Independent Submission
Request for Comments: 5563
Category: Informational
ISSN: 2070-1721

K. Leung
G. Dommety
Cisco Systems
P. Yegani
Juniper Networks
K. Chowdhury
Starent Networks
February 2010

WiMAX Forum / 3GPP2 Proxy Mobile IPv4

Abstract

Mobile IPv4 is a standard mobility protocol that enables an IPv4 device to move among networks while maintaining its IP address. The mobile device has the Mobile IPv4 client function to signal its location to the routing anchor, known as the Home Agent. However, there are many IPv4 devices without such capability due to various reasons. This document describes Proxy Mobile IPv4 (PMIPv4), a scheme based on having the Mobile IPv4 client function in a network entity to provide mobility support for an unaltered and mobility-unaware IPv4 device. This document also describes a particular application of PMIPv4 as specified in the WiMAX Forum and another application that is to be adopted in 3GPP2.

Status of This Memo

Table of Contents

1. Introduction

There are many IPv4 devices that do not have or cannot be enabled with Mobile IPv4 [RFC3344] functionality. Yet, mobility for them is essential. Proxy Mobile IPv4 provides mobility support without "touching" these devices. The scheme is based on network entities that perform the mobility-management function for a mobile device. The location of the device is signaled by the network element on the access network (referred to as the Proxy Mobility Agent (PMA)) to inform the network entity on the home network (referred to as the Home Agent (HA)) associated with the IPv4 address used by the device. Mobile IPv4 messaging is used by the PMA and HA, which correspond to the RFC 3344 entities Mobile Node (in proxy mode) and Home Agent, respectively.

These are some examples of Proxy Mobile IPv4:

1. A Wireless Local Area Network (WLAN) access point or cellular base station performs registration with the Home Agent when a mobile device is associated on the air-link.

2. An access router or Foreign Agent performs registration with the Home Agent when a mobile device is detected on the network.

Mobile IPv4 is used by the network entities because the mobility protocol has the functions needed to set up the route and tunneling endpoints for the mobile device’s IP address and to deliver configuration parameters (e.g., DNS server addresses, default gateway) for enabling the mobile device’s IP stack. When Mobile IPv4 is used in this way, the security association is between the PMA and

the HA because these entities are the signaling endpoints. Also, when the mobile device moves to a new PMA, the sequencing of messages sourced from multiple PMAs needs to be handled properly by the HA.

This document describes how the network entities, PMA and HA, provide mobility management for the mobile device. It is organized to cover the generic functionality of Proxy Mobile IPv4 and also the specifics pertaining to WiMAX (Section 10) and 3GPP2 (Section 11).

Note that Proxy Mobile IPv6 [RFC5213] is an IETF standard for network-based mobility management that enables IP mobility for a host without requiring its participation in any mobility-related signaling.

2. Conventions Used in This Document

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

The following new terminology and abbreviations are introduced in this document; all other general mobility-related terms are as defined in Mobile IPv4 specification [RFC3344].

Mobile Device

The mobile device is used to refer to an IPv4 device with its mobility provided by the network. The mobile device is not required to participate in any mobility-related signaling for achieving mobility for an obtained IP address.

Proxy Mobile IPv4 Client (PMIPv4 Client)

This network function is responsible for initiating and maintaining the Proxy Mobile IPv4 registration on behalf of the mobile device. Essentially, it performs the Mobile IPv4 client function but is hosted in the network. In some cases, this function is collocated with the Foreign Agent; in others, it is not. In both cases, Proxy Mobile IPv4 registration still goes via the Foreign Agent at all practical effects, even if it is internal to the node.

Home Agent (HA)

The Home Agent that is defined in Mobile IPv4 [RFC3344] is used in the Proxy Mobile IPv4 scheme. It is the topological anchor point for the mobile device’s home network and is the entity that manages the mobile device’s reachability state. The additional

capabilities for supporting Proxy Mobile IPv4 in the Home Agent are defined in this document.

Foreign Agent (FA)

The Foreign Agent that is defined in [RFC3344] is used in the Proxy Mobile IPv4 scheme. It is either collocated with or separate from the PMIPv4 client. It serves the purpose of tunnel endpoint from Proxy Mobile IPv4 perspective.

Access Router (AR)

Access Router is a commonly used term that refers to the node in the network that connects the hosts to the IP network.

Proxy Mobility Agent (PMA)

Proxy Mobility Agent is the logical entity in the network that encompasses both the PMIPv4 client and the FA functions. The PMIPv4 client and the FA collocation in the Access Router constitute an integrated PMA. When the PMIPv4 client and the FA functions are not collocated in the Access Router, it is referred to as a split PMA. A PMIPv4 client may have association with multiple FAs, and vice versa.

Proxy Registration Request (PRRQ)

The Registration Request message is sent by the Proxy Mobility Agent to the Home Agent in order to set up a mobility binding entry for a mobile device. The message format is identical to that of the Mobile IPv4 Registration Request, though the Proxy Mobile IPv4 extensions that are defined in this document may be included for enhanced features of network-based mobility management.

Proxy Registration Reply (PRRP)

The Registration Reply message is sent by the Home Agent in response to the Proxy Registration Request received from the Proxy Mobility Agent. The message format is identical to that of the Mobile IPv4 Registration Reply, though the Proxy Mobile IPv4 extensions that are defined in this document may be included for enhanced features of network-based mobility management.

3. Benefits of Proxy Mobile IPv4

Proxy Mobile IPv4 (PMIPv4) is designed to satisfy the requirements listed below. In addition, while this specification and Proxy Mobile IPv4 are not standards, they employ a standard: Mobile IPv4. Implementations of Mobile IPv4 can be re-used (i.e., a client-based mobility protocol can be used "as-is" to support network-based mobility). However, new PMIPv4 extensions that are added to Mobile IPv4 improves the flexibility of the solution. The practical advantage of having a common mobility protocol for both client-based and network-based mobility is that a Home Agent can anchor all types of mobile devices, both ones that have and ones that lack the Mobile IPv4 function.

The network-based mobility management solution defined in this document has the following significant reasons for its use in any wireless network:

1. Support for Unmodified Hosts

   An overwhelming majority of IPv4 hosts do not have Mobile IPv4 capability. Providing mobility for them is achievable using Proxy Mobile IPv4. This is accomplished without "touching" the user’s devices by running on a myriad of operating systems and networking stacks.

2. Re-Use of Existing Home Agent

   An existing Home Agent implementation can be used for network-based mobility as well. Further enhancements are optional and only incremental in nature. There are many commonalities between client-based and network-based mobility, and sharing the same protocol is a significant benefit.

3. Reduction of Air-Link Resource Consumption

   Mobility-related signaling over the air-link is eliminated.

4. Support for Heterogeneous Wireless Link Technologies

   Since Proxy Mobile IPv4 is based on an access, technology-independent, mobility protocol, it can be used for any type of access network.

   From the network perspective, a mobile device is identified by the Network Access Identifier (NAI) and the forwarding is set up between the PMA and HA for the mobile device’s current point of attachment on the network. The mobile device may be attached to

multiple networks concurrently, although the network treats each access interface independently. This feature can be supported with the use of the PMIPv4 Access Technology Type Extension (Section 5.5).

5. Support for IPv4 and IPv6 Hosts

As IPv6 increases in popularity, the host will likely be dual stack. Adding IPv6 support to the host for Proxy Mobile IPv4 involves the methods defined in [RFC5454]. There are additional enhancements needed, which are described in "Proxy Mobile IPv6" [RFC5213]. However, support for an IPv6 host is out of the scope of this document.

4. Overview of Proxy Mobile IPv4

4.1. Mobility Signaling for Mobile Device

After the mobile device completes network-access authentication, the PMA exchanges Proxy Mobile IPv4 registration messages with the HA to set up proper routing and tunneling of packets from/to the Mobile Node. The PMIPv4 client is responsible for initiating the Proxy Mobile IPv4 registration. For integrated PMA, the PMIPv4 client and the FA interaction is all within the node. In the case of split PMA implementation, the interactions between the PMIPv4 client and the FA are exposed. The interface between the PMIP Client and the FA in the split PMA scenario is defined in a standards organization specification [NWG] and is consequently out of the scope of this document.

The following call flows describe the operations of Proxy Mobile IPv4. The initial network attachment, registration renewal, and resource cleanup procedures are covered. Note that the protocols that interact with Proxy Mobile IP are identified and explained in more detail. The PPP/IPCP (IP Control Protocol) protocol involves a PPP client in the mobile device and a Network Access Server (NAS) in the AR. DHCP involves a DHCP client in the MN and a DHCP server in either the AR or the HA. PMIPv4 involves a PMA in the AR and an HA in the router on the home network. The Authentication, Authorization, and Accounting (AAA) protocol involves a AAA client in the AR and a AAA server in the network. The collocation of the functional entities in the AR/HA enables parameters to be shared/processed among the protocols.

When the various network entities are not collocated, any sharing of parameters or other state information between them is out of the scope of this document.

4.1.1. Proxy Registration during Initial Network Attachment

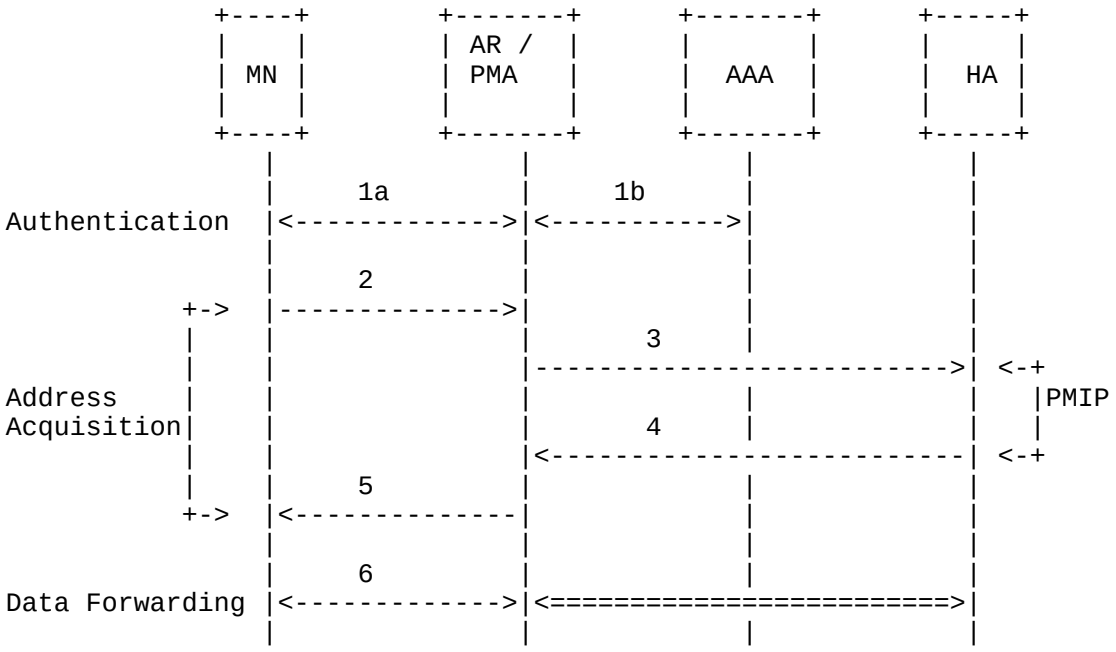


Figure 1: Network Connection Setup

The initial network-attachment procedure is described below. There are three distinct phases. First, authentication and authorization happen when the mobile device accesses the network. Then, the mobile device attempts to obtain an IP address. This triggers Proxy Mobile IP, which assigns/authorizes the IP address and sets up forwarding between the PMA and HA. The host configuration parameters may be passed in the PMIPv4 signaling. Finally, the mobile device configures its IP stack with the IP address and the obtained host configuration. Packets to and from the mobile device transit both the PMA and HA.

1a. The mobile device establishes a L2 (Layer 2) link with the base station (not shown) and performs access authentication/authorization with the AR (Access Router). During this phase, the mobile device may run either the Challenge Handshake Authentication Protocol (CHAP) [RFC1994] if PPP [RFC1661] is used or the Extensible Authentication Protocol (EAP) [RFC3748] over foo (foo being the specific access technology, or PANA [RFC4058]). The AR acts as the NAS (Network Access Server) in this step.

1b. The AAA client exchanges AAA messages with the AAA infrastructure to perform authentication and authorization of the mobile device. As part of this step, the AAA server may download some information about the mobile device (e.g., the user's profile, handset type, assigned Home Agent address, and other capabilities of the mobile device).

2. The mobile device requests an IP address via a PPP/IPCP [RFC1332] or DHCP [RFC2131]. Specifically for PPP, the PPP client sends an IPCP Configure-Request to the NAS. As for DHCP, the DHCP client sends the DHCP Discover message to the DHCP relay agent/ server.

   For the DHCP case, the DHCP server or DHCP relay agent sends the DHCP Ack message to the DHCP client after PMIPv4 signaling has completed.

3. Triggered by step 2, the PMA sends a Proxy Registration Request (PRRQ) to the HA. The HA's IP address is either obtained from the AAA server at step 1b or discovered by some other method. The PRRQ contains the Care-of Address (CoA) of the PMA (the collocated FA in this case). The Home Address field is set to zero or the IP address is specified as a hint in the DHCP or IPCP message. The PRRQ MUST be protected by the methods described in the Security Considerations (Section 13) of this document. The derivation and distribution of the MN-HA or FA-HA key is outside the scope of this document.

4. The Home Agent sets up the mobility binding entry for the mobile device after assigning an IP address or authorizing the requested Home Address. The Home Agent may also assign a Generic Routing Encapsulation (GRE) key in this step (if GRE tunneling is used between the PMA and HA). The HA returns the Home Address and the GRE key (if applicable) in the Proxy Registration Reply (PRRP) to the PMA. If the requested Home Address is not authorized, the Home Agent denies the registration with error code 129 (administratively prohibited). After the PMA processes the PRRP, the forwarding path for the Home Address between the PMA and HA is established. A GRE tunnel may be used between the PMA and the HA [MIP4GREKEY]. This event completes the Proxy Mobile IPv4 signaling for initial network attachment.

5. After the Proxy Mobile IPv4 registration exchange, the AR provides the IP address to the mobile device in response to step 2. For IPCP, the NAS replies to the PPP client with an IPCP Configure-Nak, which includes the PMIPv4-assigned Home Address

in the IP address configuration option and the DNS server address in the IPCP configuration option.

The following procedure happens when the DHCP server is on the AR. The DHCP server sends a DHCP Offer with the PMIPv4-assigned Home Address in the yiaddr field to the DHCP client. The DHCP client sends a DHCP Request to the DHCP server, which replies with a DHCP Ack. The host configuration (such as the DNS server address) is included in the DHCP options in the message. Note that the DHCP messages are exchanged directly between the DHCP client and the DHCP server.

In the case when AR acts as a DHCP relay agent, the DHCP Discover is relayed to the DHCP server on the HA. The DHCP server sends a DHCP Offer with the PMIPv4-assigned Home Address in the yiaddr field to the DHCP relay agent, which forwards it to the DHCP client. The DHCP Request and DHCP Ack messages are exchanged between the DHCP client and DHCP server via the DHCP relay agent. Regardless of the sequence of PMIPv4 signaling and DHCP exchanges, the interaction between PMIPv4 and DHCP involves in the same IP address for Home Address field and yiaddr field, respectively.

6. At this step, the mobile device’s IP stack is configured with an IP address that has a forwarding path between the AR/PMA and HA. Also, the host configuration (such as DNS servers) is configured at this time. Now that the IPCP or DHCP procedure has completed, the mobile device is ready to receive or send IP packets. If DHCP is used, the DHCP client renews the IP address by sending a DHCP Request directly to the DHCP server. The lease for the IP address is extended when a DHCP Ack from the DHCP server is received by the DHCP client.

4.1.2. Proxy Registration Renewal

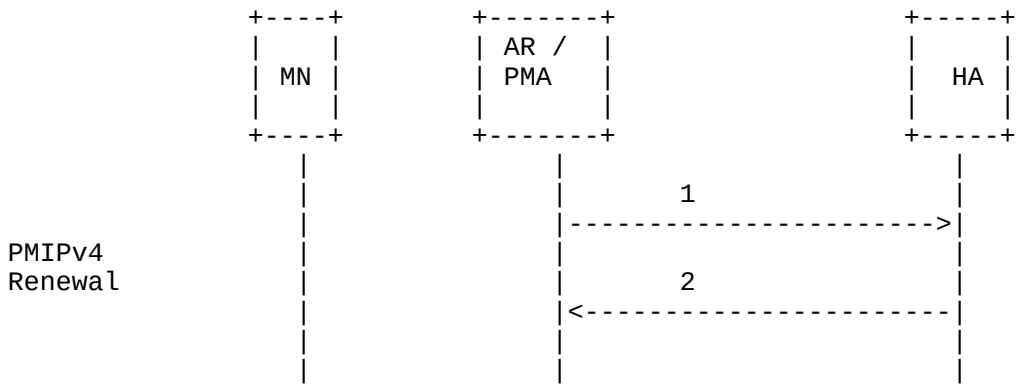


Figure 2: Network Connection Maintenance

The network-connection maintenance procedure is described below. As long as the mobile device remains attached to the AR, the Proxy Mobile IPv4 session is maintained by re-registration exchanges between the AR and HA.

1. Before the PMIPv4 registration lifetime expires, and assuming the AR has not received any indication that the mobile device detached from the network, the PMA sends a PRRQ to the HA to extend the duration of the mobility binding of the mobile device. This PRRQ is similar to the initial PRRQ (i.e., HA field set to the assigned HA, and CoA field set to the PMA), though the Home Address field is always set to the assigned IP address of the mobile device. The mobile device's IP stack can continue to send and receive IP packets using the Home Address anchored at the HA.

2. The HA sends the PRRP in response to the PRRQ received from the PMA. After the PMA processes the PRRP, the forwarding path between AR and HA remains intact.

4.1.3. Proxy Handover Support

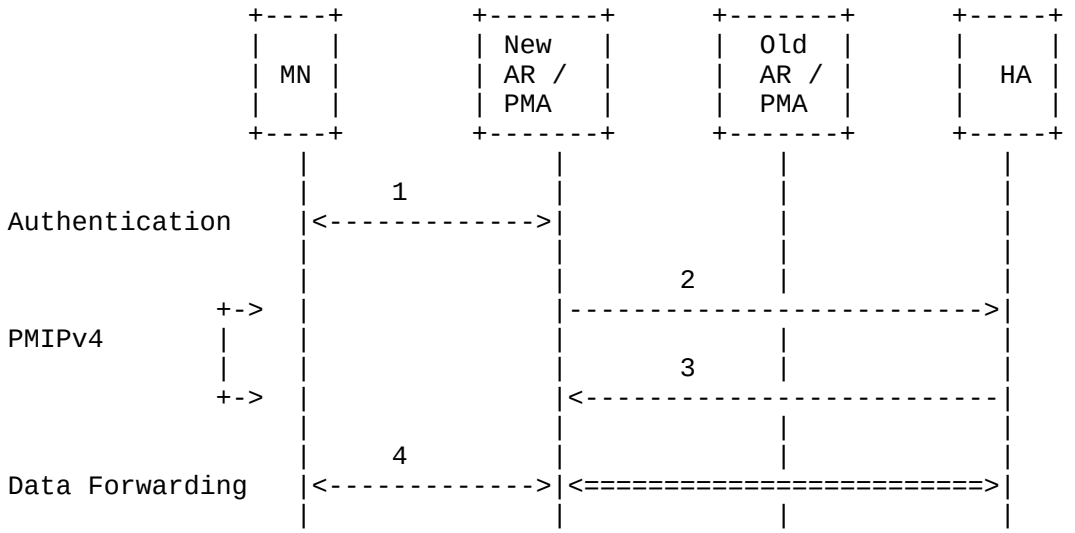


Figure 3: AR Handover

The AR handover procedure is described below. There are three phases. First, authentication and authorization happen when the mobile device attaches to the new AR in the network. The successful authentication triggers the Proxy Mobile IPv4 signaling. In the last phase, the forwarding path between the new AR and HA is set up for the mobile device to send and receive IP packets using the same Home Address anchored at the HA.

1. The mobile device establishes L2 link with the base station (not shown) and performs access authentication/authorization with the new AR, using the security method for network re-attachment.

2. Triggered by successful authentication, the PMA sends a PRRQ to the HA. The HA's IP address is typically obtained or is known by the method used for fast re-authentication during AR handover (e.g., context transfer between the two ARs), though other methods may be used. The PRRQ contains the CoA of the new PMA. The Home Address field is set to zero or the assigned IP address of the mobile device. The IP address is also obtained/known by the same method mentioned before.

3. The Home Agent updates the existing mobility binding entry for the mobile device upon processing the PRRQ. The Home Agent returns the Home Address, fetched from the binding, in the PRRP to the new PMA. After the PMA processes the PRRP, the forwarding

path for the Home Address between the new AR and HA is established. The event completes the Proxy Mobile IPv4 signaling for AR handover.

4. At this step, which happens around the same time as step 2, the mobile device's IP stack may detect L2 link going down and up after access re-authentication. The mobile device's IP stack may attempt to validate its IP address connectivity. See Sections 6.1, 6.2, and 6.3 of this document for considerations on ARP [RFCARP], ICMP [RFCICMP], and DHCP [RFC2131], respectively. Because the forwarding path is established between the new PMA and HA, the mobile device can receive or send IP packets using the Home Address.

4.1.4. Resource Cleanup

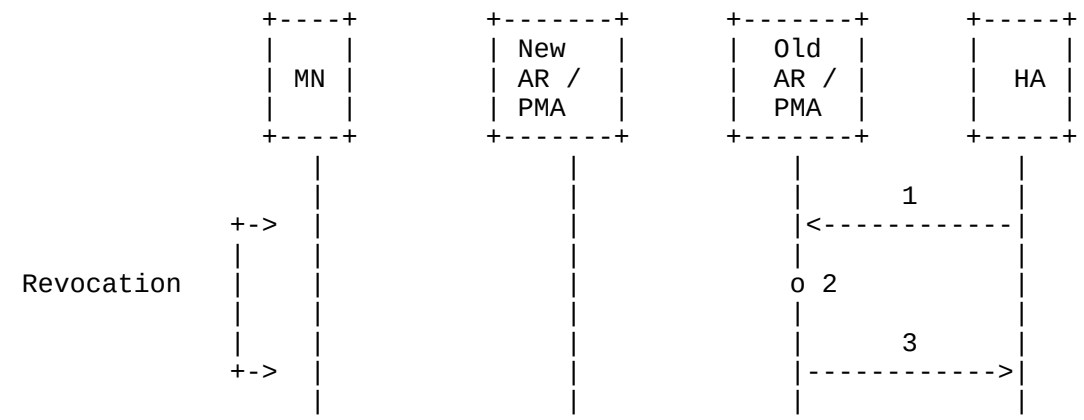


Figure 4: Registration Revocation for Previous PMA

The resource cleanup procedure for the old AR is described below. This cleanup is necessary when the old AR needs to delete its PMIPv4 and other associated states for a mobile device that has moved to another AR. Therefore, this is an optional procedure for Proxy Mobile IP. The alternative method is based on the new PMA notifying the old PMA to clean up resources. The alternative method is out of the scope of this document.

1. Triggered by the update of the mobility binding entry for a mobile device that has moved to a new AR, the HA may send a Registration Revocation (as specified in RFC 3543 [RFC3543]) to the old PMA (i.e., specifically to the Foreign Agent entity) in order to clean up unused resources in an expeditious manner.

2. The old PMA removes the PMIPv4 states for the mobile device.

3. The old PMA sends revocation acknowledgement to the HA.

4.2. Establishment of a Bi-Directional Tunnel

The PMA and HA set up a tunnel between them for the Home Address after the PMIPv4 registration message exchange.

4.2.1. Packet Forwarding

The bi-directional tunnel between the PMA and the HA allows packets to flow in both directions, while the mobile device is connected on the visited network. All traffic to and from the mobile device travels through this tunnel.

While the PMA is serving a mobile device, it MUST be able to intercept all packets sent from the mobile device and forward them out the tunnel created for supporting that mobile device. Typically, forwarding is based on layer 2 information such as the source Media Access Control (MAC) address or ingress interface. This allows overlapping IP addresses to be supported for the packet from the mobile device. For example, the PMA forwards packets from mobile devices with the same IP address to the tunnel associated with each mobile device, based on the source MAC address.

The PMA de-encapsulates any packets received on the tunnel from the HA before forwarding to the mobile device on its link. Typically, the forwarding is based on the destination IP address and ingress HA tunnel (which may have a GRE key). This allows overlapping IP addresses to be supported for the packet destined to the mobile device. For example, the PMA forwards packets to mobile devices with the same IP address to the link associated with each mobile device, based on the GRE key value of the tunnel created for the HA that serves these mobile devices.

The tunnel operation between the PMA and HA is the same as between the FA and HA in RFC 3344. The IP TTL (Time to Live), fragmentation, re-assembly, etc. logic remain the same. The tunnel mode is IPinIP by default or GRE as an option.

4.2.2. Broadcast and Multicast

Broadcast packet processing for DHCP and ARP (Address Resolution Protocol) messages are described in Section 6.3 and Section 6.1, respectively. For other types of broadcast packets, the PMA and HA

process them in accordance to [RFC3344], [RFC3024], and [MIP4MCBC]. Only the Direct Encapsulation Delivery Style is supported, as there is no encapsulation for the packets between the mobile device and PMA.

4.2.3. Forwarding between Devices on the Same PMA

When the communication peers are both attached to the same PMA, the packet is forwarded as specified in Section 4.2.1. The traffic between them should be routed via the HA without taking a local shortcut on the PMA. This ensures that data-traffic enforcement at the HA is not bypassed.

4.3. Security Association between the PMA and the HA

The security relationship for protecting the control message exchanges between the PMA and the HA may be either per node (i.e., same security association for all mobile devices) or per MN (i.e., unique security association per mobile device). The method of obtaining the security association is outside the scope of this document.

For per-node SA support, the FA-HA Authentication extension or IPsec (indicated in the PMIPv4 extension) is used to authenticate the signaling messages (including Registration Revocation [RFC3543]) between PMA and HA. In the case of IPsec, Encapsulating Security Payload (ESP) [RFC4303] in transport mode with mandatory integrity protection should be used. The IPsec endpoints are the IP addresses of the PMA and HA.

For per-MN SA support, the MN-HA Authentication extension and/or MN-AAA Authentication extension are used to authenticate the signaling.

The creation of the security association may be assisted by the AAA server at the time of access authentication.

4.4. Registration Sequencing

The Identification field in the registration message provides replay protection and sequencing when the timestamp method is used. This mechanism allows the HA to know the sequence of messages from the same PMA or different PMAs based on the Identification field. The HA can also synchronize the PMA’s clock by using the Identification mismatch error code in the Proxy Registration Reply. This reply message would not be necessary when the PMA’s clocks are synchronized using the Network Time Protocol [RFC1305] or some other method. Note that the use of nonce for sequencing and replay protection is outside the scope of this document.

The method above is sufficient when there is a single source for signaling as in the split PMA case. However, in the integrated PMA case, the Proxy Registration Request is sent from different sources (i.e., different PMAs). If the previous PMA is unaware that the mobile device has moved away and continues to send re-registration, then the HA would be misinformed on the location of the device. Therefore, an integrated PMA MUST confirm that the mobile device is still attached before sending a Proxy Registration Request.

Note that, for the split PMA model as used in WiMAX Forum (see Section 10), the PMIPv4 client remains anchored during handover (see Section 10.1). In this case, the PMIPv4 client is the only source of the PRRQ. However, there are cases (such as PMIPv4 client relocation and uncontrolled handover events) when more than one PMA performs registration. The same method for the integrated PMA is used to ensure proper sequencing of registration on the HA.

4.5. Mobile Device Interface Configuration

Typically, the mobile device's interface needs to be configured with an IP address, network prefix, default gateway, and DNS server addresses before the network connection can be enabled to be used for communication. For some IP stacks, the default gateway IP address has to be on the same subnet as the mobile device's IP address. When the Home Agent's IP address is not on the same subnet as the Home Address, vendor-specific extensions (e.g., [RFC4332]) or other methods MAY be used by the PMA to obtain the default gateway.

4.6. Dynamic HA Discovery

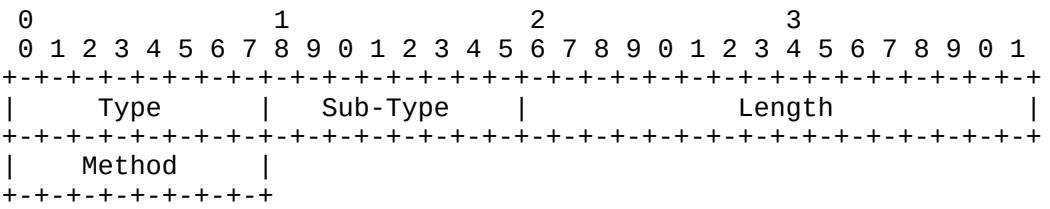
The PMA can perform dynamic HA discovery by sending the registration with Home Agent field set to 0.0.0.0 or 255.255.255.255. The Home Agent responds with its IP address in the Home Agent field as specified in "Mobile IPv4 Dynamic Home Agent (HA) Assignment" [RFC4433].

5. Proxy Mobile IPv4 Extensions

The following PMIPv4 extensions are not required for base functionality but may be used in some cases where such features are applicable. They are included before the authentication extension (e.g., MN-HA or FA-HA Authentication extension) in the registration message.

5.1. PMIPv4 Per-Node Authentication Method Extension

The Proxy Mobile IPv4 Authentication Method extension indicates alternative methods for authenticating the registration besides the default MN-HA Authentication extension as specified in RFC 3344. This extension MUST be included in the Registration Request and Registration Reply when the security association for authenticating the message is between the PMA and HA on a per-node basis. This means that a common key or set of keys (indexed by the SPI) are used for message authentication by the PMA and HA. The key is independent of the mobile device, which is identified in the registration.



PMIPv4 Per-Node Authentication Method Extension

Type

47 (Proxy Mobile IPv4 Non-Skippable Extension)

Sub-Type

1 (PMIPv4 Per-Node Authentication Method)

Length

1

Method

An 8-bit field that specifies the authentication type for protecting the signaling messages.

The values (0 - 255) are allocated and managed by IANA. The following values have been assigned to the specified method types.

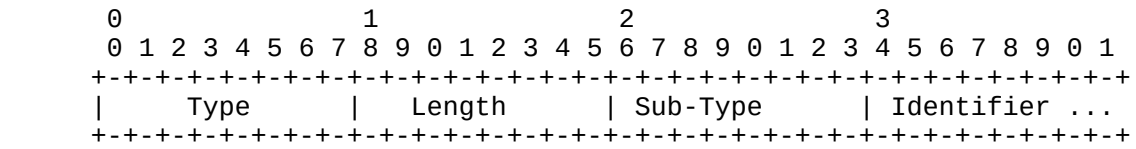
0: Reserved

1: FA-HA Authentication

2: IPsec Authentication

5.2. Proxy Mobile IPv4 Interface ID Extension

The Proxy Mobile IPv4 Interface ID extension identifies the interface address of the device used to attach to the network. The information MAY be included in the Registration Request when the PMA is aware of it.



PMIPv4 Interface ID Extension

Type

147 (Proxy Mobile IPv4 Skippable Extension)

Length

The length of the extension in octets, excluding Type and Length fields.

Sub-Type

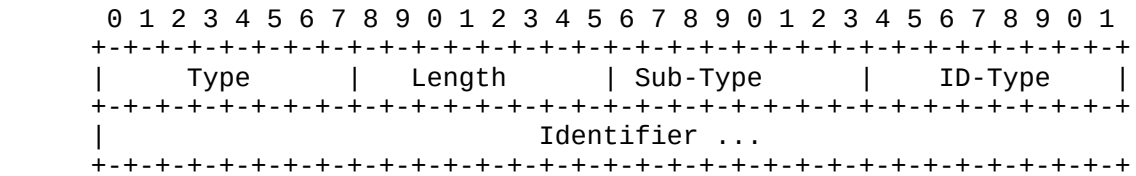
1 (PMIPv4 Interface ID)

Identifier

A variable-length octet sequence that contains an identifier of the interface.

5.3. Proxy Mobile IPv4 Device ID Extension

The Proxy Mobile IPv4 Device ID extension identifies the device used to connect to the network. The information MAY be included in the Registration Request when the PMA is aware of it.



PMIPv4 Device ID Extension

Type

147 (Proxy Mobile IPv4 Skippable Extension)

Length

The length of the extension in octets, excluding Type and Length fields.

Sub-Type

2 (PMIPv4 Device ID)

ID-Type

An 8-bit field that specifies the device ID type.

The values (0 - 255) are allocated and managed by IANA. The following values have been assigned to the specified device ID types.

0: Reserved

1: Ethernet MAC address

2: Mobile Equipment Identifier (MEID)

3: International Mobile Equipment Identity (IMEI)

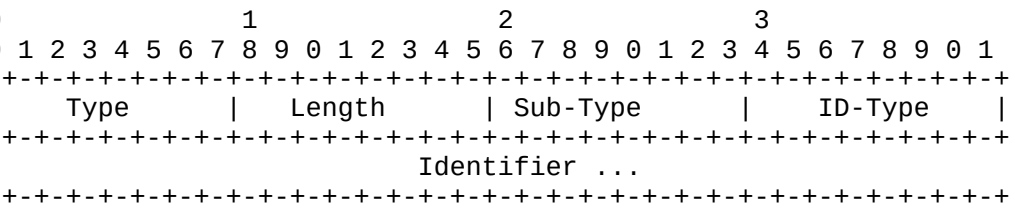
4: Electronic Serial Number (ESN)

Identifier

A variable-length octet sequence that contains an identifier of the type indicated by the ID-Type field.

5.4. Proxy Mobile IPv4 Subscriber ID Extension

The Proxy Mobile IPv4 Subscriber ID extension identifies the mobile subscription. The information MAY be included in the Registration Request when the PMA is aware of it.



PMIPv4 Subscriber ID Extension

Type

147 (Proxy Mobile IPv4 Skippable Extension)

Length

The length of the extension in octets, excluding Type and Length fields.

Sub-Type

3 (PMIPv4 Subscriber ID)

ID-Type

An 8-bit field that specifies the subscriber ID type.

The values (0 - 255) are allocated and managed by IANA. The following values have been assigned to the specified subscriber ID types.

0: Reserved

1: International Mobile Subscriber Identity (IMSI)

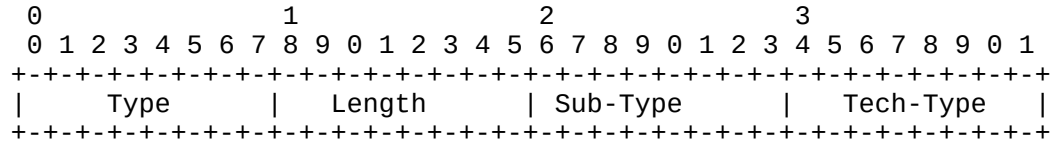
Identifier

A variable-length octet sequence that contains an identifier of the type indicated by the ID-Type field.

5.5. PMIPv4 Access Technology Type Extension

The Proxy Mobile IPv4 Access Technology Type extension indicates the type of radio-access technology on which the mobile device is attached. This extension MAY be included in the Registration Request when the PMA is aware of the information. The HA can provide mobility on the same access technology type for a mobile device with

multiple interfaces, assuming each interface is connected on a different access technology type. The HA does not include the extension in the associated Registration Reply.



PMIPv4 Access Technology Type Extension

Type

147 (Proxy Mobile IPv4 Skippable Extension)

Length

2

Sub-Type

4 (Access Technology Type)

Tech-Type

An 8-bit field that specifies the access technology through which the mobile device is connected to the access network.

The values (0 - 255) are allocated and managed by IANA. The following values have been assigned to the specified access technology types.

0: Reserved

1: 802.3

2: 802.11a/b/g

3: 802.16e

4: 802.16m

5: 3GPP EUTRAN/LTE

6: 3GPP UTRAN/GERAN

7: 3GPP2 1xRTT/HRPD

8: 3GPP2 UMB

6. Appearance of Being at Home Network

Since the Mobile Node is not aware of its mobility and does not participate in handover signaling, the network entities emulate the home network to the mobile device attached on the network. From the mobile device's perspective, it operates as if it were at the home network. However, the network is directing the mobile device's traffic to and from its current location and will continue to do so when it moves to a new location.

An unmodified mobile device on a shared link learns the MAC address of another host on the home network via ARP ([RFCARP]), obtains an IP address and other host configuration via DHCP ([RFC2131]), and sends link-local multicast and broadcast packets. The network's response to the host is equivalent to the situation when a host is on the home network. When the link state changes, some hosts use ARP, ICMP, and/or DHCP to detect if it has changed the point of attachment on the network.

6.1. ARP Considerations

For IEEE 802 type of access networks (e.g., WLAN, WiMAX Ethernet Convergence Sublayer), the mobile device sends ARP requests for the Corresponding Node (CN) and default gateway on the same network. The purpose of maintaining an ARP entry is to allow the delivery of the packet from the mobile device to the CN using the destination MAC address. The ARP procedure for resolving IP and MAC address mapping is not needed for 3GPP2's cdma2000 and WiMAX IP Convergence Sublayer networks.

The access router is always the L2 endpoint for the mobile device. The destination MAC address in the packet does not need to be set to the CN's MAC address. As long as the packet can be received by the access router, it will be forwarded toward the CN via the home network node (further details in Section 4.2.1). The ARP table in the mobile device does not need to be populated with CNs' MAC addresses in order for the packet to reach the CNs.

A mobile device has ARP entries for the default gateway and hosts on the same subnet. Regardless of what the MAC addresses are, the AR receives the packets sent from the mobile device.

6.2. ICMP Considerations

For movement detection, certain types of network stack on the mobile device will send an ICMP request [RFCICMP] to the default gateway after detecting the link went down and up. The IP TTL in the message is set to 1 to check if the default gateway is still directly reachable on the access network. The PMA MAY send an ICMP reply when it is providing Proxy Mobile IPv4 service for the mobile device. This response confirms to the mobile device that it has remained on the home network after link state change. This behavior is observed on existing client implementation. "Detecting Network Attachment in IPv4 (DNAv4)" [RFC4436] can be employed.

General ICMP traffic is handled as normal IP packets and tunneled between the PMA and HA.

6.3. DHCP Considerations

DHCP [RFC2131] is used to obtain an IP address and other host configuration parameters for a mobile device. The mobile device is expected to behave as a normal DHCP client when connected to the network with Proxy Mobile IPv4 service. There are two DHCP phases: bootup and renewal/release. The bootup procedure relies on the DHCP relay agent to obtain a lease on the IP address for the DHCP client from the DHCP server. The DHCP client directly renews and releases the lease with the DHCP server.

In Proxy Mobile IPv4, the mobile device boots up on a network that is not the home network associated with the leased IP address. Also, the mobile device can move to other networks that are not related to that IP address. Yet, the DHCP client on the mobile device continues to operate as a stationary device that is directly on the network associated with its IP address. The PMA and HA create the transparency of the remote home network and mobility events by providing the expected network response to the DHCP client.

There are several methods for the network infrastructure to interface with the mobile device such that the mobile device believes it is always fixed on the same network. The following methods are identified here, though others may be used as well.

DHCP Server in the AR:

The mobile device boots up and initiates DHCP. The procedure is described in Figure 1. The DHCP client renews or releases the IP address directly with the DHCP server in the AR. When the mobile device is on a different AR than the AR/DHCP server, the DHCP message from the client needs to be able to either be forwarded to

the DHCP server in the previous AR or handled by the DHCP server in the new AR. When the DHCP lease time expires for the mobile device's IP address or the DHCP release message is received on the current AR, the AR sends PMIPv4 de-registration to the HA.

DHCP Relay Agent in the AR:

The mobile device boots up and initiates DHCP. The procedure is described in Figure 1. The DHCP client renews or releases the IP address directly with the DHCP server in the HA. When the mobile device is on a different AR, DHCP messages from the client are relayed to the DHCP server in the HA. When the DHCP lease time expires for the mobile device's IP address or the DHCP release message is received on the HA, the HA deletes the mobility binding entry for the mobile device and sends registration revocation [RFC3543] to the AR.

6.4. PPP IPCP Considerations

When the mobile device accesses the network via PPP [RFC1661], LCP (Link Control Protocol) CHAP is used to authenticate the user. After authentication, the NAS (which is the AR/PMA) sends the Proxy Mobile IPv4 Registration Request to the HA. The HA responds with the Home Address in the Proxy Registration Reply. The NAS informs the mobile device to use the Home Address during IPCP [RFC1332]. When the mobile device moves to a new NAS, the same procedure happens and that mobile device has the same IP address for communication.

The message exchange is illustrated in Figure 1.

6.5. Link-Local Multicast and Broadcast Considerations

Depending on configuration policies, the PMA may tunnel all packets destined to Link-Local Multicast or Broadcast to the HA. The HA looks up the hosts that are in the same subnet and sends a duplicated packet to each of them.

7. Proxy Mobility Agent Operation

The PMA performs the functions of a Mobile Node entity as described in RFC 3344, with the exceptions identified below.

- No agent discovery (i.e., agent solicitation and advertisement) is supported.

- The D-bit (De-encapsulation by MN) in the Registration Request is always set to zero.

The main responsibility of the PMA is to set up and maintain the routing path between itself and the HA for a mobile device that is attached on the network. When it detects a mobile device is no longer attached, the routing path is torn down. It is possible that the PMA functions may be split up in implementations such as WiMAX (Section 10).

The PMA needs to know the following information, at a minimum, for sending a proxy registration:

1. NAI of the mobile device.

2. MN-HA security association, when per-mobile device security association is used.

3. FA-HA Mobility security association or IPsec security association when per-node security association is used. Note that these associations are specific only between PMA and HA, and are cryptographically unrelated to the associations between the MN and other network nodes.

4. HA Address.

This information is typically downloaded from the AAA server during access authentication.

8. Home Agent Operation

The Home Agent has the functionality described in RFC 3344 [RFC3344]. In addition, the following features are introduced by Proxy Mobile IPv4:

1. Sequencing between PRRQs from multiple PMAs. For the integrated PMA case, there is a period after handover that may result in both the new PMA and old PMA sending PRRQs. It is imperative that the old PMA confirm that the mobile device is attached before sending a PRRQ when the re-registration timer expires. This would ensure that the HA only receives registration from the PMA that is serving the mobile device.

2. Authentication of PRRQs based on per-node security associations (FA-HA AE or IPsec AH/ESP) is applicable in the integrated PMA case. The presence of MN-HA AE or MN-AAA AE in the PRRQ is not necessary in this case. Since PMIPv4 is based on signaling between the PMA and the HA, the security for the message can be authenticated based on the peers' relationship. The HA can authorize PMIPv4 service for the mobile device at the PMA by contacting the AAA server.

3. The ability to process the Proxy Mobile IPv4 extensions defined in this document for enhanced capabilities of PMIPv4.

8.1. Processing Proxy Registration Requests

When a Proxy Registration Request is received, the HA looks up the mobility binding entry indexed by the NAI. If the entry exists, HA compares the sequence numbers between the message and mobility binding entry (MBE), if present. If the value in the message is zero or greater than or equal to the one in the MBE, HA accepts the registration. The HA replies with a sequence number that is one greater than the larger value of either the MBE or Proxy Registration Request. If the registration is denied, then HA sends error code "Administratively prohibited (65)". If the HA is not enabled with Proxy Mobile IPv4 or cannot process the Proxy Mobile IPv4 Extensions defined in this document, it sends a Registration Reply with error code PMIP_UNSUPPORTED ("Proxy Registration not supported by the HA"). In the case when the PMA is not allowed to send a Proxy Registration Request to the HA, the HA sends a Proxy Registration Reply with error code PMIP_DISALLOWED ("Proxy Registrations from this PMA are not allowed").

A PMA receiving these error codes SHOULD NOT retry sending Proxy Mobile IPv4 messages to the HA that sent replies with these error codes.

9. Mobile Device Operation

As per this specification, a mobile device would function as a normal IPv4 host. The required behavior of the node will be consistent with the base IPv4 specification [RFC0791]. The mobile station will have the ability to retain its IPv4 address as it moves from one point of network attachment to the other without ever requiring it to participate in any mobility-related signaling.

When booting up for the first time, a mobile device obtains an IPv4 address using DHCP or IPCP.

As the mobile device roams, it is always able to communicate using the obtained IP address on the home network. The PMA on the currently attached network signals to the HA to ensure a proper forwarding path for the mobile device’s traffic.

9.1. Initial Network Access

When the mobile device accesses the network for the first time and attaches to a network on the PMA, it will present its identity in the form of an NAI to the network as part of the network-access authentication process.

Once the address configuration is complete, the mobile device will always be able to use that IP address anywhere in the network.

9.2. Mobile Device Mobility

When a mobile device moves to a new PMA from another PMA, the following occurs:

The mobile device may perform a network-access authentication with the new AR/PMA. If the authentication fails, the mobile device will not be able to use the link. After a successful authentication, the new PMA will have the identifier and the other profile data of the mobile device. The new PMA can also obtain the mobile device's information using a context-transfer mechanism, which is out of the scope of this document.

Once the network-access authentication process is complete, the mobile device may sense a change in the Link Layer and use ARP, DHCP, and/or ICMP to detect if it is still on the same subnet. These mechanisms are handled by the network as described in "Appearance of Being At Home Network" (Section 6).

9.3. Sending and Receiving Packets

All packets that are to be sent from the mobile device to the Corresponding Node (CN) will be sent as normal IPv4 packets, setting the Source Address of the IPv4 header to the Home Address and the Destination Address to the Corresponding Node's IP address. In Proxy Mobile IPv4 operation, the default gateway for the mobile device is set up to reach the PMA.

Similarly, all packets sent to the mobile device's IP address by the Corresponding Node will be received by the mobile device in the original form (without any tunneling overhead).

For Proxy Mobile IP, the packet from the mobile device is transported to the HA to reach the destination, regardless of the destination IP address. For a CN with an IP address on the same network as the mobile device but that is physically located elsewhere, the HA will tunnel the packet to the CN. Otherwise, the HA forwards the traffic via normal routing.

No special operation is required by the mobile device to either send or receive packets.

Mobile devices attached to the same PMA may be using different HAs for transporting their traffic.

10. Proxy Mobile IPv4 Use Case in WiMAX

WiMAX Forum Network Working Group (NWG) uses the Proxy Mobile IPv4 scheme to provide IPv4 connectivity and IP mobility. The relevant specification from WiMAX Forum is [NWG].

The Proxy Mobile IPv4 protocol is used over NWG reference point 3 (R3). Most of the Proxy Mobile IPv4 related procedures and requirements are described in reference to mobility management over R3.

The Proxy Mobile IPv4 use case in the WiMAX Forum specification is illustrated in the following diagram:

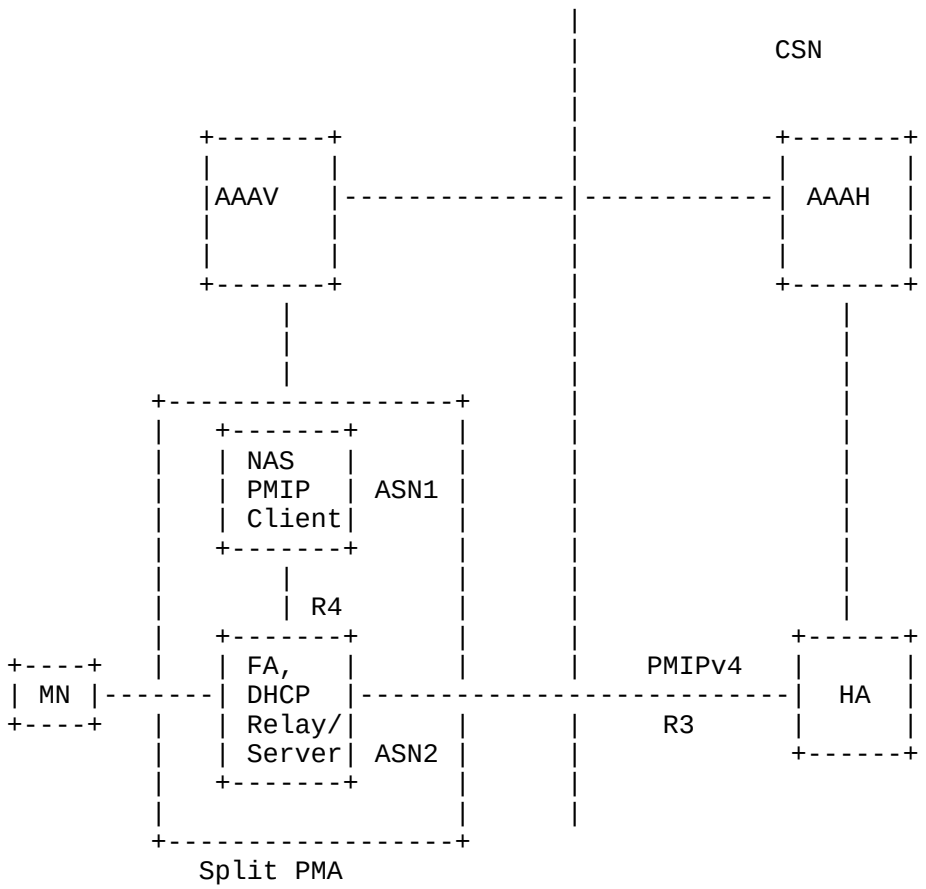


Figure 5: WiMAX NWG Network Configuration for PMIPv4 Use

As shown in the figure above, WiMAX NWG uses the split PMA model. The PMIPv4 client is collocated with the NAS in ASN1 (aka, Authenticator ASN). The NWG architecture divides the network into two parts. The Access part is termed the "Access Service Network" (ASN). The Core part is termed the "Connectivity Service Network" (CSN). The MN attaches to an 802.16 radio in the ASN2 (aka, Anchor Data Path Function). The radio (base station) connects to the Anchor Data Path Function (A_DPF) in ASN2, which in turn connects to the Authenticator ASN (NAS) in ASN1. ASN1 authenticates and authorizes the MN. The AAA infrastructure is used to authenticate and authorize the MN.

Note that, during initial network entry by the MN, the PMA can be an integrated PMA with all the functions collocated in ASN1. Due to mobility, the FA part of the PMA may have to be relocated to a more

optimized location for better bearer management. However, to describe the WiMAX specific use case for Proxy Mobile IPv4, we will use the split PMA model since it is a more generic representation of the WiMAX NWG mobility framework.

The WiMAX NWG specification [NWG] defines a key bootstrapping scheme for use with Proxy Mobile IPv4. The specification uses per-MN security association for Proxy Mobile IPv4 operation. The relevant keys (e.g., MN-HA key) are derived using EAP authentication as specified in this document. For more information, please refer to Section 4.3 of [NWG], stage-3 specification.

Mobile IPv4 Registration Revocation is optionally supported in WiMAX. The security association for this is per node. It is provided with FA-HA AE. The FA-HA key is also bootstrapped via the same key hierarchy that is described in Section 4.3 of [NWG].

The Proxy Mobile IPv4 operation in WiMAX NWG is aligned with the basic Proxy Mobile IPv4 operation as described in Section 4 of this document. There are specific considerations for WiMAX NWG 1.0.0 use of Proxy Mobile IPv4. These are listed below:

1. Use of per-MS SA for Proxy Mobile IPv4 registration. In this case, MN-HA AE is used.

2. Use of split PMA to handle FA relocation while the PMIPv4 client remains anchored with the NAS (Authenticator ASN).

3. Only the Proxy Mobile IPv4 Access Technology Type extension defined in this document is used in the NWG specification [NWG].

4. GRE key identifier is optionally used between the HA and the PMA.

5. The PMIPv4 client and the FA interact via the WiMAX specific reference point and protocol (aka, R4). For more information, please refer to the NWG specification [NWG].

6. In order to handle inter-ASN (inter Access Router) handover and still allow the MN to use the same DHCP server’s IP address that was sent in DHCPOFFER/ACK, the DHCP server (aka, proxy) functions in the ASN are required to be configured with the same IP address.

7. The MN - AR (trigger for Proxy Mobile IPv4) interaction is based on DHCP. DHCPDISCOVER from the MN triggers the Proxy Mobile IPv4 process in the ASN.

10.1. Proxy Mobile IPv4 Call Flow Examples with Split PMA in WiMAX

Since WiMAX uses the split PMA model, the call flows involve WiMAX proprietary signaling between the PMIPv4 client and FA within the PMA. The following call flows illustrate this.

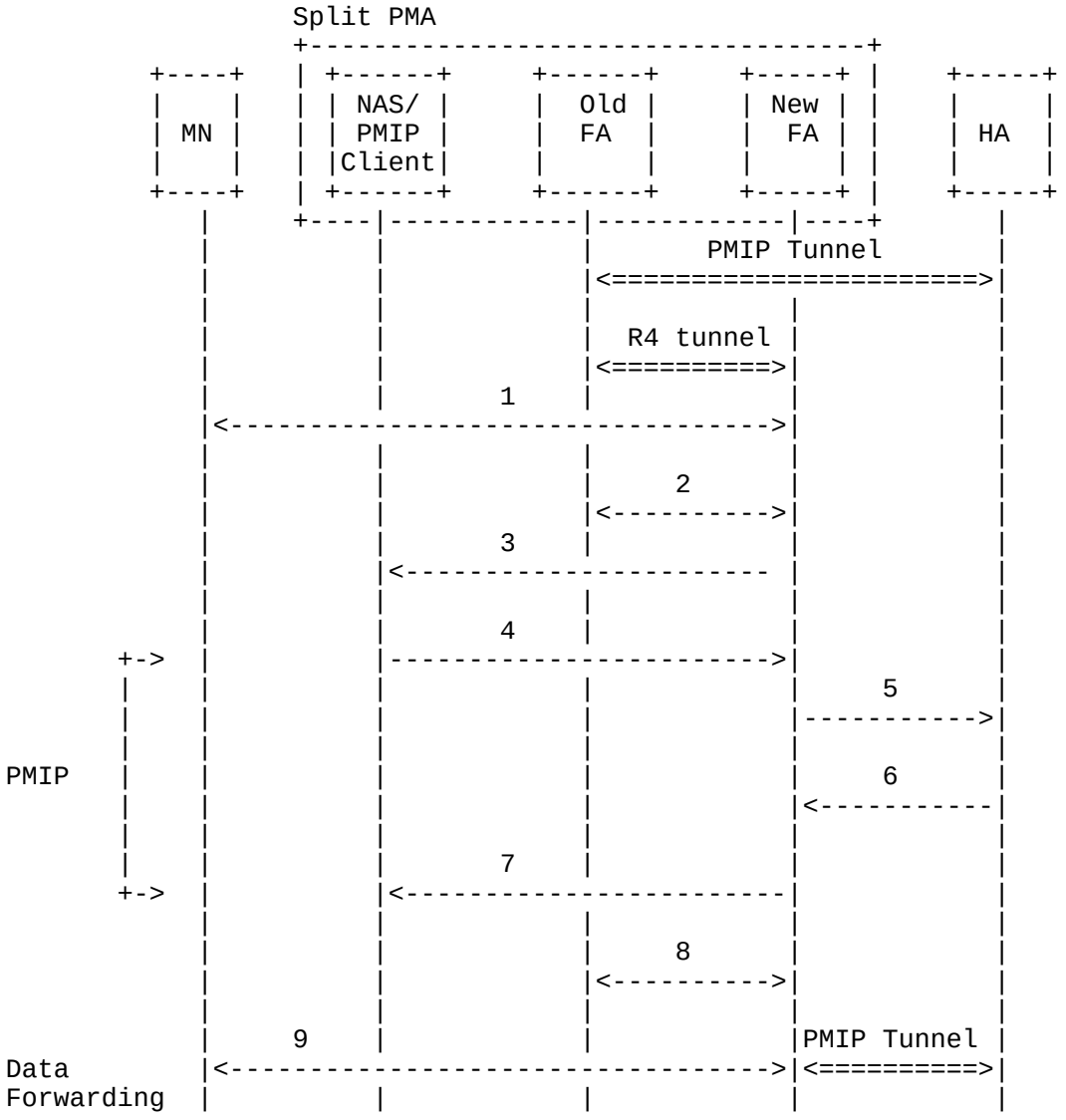


Figure 6: Proxy Handover Operation in WiMAX with Split PMA

In this scenario, the MN has moved to a new FA's area (known as the Data Path Function in WiMAX). The old FA and the new FA interact with each other and also with the PMIPv4 client over a WiMAX-specified R4 reference point to perform the handover. The steps are described below:

1. The mobile device establishes a L2 link with a base station (not shown), which connects to a new FA (aka, new Data Path Function in WiMAX). Note that, in this case, the MN does not perform authentication and authorization. The PMIPv4 tunnel remains between the old FA (aka, old Data Path Function in WiMAX). The data flows through the PMIPv4 tunnel between the HA and the old FA, and through the WiMAX-specific R4 tunnel between the old FA and the new FA and from the new FA to the MN.

2. The new FA interacts with the old FA using a WiMAX-specific R4 reference point to initiate the handover process.

3. The new FA uses the WiMAX-specific R4 reference point to request the PMIPv4 client to begin the PMIPv4 handover.

4. Triggered by step 3, the PMIPv4 client sends a PRRQ to the new FA. The PRRQ contains the FA-CoA of the new FA. The Home Address field is set to the address of the assigned IP address of the Mobile Node. The PRRQ is embedded in the WiMAX-specific R4 packet.

5. The new FA forwards the PRRQ to the HA.

6. The Home Agent updates the existing mobility binding entry for the mobile device upon processing the PRRQ. The Home Agent responds back to the new FA with PRRP.

7. The new FA forwards the PRRP after encapsulating it in a WiMAX-specific R4 packet to the PMIPv4 client.

8. The new FA and the old FA exchange WiMAX-specific R4 messages between them to confirm the handover. The old FA cleans up its resources for the MN. The R4 bearer forwarding also stops at this point.

9. The forward and reverse direction traffic flows via the new FA. The handover is complete at this point.

11. Proxy Mobile IPv4 Use Case in 3GPP2

3GPP2 uses the Proxy Mobile IPv4 scheme to provide mobility service for the following scenarios (as shown in the figures below):

1. Mobility between the base station (BS) and access gateway (AGW)

2. Mobility between the AGW and the Home Agent (HA).

As shown in the diagrams below, in use case 1, the BS acts as the PMA and the AGW acts as the HA for Proxy Mobile IPv4 operation. In use case 2, the AGW acts as the PMA while the HA assumes the role of the Home Agent.

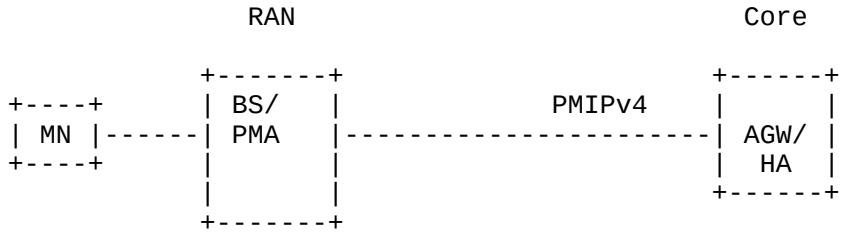


Figure 7: 3GPP2's PMIPv4 Use Case 1 - BS-AGW Interface Mobility

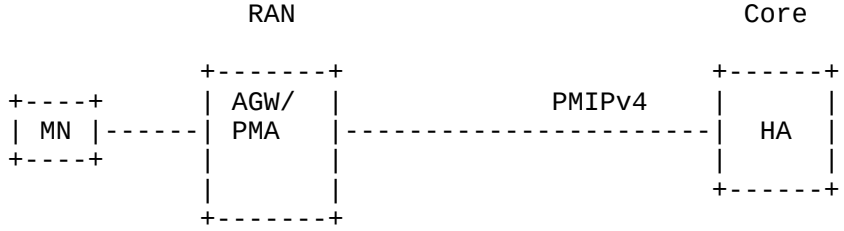


Figure 8: 3GPP2's PMIPv4 Use Case 2 - AGW-HA Interface Mobility

The figure below shows a simplified 3GPP2 architecture. For details, please refer to the 3GPP2 Converged Access Network (CAN) architecture ([3GPP2]).

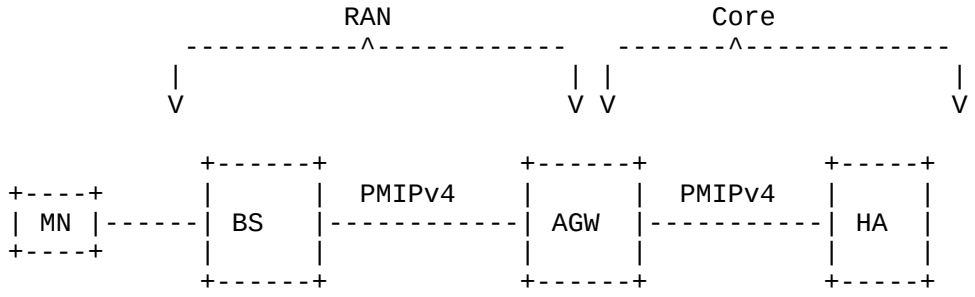


Figure 9: Simplified 3GPP2 Architecture

The Proxy Mobile IPv4 usage scenario in 3GPP2 (case 1) is illustrated in the following diagram:

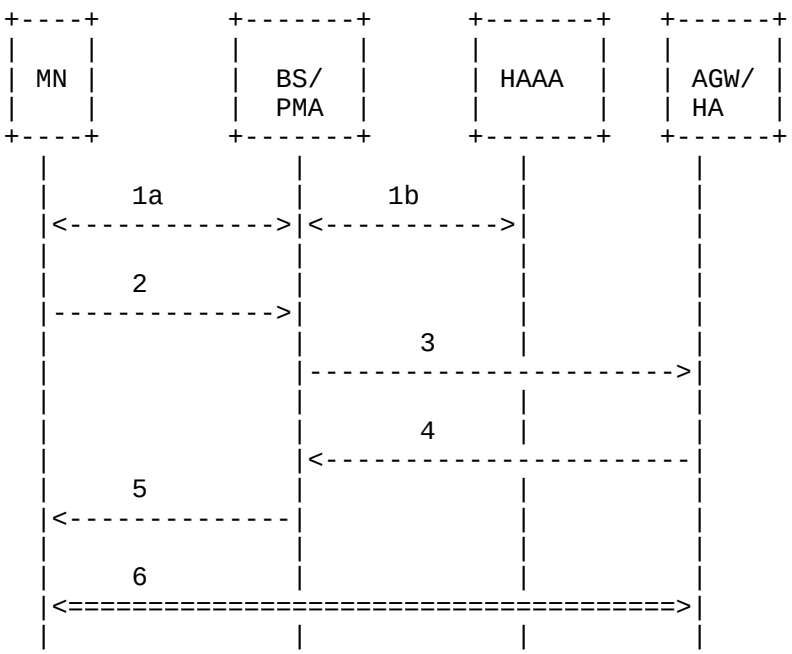


Figure 10: Network Connection Setup (use case 1)

Description of the steps:

1a. MN performs layer 2 establishment with the BS/PMA and performs access authentication/authorization. During this phase, the MN runs EAP over Ultra Mobile Broadband (UMB). The BS acts as the NAS in this phase.

1b. The BS exchanges AAA messages with the Home AAA server via the AR (not shown in the figure) to authenticate the MN. As part of this step, the AR may download some information about the MN (e.g., user's profile, handset type, assigned Home Agent address, and other capabilities of the MN). This information is passed to the PMA/BS (as necessary) to set up the PMIPv4 tunnel in the next step(s).

2. The MN sends layer 2 signaling messages to the BS/PMA to trigger the PMIPv4 tunnel setup process.

3. Triggered by step 2, the PMA/BS sends a PRRQ to the AGW/HA. The HA's address is either received at step 1b from the Home AAA server (HAAA) or is discovered by other means. The PRRQ contains the Care-of Address (CoA) of the PMA (collocated FA in this case). The HoA field is set to all zeros (or all ones). The PRRQ is protected by the method described in this document. The derivation and distribution of the MN-HA or FA-HA key is outside the scope of this document.

4. The AGW/HA registers the MN's session, assigns a symmetric GRE key, and returns this key in the PRRP to the BS/PMA.

5. The BS/PMA responds back to the MN with a layer 2 signaling message.

6. At this step, the MN is assigned an IP address and is connected to the network (via the AGW).

In use case 2, the same procedures are followed except the PMIPv4 tunnel is established between the AGW and the HA. In this case, GRE tunneling may not be used.

11.1. Handover Considerations in 3GPP2

There are some special handover considerations in 3GPP2's Proxy Mobile IPv4 use case. Below is an illustration of the specific use case:

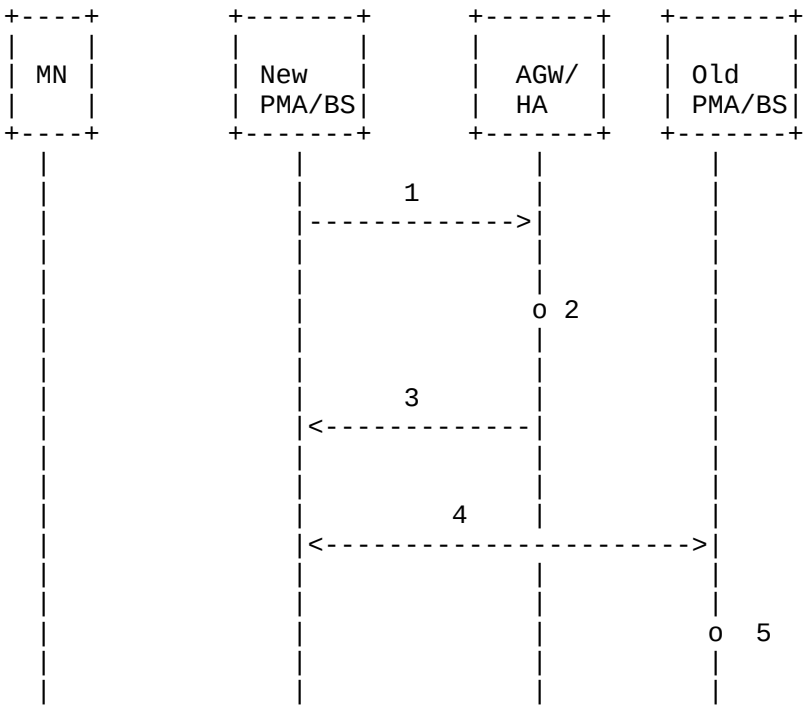


Figure 11: 3GPP2 Registration Revocation for Previous PMA

Description of the steps:

1. MN attaches to the new BS (L2 gets established). There is an ongoing mobility binding entry (MBE) in the AGW for the MN. The PMA in the new BS sends a PRRQ to the AGW.

2. The AGW receives a Proxy Registration Request for a Mobile Node and detects that it has an existing Mobility Binding Entry (MBE). The AGW validates the PRRQ from the new BS and updates the MBE for the MN. The MBE is kept tentative at this point.

3. The AGW sends a Proxy Registration Reply to the new BS. No Registration Revocation is used in the 3GPP2's use case.

4. A 3GPP2's proprietary PMA movement notification message may be exchanged between the AGW and the old BS.

5. The MBE update with the new BS is committed at this step.

12. IANA Considerations

This specification registers 47 for the Proxy Mobile IPv4 Non-Skippable Extension and 147 for Proxy Mobile IPv4 Skippable Extension, both of which are described in Section 5. The ranges for Mobile IPv4 [RFC3344] extension types are defined at http://www.iana.org. This specification also creates a new subtype space for the type number of the extensions. The subtype value 1 is defined for the PMIPv4 Non-Skippable Extension. The subtype values 1 to 4 are defined for the PMIPv4 Skippable Extension. Similar to the procedures specified for Mobile IPv4 number spaces, future allocations from the number space require expert review [RFC5226].

The PMIPv4 Per-Node Authentication Method extension defined in Section 5.1 of this document, introduces a new authentication method numbering space, where the values from 0 to 2 have been assigned per this document. Approval of new Access Technology type values are to be made through IANA Expert Review.

The PMIPv4 Device ID extension defined in Section 5.3 of this document, introduces a new ID type numbering space, where the values from 0 to 4 have been assigned per this document. Approval of new Access Technology type values are to be made through IANA Expert Review.

The PMIPv4 Subscriber ID extension defined in Section 5.4 of this document, introduces a new ID type numbering space, where the values from 0 to 1 have been reserved by this document. Approval of new Access Technology type values are to be made through IANA Expert Review.

The PMIPv4 Access Technology Type extension defined in Section 5.5 of this document, introduces a new technology type numbering space, where the values from 0 to 8 have been reserved by this document. Approval of new Access Technology type values are to be made through IANA Expert Review.

12.1. Mobile IPv4 Extension Types

This document introduces the following Mobile IP extension types.

Name : Proxy Mobile IPv4 Non-Skippable Extension
Type Value : 47
Section : 5

Name : Proxy Mobile IPv4 Skippable Extension
Type Value : 147
Section : 5

12.2. Mobile IPv4 Error Codes

This document introduces the following error code that can be returned by the HA in a Proxy Registration Reply.

Name	Value	First referenced
PMIP_UNSUPPORTED	149	Section 8.1 of RFC 5563
PMIP_DISALLOWED	150	Section 8.1 of RFC 5563

13. Security Considerations

The functionality in this document is protected by the authentication extensions described in RFC 3344 [RFC3344] or IPsec [RFC4301]. Each PMA needs to have an security association (e.g., MN-HA, FA-HA, IPsec AH/ESP) with the HA to register the MN's IP address. The security association can be provisioned by the administrator or dynamically derived. The dynamic key derivation and distribution for this scheme is outside the scope of this document.

14. Acknowledgements

The authors would like to thank the following individuals for their review, comments, and suggestions to improve the content of this document.

Shahab Sayeedi (Motorola), Alper Yegin (Samsung), Premec Domagoj (Siemens), Michael Hammer (Cisco), Jun Wang (Qualcomm), Jayshree Bharatia (Nortel), Semyon Mizikovsky (Alcatel-Lucent), Federico De Juan Huarte (Alcatel-Lucent), Paula Tjandra (Motorola), Alice Qinxia (Huawei), Howie Koh (Greenpacket), John Zhao (Huawei), Pete McCann (Motorola), and Sri Gundavelli (Cisco).

15. References

15.1. Normative References

[3GPP2] "3GPP2 Basic IP Service for Converged Access Network", X.S0054-100-0 Version 2.0, August 2008.

[NWG] "WiMAX Forum Network Architecture (Stage 3: Detailed Protocols and Procedures)" Release 1, Version 1.2.3, July 2008.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC3024] Montenegro, G., Ed., "Reverse Tunneling for Mobile IP, revised", RFC 3024, January 2001.

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

[RFC3543] Glass, S. and M. Chandra, "Registration Revocation in Mobile IPv4", RFC 3543, August 2003.

15.2. Informative References

[MIP4GREKEY] Yegani, P., "GRE Key Extension for Mobile IPv4", Work in Progress, June 2007.

[MIP4MCBC] Chakrabarti, S., "IPv4 Mobility extension for Multicast and Broadcast Packets", Work in Progress, November 2007.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

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

[RFC1332] McGregor, G., "The PPP Internet Protocol Control Protocol (IPCP)", RFC 1332, May 1992.

[RFC1661] Simpson, W., Ed., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[RFC1994] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC4058] Yegin, A., Ed., Ohba, Y., Penno, R., Tsirtsis, G., and C. Wang, "Protocol for Carrying Authentication for Network Access (PANA) Requirements", RFC 4058, May 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4332] Leung, K., Patel, A., Tsirtsis, G., and E. Klovning, "Cisco's Mobile IPv4 Host Configuration Extensions", RFC 4332, December 2005.

[RFC4433] Kulkarni, M., Patel, A., and K. Leung, "Mobile IPv4 Dynamic Home Agent (HA) Assignment", RFC 4433, March 2006.

[RFC4436] Aboba, B., Carlson, J., and S. Cheshire, "Detecting Network Attachment in IPv4 (DNAv4)", RFC 4436, March 2006.

[RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5454] Tsirtsis, G., Park, V., and H. Soliman, "Dual-Stack Mobile IPv4", RFC 5454, March 2009.

[RFCARP] Plummer, D., "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware", STD 37, RFC 826, November 1982.

[RFCICMP] Postel, J., "Internet Control Message Protocol", STD 5, RFC 792, September 1981.

Authors' Addresses

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

EMail: kleung@cisco.com

Gopal Dommety
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134
US

EMail: gdommety@cisco.com

Parviz Yegani
Juniper Networks
1194 North Mathilda Ave.
Sunnyvale, CA 94089-1206

EMail: pyegani@juniper.net

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury, MA 01876
USA

EMail: kchowdhury@starentnetworks.com