be extended with the following additional fields.

- List of IPv4 home addresses assigned to the mobile node's attached interface. These IPv4 home addresses may have been statically configured in the mobile node's policy profile, or, may have been dynamically allocated by the local mobility anchor through the received Proxy Binding Acknowledgement message. Each of these IPv4 home address entries 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 message.

3.2.2. Extensions to Mobile Node's Policy Profile

For supporting this feature the mobile node's policy profile, specified in Section 6.2 of [RFC-5213] MUST be extended with the following additional fields.

Extensions to the mandatory section of the policy profile:

- This field indicates the scope of IP address mobility support that needs to be extended for the mobile node. If the mobile access gateway should enable support for IPv4, IPv6 or IPv4/IPv6 home address mobility support.

Extensions to the optional section of the policy profile:

- The IPv4 home addresses assigned to the mobile node's attached interface. These addresses have to be maintained on a per-interface basis. The specific details on how the network

maintains the association between the addresses and the interfaces

is outside the scope of this document. These address entries also include the corresponding prefix length.

3.2.3. Signaling Considerations

3.2.3.1. Mobile Node Attachment and Initial Binding Registration

After detecting a new mobile node on its access link, the mobile access gateway on the access link MUST determine if IPv4 home address mobility support needs to be enabled for that mobile node. The mobile node's policy profile specifies if IPv4-only, IPv6-only or IPv4/IPv6 home address mobility service needs to be enabled for that mobile node. Based on those policy considerations, if it is determined that IPv4 home address mobility support is required to be enabled for the mobile node, the considerations from section 6.9.1.1 of [RFC-5213] MUST be applied with the following exceptions.

- The IPv4 Home Address option(s) MUST be present in the Proxy Binding Update request.
  - If the mobile access gateway learns the mobile node's IPv4 home address(es) either from its policy profile, or from other means the mobile access gateway MAY choose to request the local mobility anchor to allocate the requested addresses by including an IPv4 Home Address option for each of those addresses. The IPv4 address and the prefix length fields in the option MUST be set to that specific address and its prefix length. The (P) flag in the option MUST be set to 0.
  - The mobile access gateway MAY also choose to request the local mobility anchor for dynamic home address allocation. It can include exactly one instance of the IPv4 home address option with the IPv4 address value, prefix length fields and (P) flag in the option set to a ALL_ZERO value. This essentially serves as a request to the local mobility anchor for the IPv4 home address allocation.
- The Proxy Binding Update message MUST be constructed as specified in Section 6.9.1.5. However, the Home Network Prefix option(s)

MUST be present in the Proxy Binding Update only if IPv6 home address mobility support also needs to be enabled for the mobile node. Otherwise, the Home Network Prefix option(s) MUST NOT be present.

- When using IPv4 transport for carrying the signaling messages, the related considerations from section 4.0 MUST be applied.

3.2.3.2. Receiving Proxy Binding Acknowledgement

All the considerations from section 6.9.1.2 of [RFC-5213] MUST be applied with the following exceptions.

- If the received Proxy Binding Acknowledgement message has the Status field value set to NOT_AUTHORIZED_FOR_IPV4_HOME_ADDRESS_SUPPORT (The mobile node is not authorized for IPv4 home address support), the mobile access gateway SHOULD NOT send a Proxy Binding Update message including the IPv4 Home Address option(s) till an administrative action is taken.

- If the received Proxy Binding Acknowledgement message has the Status field value set to NOT_AUTHORIZED_FOR_REQ_IPV4_HOME_ADDRESS (The mobile node is not authorized for the requesting IPv4 home address), the mobile access gateway SHOULD NOT request for the same address again, but MAY request the local mobility anchor to do the assignment of address by including exactly one instance if IPv4 Home Address option with the address value set to ALL_ZERO.

- If there is no IPv4 Address Acknowledgement option present in the received Proxy Binding Acknowledgement message, the mobile access gateway MUST NOT enable IPv4 support for the mobile node and the rest of the considerations from this section can be skipped.

- 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 forwarding for that specific IPv4 home address.

- 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 for that mobile node. The entry MUST be updated with the assigned IPv4 home address(es).

- The bi-directional established with the local mobility anchor with IPv4 or IPv6 transport and using any of the supported encapsulation mode, as per [RFC-5213] or as per this specification when using IPv4 transport, MUST be enabled to carry IPv4 traffic.

- The mobile access gateway MUST set up the route for forwarding the IPv4 packets received from the mobile node through the bi-directional tunnel set up for that mobile node.

3.2.3.3. Binding Re-Registration and De-Registrations

When sending a Proxy Binding Update either for extending the lifetime of a mobility session or for de-registering the mobility session, the respective considerations from [RFC-5213] MUST be applied. However, the following additional considerations MUST be applied.

- There MUST be an IPv4 Home Address option for each of the assigned IPv4 home address(es) for that mobility session. The IPv4 address and the prefix length fields in the option MUST be set to that specific address and its prefix length. The (P) flag in the option MUST be set to 0.

- The Home Network Prefix option(s) MUST NOT be present if the same option(s) was not present in the initial Proxy Binding Update message. Otherwise considerations from [RFC-5213] with respect to this option MUST be applied.

3.2.4. Routing Considerations for the Mobile Access Gateway

- On receiving a packet from the bi-directional tunnel established with the mobile node's local mobility anchor, the mobile access gateway MUST remove the outer header before forwarding the packet to the mobile node.

- Considerations from Section 6.10.3 of [RFC-5213] MUST be applied with respect the local routing and on the use of EnableMAGLocalRouting flag.

- On receiving a packet from a mobile node connected to its access link, the packet MUST be forwarded to the local mobility anchor through the bi-directional tunnel established with the local mobility anchor. The encapsulation considerations specified in section 3.1.3 MUST be applied.

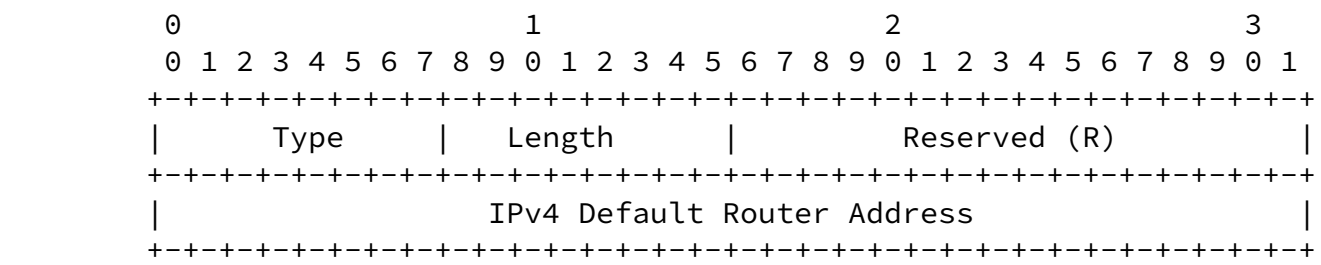
3.3. Mobility Options and Status Codes

For supporting IPv4 home address mobility feature, this specification defines the following new options and Status Codes.

3.3.1. 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 3: IPv4 Default-Router Address Option

3.3.2. Status Codes

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

NOT_AUTHORIZED_FOR_IPV4_HOME_ADDRESS: IANA

Mobile node not authorized for the requesting IPv4 home address

3.4. Supporting DHCP Based Address Configuration

This section explains how DHCP based address configuration support can be enabled for a mobile node in a Proxy Mobile IPv6 domain. It explains the protocol operation, supported DHCP server deployment configurations and the protocol interactions between DHCP agents and mobility entities in each of the supported configurations.

This specification supports the following two DHCP deployment configurations.

- DHCP relay agent co-located with the mobile access gateway.
- DHCP server co-located in the mobile access gateway.

The following are the configuration requirements:

- The DHCP server or the DHCP relay agent configured on the mobile access gateway is required to have an IPv4 address for exchanging the DHCP messages with the mobile node. This address can either the IPv4 Proxy Care-of Address or the mobile node's default-router address provided by the local mobility anchor. Optionally, all the DHCP servers co-located with the mobile access gateways in the Proxy Mobile IPv6 domain can be configured with a fixed IPv4 address. This can be a virtual address used only for the DHCP protocol communication on any of the access links. This address will be the server identifier in the DHCP messages.
- The DHCP server identifies the a DHCP client either from the client identifier or the client hardware address (chaddr). A mobile node in a Proxy Mobile IPv6 domain may present any of these identifiers to the DHCP server as long as the identifier remains the same through out the mobile node's attachment in that Proxy Mobile IPv6 domain. If the client hardware address is used as the identifier and if the mobile node performs an handoff between two interfaces, this hardware identifier will change and the DHCP server will not be able to identify the mobile node. Thus, it is recommended that the DHCP client in the mobile node is configured to use a stable client identifier that does not change during the active life of that DHCP session.
- All the DHCP servers co-located with the mobile access gateways in a Proxy Mobile IPv6 domain SHOULD be configured with the same set

of DHCP option values (Ex: DNS Server, SIP Server ..etc.).

3.4.1. DHCP Server co-located with the Mobile Access Gateway

Figure 4 shows the operational sequence of the home address

assignment when a DHCP server is co-located with the mobile access gateways.

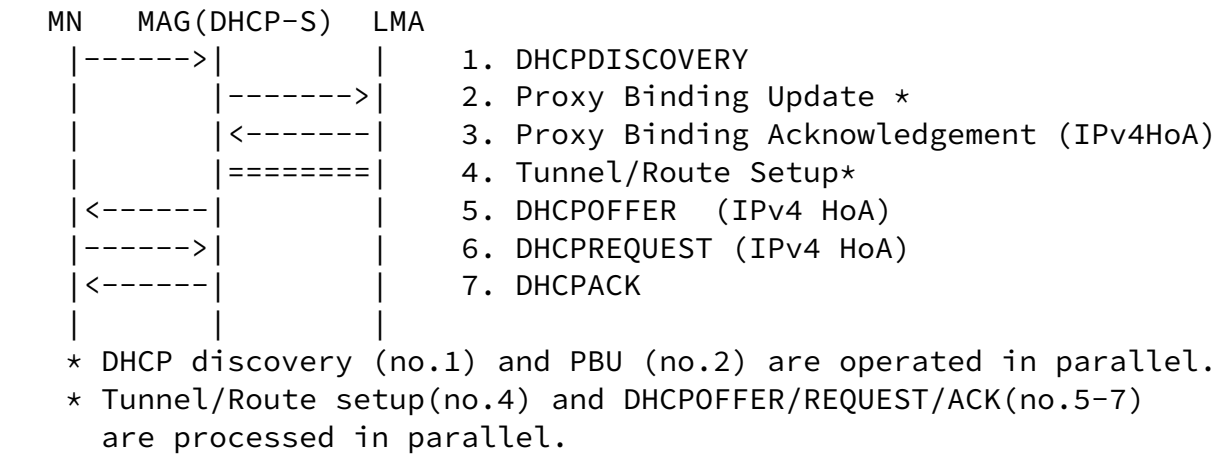


Figure 4: Overview of DHCP Server located at Mobile Access Gateway

Initial IPv4 Home Address Assignment:

- If the mobile node attached to the access link sends a DHCPDISCOVERY message, the DHCP server co-located with the mobile access gateway will trigger the mobile access gateway to complete the Proxy Mobile IPv6 signaling. This is the required interaction between these two protocols. If the mobile access gateway is unable to complete the Proxy Mobile IPv6 signaling or if the local mobility anchor does not assign an IPv4 address for the mobile node, the mobile access gateway MUST tear down the point-to-point link shared with the mobile node.

- After a successful completion of the Proxy Mobile IPv6 signaling and acquiring the mobile node's IPv4 home address assigned by the local mobility anchor, the DHCP server on the mobile access gateway will send a DHCP offer message to the mobile node. The offered address will the mobile node's IPv4 home address, assigned by the local mobility anchor. The 'siaddr' field of the DHCPOFFER message will be set to the mobile node's default-router address or to the globally fixed address used for all DHCP servers. The DHCPOFFER message will be unicasted to the mobile node.

o If the mobile node sends the DHCPREQUEST message, the DHCP server will send DHCPACK message, as per [RFC-2131].

IPv4 Home Address Renewal with the DHCP server (No Handoff):

o When the DHCP client goes into the DHCP-RENEWING-STATE [RFC-2131], it simply unicasts DHCPREQUEST message including the assigned IPv4 home address in the 'requested IPv4 address' option. The DHCPREQUEST is sent to the address specified in 'server identifier' field of the previously received DHCPOFFER and DHCPACK messages.

o The DHCP server will send a DHCPACK to the mobile node.

IPv4 Home Address Renewal with the different DHCP server (After Handoff):

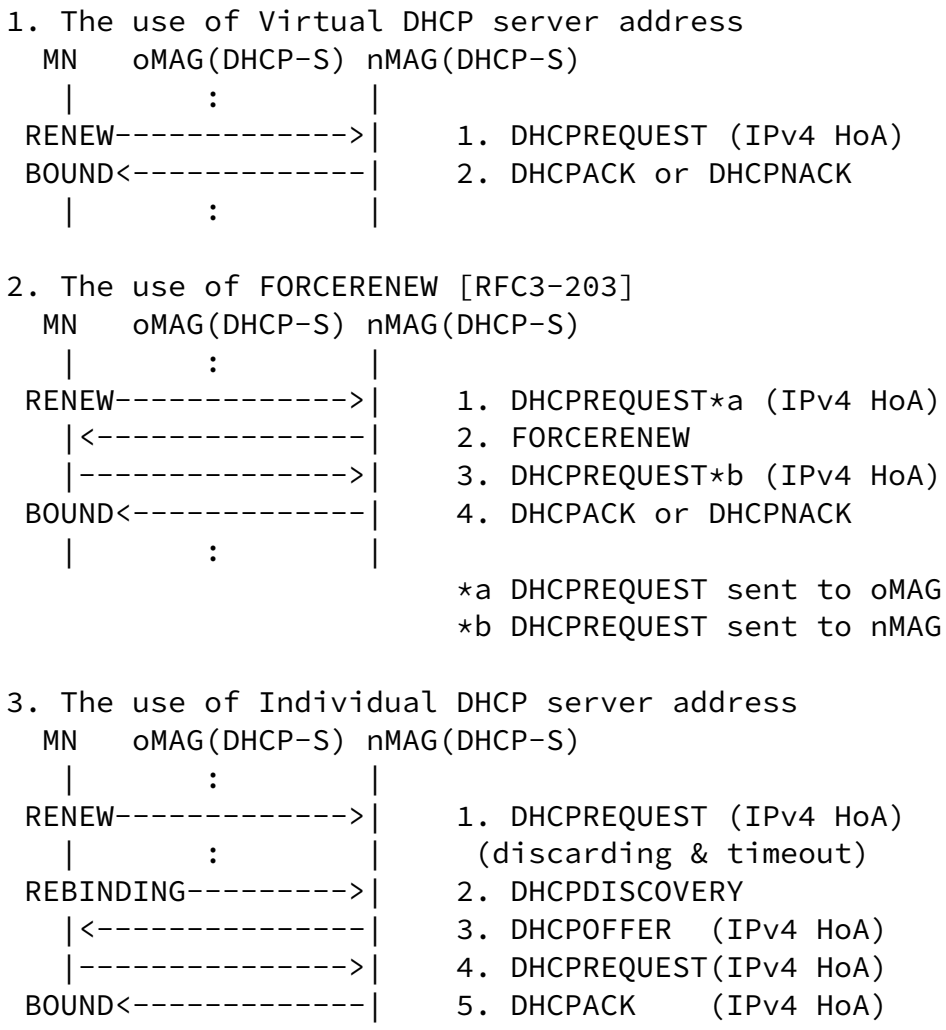


Figure 5: Renewing Address to different DHCP server

- When the DHCP client goes into the DHCP-RENEWING-STATE [RFC-2131], it directly unicasts DHCPREQUEST message to the DHCP server. If the mobile node moves and attaches to a new mobile access gateway, it needs to update the DHCP server address to the new one (i.e. the address of the currently attached mobile access gateway). Thus, one of following operations is required.

- If the IPv4 virtual DHCP address is used, the DHCPREQUEST for renewing address is received by the mobile access gateway to which the mobile node is currently attached. The mobile access gateway SHOULD reply DHCPACK or DHCPNACK depending on the correctness of the requesting IPv4 home address in the DHCPREQUEST as shown in Figure 5-1).

- If the IPv4 virtual DHCP address is not used, the mobile node reconfigures the DHCP server address whenever it changes the attached mobile access gateway.

  * If a mobile access gateway receives any DHCP messages unicasted to a different mobile access gateway from the mobile node, it SHOULD unicast FORCERENEW message [RFC-3203] to the mobile node as shown in Figure 5-2). In the FORCERENEW, the 'server identifier' field MUST be overwritten by the IPv4 address of the current mobile access gateway so that the client can update the DHCP server address.

  * If the IPv4 virtual DHCP address is not used and the FORCERENEW [RFC-3203] is not supported at the mobile access gateway, the mobile access gateway SHOULD discard any DHCPREQUEST message sent not to the mobile access gateway itself, so that the mobile node should go into the DHCP-REBINDING-STATE and broadcast DHCPDISCOVERY without server identifier as shown in Figure 5-3).

Additional Operation:

- o At an point the mobile access gateway fails to extend the binding lifetime with the local mobility anchor, it MUST send an unsolicited DHCPNACK to the mobile node. It MUST also tear down the point-to-point link shared with the mobile node.

3.4.2. DHCP Relay Agent co-located with the Mobile Access Gateway

A DHCP relay is co-located with each mobile access gateway. A DHCP server is located somewhere in the Proxy Mobile IPv6 domain or is co-located with the local mobility anchor. Figure 6 are the sequence of IPv4 home address assignment using DHCP Relay.

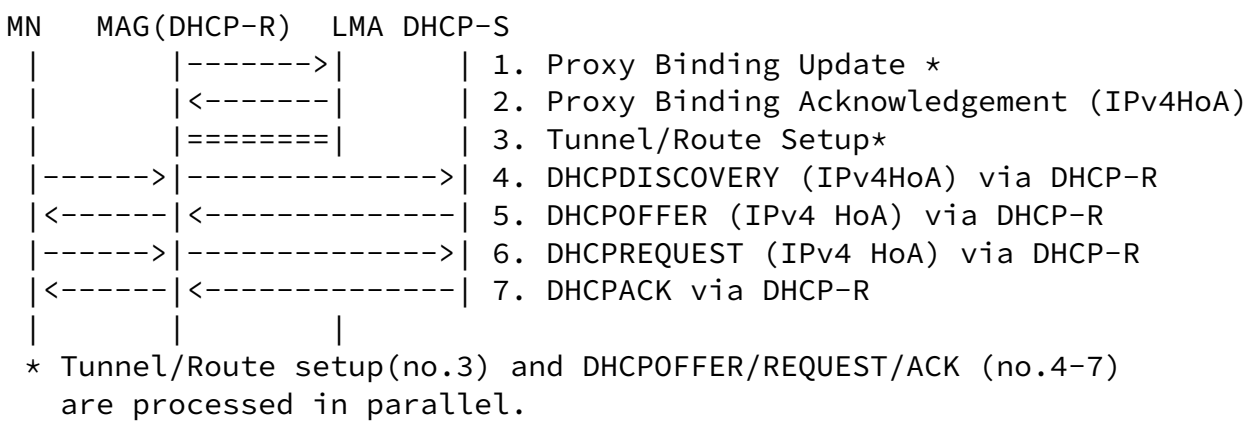


Figure 6: Overview of the DHCP relay located at mobile access gateway

Initial IPv4 Home Address Assignment:

- o When the mobile access gateway receives a DHCPDISCOVERY message from a mobile node, it MUST check whether it has already obtained the IPv4 home address for the mobile node from the local mobility anchor.

- o If the IPv4 home address is not yet assigned by the local mobility anchor, the mobile access gateway MUST send a Proxy Binding Update for that.

- If the IPv4 home address is not assigned to the mobile node by the local mobility anchor due to administrative policy or resource limitation, it MUST discard the DHCPDISCOVERY messages from the mobile node.

- Otherwise, it MUST add the DHCP relay agent information option [RFC-3046] to the DHCPDISCOVERY message. The assigned IPv4 home address (32-bit full address) is included in the Agent Remote ID Sub-option of the DHCP relay agent information option. This sub-option is used as a hint of address assignment of the DHCP server.

- When the mobile access gateway receives the DHCPOFFER from the DHCP server, it MUST verify whether the DHCP server offers the

  correct IPv4 home address which is indicated in the Agent Remote ID Sub-option of the DHCPDISOCVERY. If the DHCP server offers the different address from the expected address, the mobile access gateway MUST drop the DHCPOFFER.

- After the successful relaying the DHCPOFFER, the mobile access gateway acts as a regular DHCP relay agent as [RFC-2131].

- As shown in Figure 6, the DHCP messages MAY be sent across an administrative boundaries. The operators MUST ensure to secure these messages. All the DHCP messages relayed by the mobile access gateway can be tunneled over the local mobility anchor if needed. Alternatively, if the networks in the Proxy Mobile IPv6 domain are secured enough, the mobile access gateway just relays the DHCP messages to the server without the tunnel. For doing this, all the mobile access gateway MUST have the route toward the DHCP server. More remarks can be found in Section 7.

IPv4 Home Address Renewal to the same DHCP server: (No Hanover)

- When the DHCP client goes into the DHCP-RENEWING-STATE [RFC-2131], it directly unicasts DHCPREQUEST message to the DHCP server. The DHCP relay agent cannot receive the DHCPREQUEST for renewing addresses. Thus, one of following operations is required.

  * The DHCP relay agent SHOULD intercept all the DHCP packets regardless of the destination address. Since the link between

a mobile node and a mobile access gateway is the point-to-point link, it is possible to check the DHCP packets at the interface by enabling the promiscuous mode.

* The cost of packets monitoring is not negligible. Therefore, The DHCP relay agent MAY use the DHCP Server Identifier Override Sub-option [RFC-5107] to intercept DHCPREQUESTs for the address renewal. The DHCP client uses the DHCP server address which is overridden by the DHCP relay agent address as a destination address of DHCPREQUEST. The DHCP Server Identifier Override Sub-option is recommended only when the Virtual DHCP address is configured on all the mobile access gateways. Otherwise, the DHCP relay agent address is changed when the mobile node changes the attached mobile access gateway. As a result, the DHCP relay agent MUST monitor DHCP packets by force as described above.

o Once the DHCP relay agent intercepts the DHCPREQUEST from the mobile node, it MUST verify the requesting IPv4 home address stored in the DHCPREQUEST message. The verification is operated

by checking it with the binding update list for the mobile node. If the requesting IPv4 home address is not registered to the local mobility anchor, the mobile access gateway MUST NOT relay the DHCPREQUEST and MUST discard it.

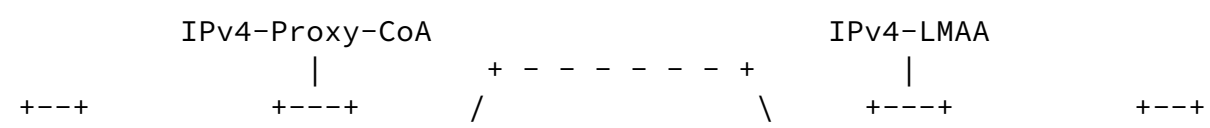
o If the address verification is successfully completed, the DHCP relay agent SHOULD forward the DHCPREQUEST to the DHCP server.

Additional Operations:

o If the mobile access gateway sends Proxy Binding Update for the IPv4 home address and receives the unsuccessful Proxy Binding Acknowledgement (by indicating the error codes), it MUST send unsolicited DHCPNACK for the invalid IPv4 home address to the mobile node. XXXX

4. IPv4 Transport Support

The Proxy Mobile IPv6 specification [RFC-5213] requires 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 only IPv4 addresses.



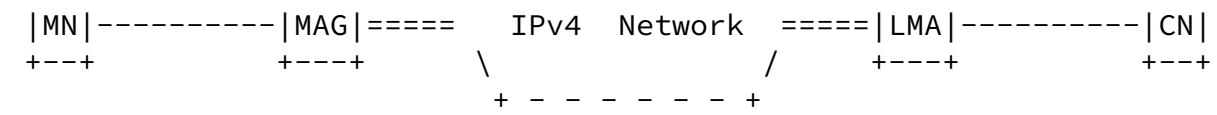


Figure 7: IPv4 Transport Network

When the local mobility anchor and the mobile access gateway are configured and reachable using only IPv4 addresses, the mobile access gateway serving a mobile node can potentially send the signaling messages over IPv4 transport and register its IPv4 address as the care-of address in the mobile node's Binding Cache entry. An IPv4 tunnel (with any of the supported encapsulation modes) can be used for tunneling the mobile node's data traffic. The following are the key aspects of this feature.

- The local mobility anchor and the mobile access gateway are both configured and reachable using only an IPv4 address. Additionally, both these entities are also IPv6 enabled and have configured IPv6 addresses on its interfaces, as specified in [RFC-5213], but are reachable only over an IPv4 transport.

- The mobile access gateway can be potentially in a private IPv4 network behind a NAT [RFC-3022] device, with a private IPv4 address configured on its egress interface. However, the local mobility anchor must not be behind a NAT and must be using a globally routable IPv4 address.

- 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 using the mobility header and the related semantics

  as specified in base Proxy Mobile IPv6 specification [RFC-5213], but carried as a payload in an IPv4 packet (IPv4-UDP encapsulation mode).

- 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 that mobile node.

- The IPv4 tunnel established between the local mobility anchor and the mobile access gateway (with any of the supported encapsulation modes over IPv4 transport) will be used for carrying the mobile node's IPv4 and IPv6 traffic. The supported encapsulation modes for carrying mobile node's IPv4 or IPv6 packets when using IPv4 transport are as shown below.

  * IPv4

  * IPv4-UDP (Payload packet carried in an IPv4 packet with UDP header)

  * IPv4-UDP-TLV (Payload packet carried in an IPv4 packet with UDP and TLV header. Refer to [ID-DSMIP6]).

  * IPv4-UDP-ESP (Payload packet carried in an IPv4 packet with UDP and ESP headers. Refer to [RFC-3948].

4.1. Local Mobility Anchor Considerations

4.1.1. Extensions to Binding Cache Entry

For supporting this feature, the conceptual Binding Cache entry data structure maintained by the local mobility anchor [RFC-5213] MUST be extended with the following additional parameters.

- The IPv4 address of the mobile access gateway. This is the address configured on the egress interface of the mobile access gateway that sent the Proxy Binding Update message. This address can be obtained from the IPv4 Care-of Address option, present in the received Proxy Binding Update message. If the option was not present in the request, this field MUST be set to the source address of the IPv4 header of the received Proxy Binding Update message. However, if the received Proxy Binding Update message is not sent as an IPv4 packet, this field MUST be set to ALL_ZERO value.

- The IPv4 NAT translated address of the mobile access gateway. If the mobile access gateway is not behind a NAT [RFC-3022], this address will be the same as the address configured on the egress

interface of the mobile access gateway. This address can be obtained from the IPv4 header of the received Proxy Binding Update message. However, if the received Proxy Binding Update message is not sent as an IPv4 packet, this field MUST be set to ALL_ZERO value.

4.1.2. Extensions to Mobile Node's Policy Profile

For supporting this feature the mobile node's policy profile, specified in Section 6.2 of [RFC-5213] MUST be extended with the following additional fields. This are mandatory fields of the policy profile required for supporting this feature.

- A flag indicating if IPv4 transport should be used. The value of this flag can be different at different mobile access gateway. The specific details on how this flag is maintained on a per mobile access gateway basis is outside the scope of this document.

- The IPv4 address of the local mobility anchor (IPv4-LMAA).

4.1.3. Signaling Considerations

This section provides the rules for processing the Proxy Mobile IPv6 signaling messages received over IPv4 transport. The local mobility anchor MUST apply these signaling rules on the IPv4 UDP encapsulated Proxy Binding Update messages received on DSMIP UDP port [ID-DSMIP6].

4.1.3.1. Processing Proxy Binding Updates

- If the received Proxy Binding Update message (encapsulated in IPv4 UDP packet) is protected using IPsec ESP header, then the message MUST be authenticated as described in Section 4 of [RFC-5213]. However, if the IPv4 packet is not protected using IPsec ESP header, then the message MUST be authenticated after removing the outer IPv4 UDP header.

- All the considerations from Section 5.3.1 of [RFC-5213] MUST be applied on the encapsulated Proxy Binding Update message, after removing the outer IPv4 UDP header.

- If there is an IPv4 Care-of Address present in the request, the NAT presence detection procedure specified in Section 4.1.3.3 MUST be used for detecting the NAT in the path.

- Upon accepting the request, the local mobility anchor MUST set up an IPv4 bi-directional tunnel to the mobile access gateway. The tunnel endpoint addresses are IPv4-LMAA and the IPv4-Proxy-CoA. The encapsulation mode MUST be determined from the below

considerations.

* If the NAT is detected on the path, then the encapsulation mode for the tunnel MUST be set to IPv4-UDP. Otherwise the encapsulation mode MUST be set to IPv4. However, if the (F) flag in the received Proxy Binding Update message is set to value of 1 and even if NAT is not detected, then the encapsulation mode MUST be set to IPv4-UDP.

* If the (T) flag in the Proxy Binding Update message is set to value of 1, then the encapsulation mode MUST be set to IPv4-UDP-TLV.

o The local mobility anchor MUST send the Proxy Binding Acknowledgement message with the Status field value set to 0 (Proxy Binding Update Accepted). The message MUST be constructed as specified in Section 4.1.3.2.

4.1.3.2. 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 Section 5.3.6 of [RFC-5213]. However, if the received Proxy Binding Update message was encapsulated in an UDP header of an IPv4 packet, the following additional considerations MUST be applied.

o The NAT Detection option [ID-DSMIP6] MUST be present only if there is a IPv4 Care-of Address option present in the received Proxy Binding Update and if the NAT detection procedure resulted in detecting a NAT on path. In all other cases, the option MUST NOT be present.

o The Proxy Binding Acknowledgement message MUST be encapsulated in an UDP header of an IPv4 packet.

o The source address in the IPv4 header of the message MUST be set to the destination IPv4 address of the received request.

o If the mobile access gateway and the local mobility anchor are using globally routable IPv4 addresses and if there is a security associated that is based of IPv4 addresses, then the encapsulated IPv4 packet (containing the IPv6 PBA) MUST be protected using

IPsec ESP [RFC-4301] mode and additionally there is no need to apply IPsec ESP header on the IPv6 packet. In all other cases, the Proxy Binding Acknowledgement message MUST be protected using IPsec prior to the IPv4 UDP encapsulation.

- The format of the Proxy Binding Acknowledgement message encapsulated in an IPv4 UDP packet and protected using IPv6 security association.

```
IPv4 header (src=IPv4-LMAA, dst=pbu_src_address)
   UDP header (sport=DSMIP_PORT, dport= pbu_sport)
       /* IPv6 PBU Packet protected with ESP header */
```

Figure 8: Proxy Binding Acknowledgment Message encapsulated in IPv4 header

- The format of the Proxy Binding Acknowledgement message encapsulated in an IPv4 UDP packet and protected using IPv4 security association.

```
IPv4 header (src=IPv4-LMAA, dst=pbu_src_address)
   ESP Header
      UDP header (sport=DSMIP_PORT, dport= pbu_sport)
         /* IPv6 PBU Packet protected with no ESP header */
```

Figure 9: Proxy Binding Acknowledgment encapsulated in IPv4 ESP header

4.1.3.3. NAT Presence Detection

When the transport network between the local mobility anchor and the mobile access gateway is an IPv4 network, the mobile access gateway will send the Proxy Binding Update messages 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 DSMIPv6 specification [ID-DSMIP6].

4.1.4. Routing Considerations

4.1.4.1. Forwarding Considerations

Forwarding Packets to the Mobile Node:

- On receiving an IPv4 or an IPv6 packet from a correspondent node with the destination address matching any of the mobile node's IPv4 or IPv6 home addresses, the local mobility anchor MUST forward the packet through the bi-directional tunnel set up for that mobile node.

- The format of the tunneled packet is shown below.

```
IPv4 Header (src= IPv4-LMAA, dst= IPv4-Proxy-CoA)] /* Tunnel Header */
  [UDP Header (src port=DSMIPv6, dst port=Z]   /* If UDP encap nego */
    [TLV Header]                               /* If TLV negotiated */
      /* IPv6 or IPv4 Payload Packet */
             IPv6 header (src= CN, dst= MN-HOA)
                        OR
             IPv4 header (src= CN, dst= IPv4 MN-HoA)
```

Figure 10: Tunneled IPv4 Packet from LMA to MAG

- Forwarding Packets Sent by the Mobile Node:

  * All the reverse tunneled packets (IPv4 and IPv6) that the local

mobility anchor receives from the mobile access gateway, after removing the tunnel header (i.e., the outer IPv4 header along with the UDP and TLV header, if negotiated) MUST be routed to the destination specified in the inner packet header. These routed packets will have the source address field set to the mobile node's home address.

4.1.4.2. ECN Considerations

The ECN considerations specified in Section 5.6.3 of [RFC-5213] apply for the IPv4 transport tunnels as well. The mobility agents at the tunnel entry and exit points MUST handle ECN information as specified in that document.

4.1.4.3. Bi-Directional Tunnel Management

The Tunnel Management considerations specified in section 5.6.1 of [RFC-5213] apply for the IPv4 transport tunnels as well, with just one difference that the encapsulation mode is different.

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 maintained by the mobile access gateway [RFC-5213] MUST be extended with the following additional parameters.

- The IPv4 address of the local mobility anchor. This address can be obtained from the mobile node's policy profile.

- The IPv4 address of the mobile access gateway. This is the address configured on the egress interface of the mobile access gateway and is registered with the mobile node's local mobility anchor as the IPv4 Proxy-CoA. However, if the mobile access gateway is in a private IPv4 network and behind a NAT, the address that is registered with the mobile node's local mobility anchor is the NAT translated public IPv4 address.

4.2.2. Signaling Considerations

The mobile access gateway when sending a Proxy Binding Update message

to the local mobility anchor MUST construct the message as specified in Section 6.9.1.5. However, if the mobile access gateway is in an IPv4-only access network, the following additional considerations MUST be applied.

- The Proxy Binding Update message MUST be encapsulated in an UDP header of an IPv4 packet.

- The IPv4 Care-of Address option [ID-DSMIP6] MUST be present. The IPv4 address in the option MUST be set to the mobile access gateway's IPv4-Proxy-CoA.

- The packet MUST be constructed as specified in Section 4.2.3.

- When sending a Proxy Binding message for extending the lifetime of a currently existing mobility session or for de-registering the mobility session, the Proxy Binding Update message MUST be constructed as the initial request.

Receiving Proxy Binding Acknowledgement

- If the received Proxy Binding Acknowledgement message (encapsulated in IPv4 UDP packet) is protected using IPsec ESP header, then the message MUST be authenticated as described in Section 4 of [RFC-5213]. However, if the IPv4 packet is not

protected using IPsec ESP header, then the message MUST be authenticated after removing the outer IPv4 UDP header.

- All the considerations from Section 6.9.1.2 of [RFC-5213] MUST be applied on the encapsulated Proxy Binding Acknowledgement message, after removing the outer IPv4 UDP header.

- If the Status field indicates Success, the mobile access gateway MUST setup a bi-directional tunnel to the local mobility anchor.

- Upon accepting the request, the local mobility anchor MUST set up an IPv4 bi-directional tunnel to the mobile access gateway. The tunnel endpoint addresses are IPv4-LMAA and the IPv4-Proxy-CoA. The encapsulation mode MUST be determined from the below considerations.

* If there is a NAT Detection option [ID-DSMIP6] in the received Proxy Binding Acknowledgement message, then the encapsulation mode for the tunnel MUST be set to IPv4-UDP. Otherwise the encapsulation mode MUST be set to IPv4.

* If the (T) flag in the Proxy Binding Acknowledgement message is set to value of 1, then the encapsulation mode MUST be set to IPv4-UDP-TLV.

4.2.2.1. Constructing the Proxy Binding Update Message

- The source address in the IPv4 header MUST be set to IPv4-Proxy-CoA of the mobile access gateway and the destination address MUST be set to the local mobility anchor's IPv4-LMAA.

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

- If the configuration variable ForceIPv4UDPEncapsulationSupport is set to value of 1, then the (F) flag in the Proxy Binding Update message MUST be enabled.

- If the mobile access gateway and the local mobility anchor are using globally routable IPv4 addresses and if there is a security associated that is based of IPv4 addresses, then the encapsulated IPv4 packet (containing the IPv6 PBU) MUST be protected using IPsec ESP [RFC-4301] mode and additionally there is no need to apply ESP header on the IPv6 packet. In all other cases, the Proxy Binding Update message MUST be protected on the IPv6 packet of the Proxy Binding Update message, prior to the IPv4 encapsulation.

- The format of the Proxy Binding Update message encapsulated in an IPv4 UDP packet with IPsec protection on the encapsulated packet:

```
IPv4 header (src=IPv4-Proxy-CoA, dst=IPv4-LMAA)
   UDP header (sport=ANY, dport= DSMIP_PORT)
       /* IPv6 PBU Packet protected with ESP header */
```

Figure 11: Proxy Binding Update Message encapsulated in IPv4 UDP header

- The format of the Proxy Binding Update message encapsulated in an IPv4 UDP packet and with IPsec protection on the encapsulated packet:

```
IPv4 header (src=IPv4-Proxy-CoA, dst=IPv4-LMAA)
   ESP Header
      UDP header (sport=ANY, dport= DSMIP_PORT)
         /* IPv6 PBU Packet protected with no ESP header */
```

Figure 12: Proxy Binding Update Message Encapsulated with IPsec protection

4.2.2.2. Forwarding Considerations

Forwarding Packets Sent by the Mobile Node:

- On receiving an IPv4 or an IPv6 packet from the mobile node to any destination, the mobile access gateway MUST tunnel the packet to the local mobility anchor. The format of the tunneled packet is shown below. However, considerations from Section 6.10.3 of [RFC-5213] MUST be applied with respect the local routing and on the use of EnableMAGLocalRouting flag.

```
IPv4 Header (src= IPv4-Proxy-CoA, dst= IPv4-LMAA)] /* Tunnel Header */
   [UDP Header (src port=DSMIPv6, dst port=Z]   /* If UDP encap nego */
       [TLV Header]                             /* If TLV negotiated */
            /* IPv6 or IPv4 Payload Packet */
            IPv6 header (src= CN, dst= MN-HOA)
                        OR
            IPv4 header (src= CN, dst= IPv4 MN-HoA)
```


Figure 13: Tunneled IPv4 Packet from LMA to MAG

- Forwarding Packets received from the bi-directional tunnel:

- On receiving a packet from the bi-directional tunnel established with the mobile node's local mobility anchor, the mobile access gateway MUST remove the outer header before forwarding the packet to the mobile node.

5. Protocol Configuration Variables

5.1. Local Mobility Anchor - Configuration Variables

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

AcceptIPv4UDPEncapsulationRequest

This flag indicates whether or not the local mobility anchor should accept IPv4 UDP encapsulation support if there is NAT detected in the path.

The default value for this flag is set to value of 1, indicating that the local mobility anchor MUST enable IPv4 UDP encapsulation support on detecting NAT in the path.

When the value for this flag is set to value of 0, the local mobility anchor MUST NOT enable IPv4 UDP encapsulation support.

5.2. Mobile Access Gateway - Configuration Variables

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

RequestIPv4UDPEncapsulationSupport

This flag indicates whether or not the mobile access gateway should request the mobile node's local mobility anchor for IPv4 UDP encapsulation support if NAT is detected in the path.

The default value for this flag is set to value of 0, indicating that the mobile access gateway MUST NOT request the mobile node's local mobility anchor for IPv4 UDP encapsulation support.

When the value for this flag is set to value of 1, the mobile access gateway MUST request the mobile node's local mobility anchor for IPv4 UDP encapsulation support if there is NAT detected in the path.

ForceIPv4UDPEncapsulationSupport

This flag indicates whether or not the mobile access gateway should request the mobile node's local mobility anchor for forcing IPv4 UDP encapsulation support even when NAT is not detected in path.

The default value for this flag is set to value of 0, indicating that the mobile access gateway MUST NOT request the mobile node's local mobility anchor for forcing IPv4 UDP encapsulation support even when NAT is not detected in path.

When the value for this flag is set to value of 1, the mobile access gateway MUST force the mobile node's local mobility anchor for IPv4 UDP encapsulation support.

This flag is applicable only when the flag RequestIPv4UDPEncapsulationSupport is set to a value of 1.

5.3. Proxy Mobile IPv6 Domain - Configuration Variables

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

FixedDHCPServerId

This variable indicates the DHCP server id that all the DHCP servers co-located with the mobile access gateways SHOULD configure in that Proxy Mobile IPv6 domain. If this variable is initialized to ALL_ZERO value, it implies the use of fixed address is not enabled for that Proxy Mobile IPv6 domain.

6. IANA Considerations

This document defines a new Mobility Header option, IPv4 Default Router Address option. This option is described in Section 3.3.1. The Type value for this option needs to be assigned from the same numbering space as allocated for the other mobility options, as defined in [RFC-3775].

This document also defines new Binding Acknowledgement status values, as described in Section 3.3.2. The status values MUST be assigned from the same number space used for Binding Acknowledgement status values, as defined in [RFC3775]. The allocated values for each of these status values must be greater than 128.

7. Security Considerations

All the security considerations from the base Proxy Mobile IPv6 protocol [RFC-5213] apply when using the extensions defined in this document. Additionally, the following security considerations need to be applied.

This document defines news mobility options for supporting the IPv4 Home Address assignment and IPv4 Transport Support features. It also uses some of the mobility options from DSMIPv6 specification [ID-DSMIP6]. These options are to be carried in Proxy Binding Update and Proxy Binding Acknowledgement messages. The required security mechanisms specified in the base Proxy Mobile IPv6 protocol for protecting these signaling messages are sufficient when carrying these mobility options.

This specification describes the use of IPv4 transport for exchanging the signaling messages between the local mobility anchor and the mobile access gateway. These messages are protected using IPsec using the security associations established using the IPv4 transport addresses and offer the same security as when the messages are protected when using IPv6 transport.

8. 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

9. Acknowledgments

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

Thanks to Jonne Soinnen, Julien Laganier, Zu Qiang, Premec Domagoj, Sammy Touati and Niklas Nuemann for their helpful review of this document.

10. References

10.1. 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.

[ID-DSMIP6] Soliman, H. et al, "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)", draft-ietf-mip6-mext-nemo-v4traversal-05.txt,July 2008.

[RFC-5213] Gundavelli, S., et.al, "Proxy Mobile IPv6", RFC 5213,

November 2007.

10.2. Informative References

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

[RFC-3011] G. Waters, "The IPv4 Subnet Selection Option for DHCP", RFC 3011, November 2000.

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

[RFC-3203] Y. T'Joens and C. Hublet and P. De Schrijver, "DHCP reconfigure extension", RFC 3203, December 2001.

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

[RFC-5107] R. Johnson and J. Jumarasamy and K. Kinnear and M. Stapp, "DHCP Server Identifier Override Suboption", RFC 5107, February 2008.

Authors' Addresses

Ryuji Wakikawa
Toyota ITC / Keio University

6-6-20 Akasaka, Minato-ku
Tokyo 107-0052
Japan

Phone: +81-3-5561-8276
Fax: +81-3-5561-8292
Email: ryuji@jp.toyota-itc.com

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).