3GPP2 X.S0061-0
Version 1.0
Date: December 5, 2008

Network PMIP Support

This page is left blank intentionally.

Network PMIP Support

CONTENTS

LIST OF FIGURES

LIST OF TABLES

REVISION HISTORY

Revision	Date	Remarks
0v1.0	December 2008	Initial Release

FOREWORD

(This foreword is not part of this Standard.)

This document was prepared by 3GPP2 TSG-X.

This document is a new specification.

This document is subject to change following formal approval. Should this document be modified, it will be re-released with a change of release date and an identifying change in version number as follows:

X.S0061 -X version n.0

where:

- X an uppercase numerical or alphabetic character [0, A, B, C, …] that represents the revision level.
- n a numeric string [1, 2, 3, …] that indicates an point release level.

This document uses the following conventions:

- "Shall" and "shall not" identify requirements to be followed strictly to conform to this document and from which no deviation is permitted.
- "Should" and "should not" indicate that one of several possibilities is recommended as particularly suitable, without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.
- "May" and "need not" indicate a course of action permissible within the limits of the document.
- "Can" and "cannot" are used for statements of possibility and capability, whether material, physical or causal.

1 Introduction

This document defines the stage-2 and stage-3 requirements for supporting PMIP between PDSN and LMA/HA. This document describes PMIP based Simple IP address assignment, and PMIP tunnel management.

This document applies to both 1x packet data system and HRPD system.

1.1 Scope

The scope of this document covers support for PMIPv4 and PMIPv6 between PDSN and LMA/HA, called network PMIP. It includes network PMIP based Simple IP address assignment and network PMIP tunnel management. The transport between PDSN and HA/LMA may use IPv4 or IPv6.

2 References

2.1 Normative References

This section provides references to other specifications and standards that are necessary to implement this document.

[1] 3GPP2 C.S0024-A Version 3.0, “cdma2000 High Rate Packet Data Air Interface Specification”, September 2006

[2] 3GPP2 A.S0008-0 v4.0, “Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network”, May 2007.

[3] IETF: draft-leung-mip4-proxy-mode

Editor Note: The above document is a work in progress and should not be referenced unless and until it is approved and published. Until such time as this Editor’s Note is removed, the inclusion of the above document is for informational purposes only.

[4] IETF: draft-yegani-gre-key-extension

Editor Note: The above document is a work in progress and should not be referenced unless and until it is approved and published. Until such time as this Editor’s Note is removed, the inclusion of the above document is for informational purposes only.

[5] IETF: RFC 2131, Dorms, “Dynamic Host Configuration Protocol”, March 1997.

[6] IETF: RFC3046, Patrik, “DHCP Relay Agent Information Option”, January 2001.

[7] IETF: RFC4039, Park, et.al., “Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)”, March 2005.

[8] IETF: RFC3543, Glass, et.al., “Registration Revocation in Mobile IPv4”, August 2003.

[9] IETF: RFC 3775, D. Johnson, et.al., “Mobility Support in IPv6”, June 2004.

[10] IETF: RFC2794, Calhoun, et.al., “Mobile IP Network Access Identifier Extension for IPv4”, March 2000.

[11] IETF: RFC4862, Thomson, et. al., “IPv6 Stateless Address Autoconfiguration”, September 2007.

[12] IETF: RFC3041, Narten, et.al., “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”, January 2001.

[13] IETF: RFC4861, Narten, et.al., “Neighbor Discovery for IP Version 6 (IPv6)”, September 2007.

[14] IETF: RFC3012, Parkins, et.al., “Mobile IPv4 Challenge/Response Extensions”, November 2000.

[15] 3GPP2: X.S0011-D v2.0, “cdma2000 Wireless IP Network Standard”, November 2008.

[16] IETF: RFC4861, Narten, et.al., “Neighbor Discovery for IP Version 6 (IPv6)”, September 2007.

[17] draft-muhanna-mip6-binding-revocation

Editor Note: The above document is a work in progress and should not be referenced unless and until it is approved and published. Until such time as this Editor’s Note is removed, the inclusion of the above document is for informational purposes only.

[18] IETF**:** RFC5213, Gundavelli, et al., “Proxy Mobile IPv6”, August 2008

[19] IETF: draft-ietf-netlmm-pmip6-ipv4-support

Editor Note: The above document is a work in progress and should not be referenced unless and until it is approved and published. Until such time as this Editor’s Note is removed, the inclusion of the above document is for informational purposes only.

[20] IETF: RFC4306, Kaufman., “Internet Key Exchange (IKEv2) Protocol”, December 2005.

[21] 3GPP2: X.S0054-910-A, “Converged Access Network Data Dictionary”, August 2008

[22] IETF: RFC 4285, Patel, et. al., “ Authentication Protocol for Mobile IPv6”, January 2006

2.2 Informative References

This section provides references to other documents that may be useful for the reader of this document.

No informative references are identified.

3 PMIPv4 Operation

This section specifies the requirements for PMIPv4 Operation.

3.1 Protocol Stack

Figure 1 shows the protocol reference model for Simple IPv4/Simple IPv6 with PMIP4 signaling data between the PDSN and the HA. Figure 2 shows the protocol reference model for Simple IPv4 with PMIP for PPP free user data between the AT and CN. Figure 3 shows the protocol reference model for Simple IPv4 with PMIP for PPP based user data between the AT and CN. Figure 4 shows the protocol reference model for Simple IPv6 with PMIP for PPP free user data between the AT and CN. Figure 5 shows the protocol reference model for Simple IPv6 with PMIP for PPP based user data between the AT and CN.

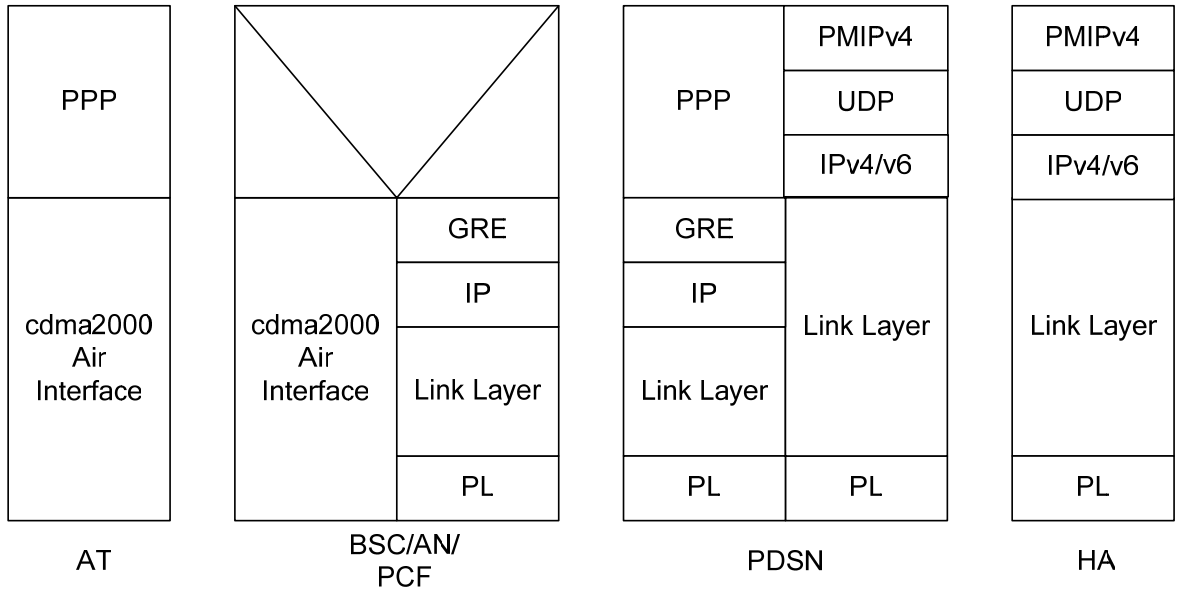

Figure 1 **Control Plane Protocol Stack for Simple IPv4/v6 with over PMIP4 Operation**

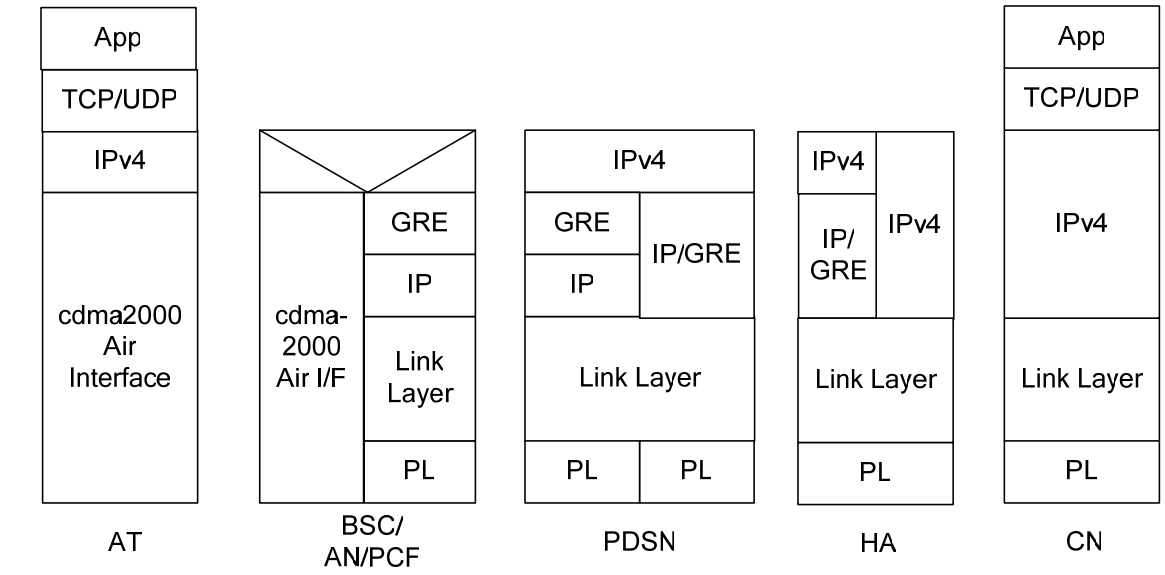

Figure 2 **PPP free (HDLC free) User Plane Protocol Stack for Simple IPv4 with PMIP4 Operation**

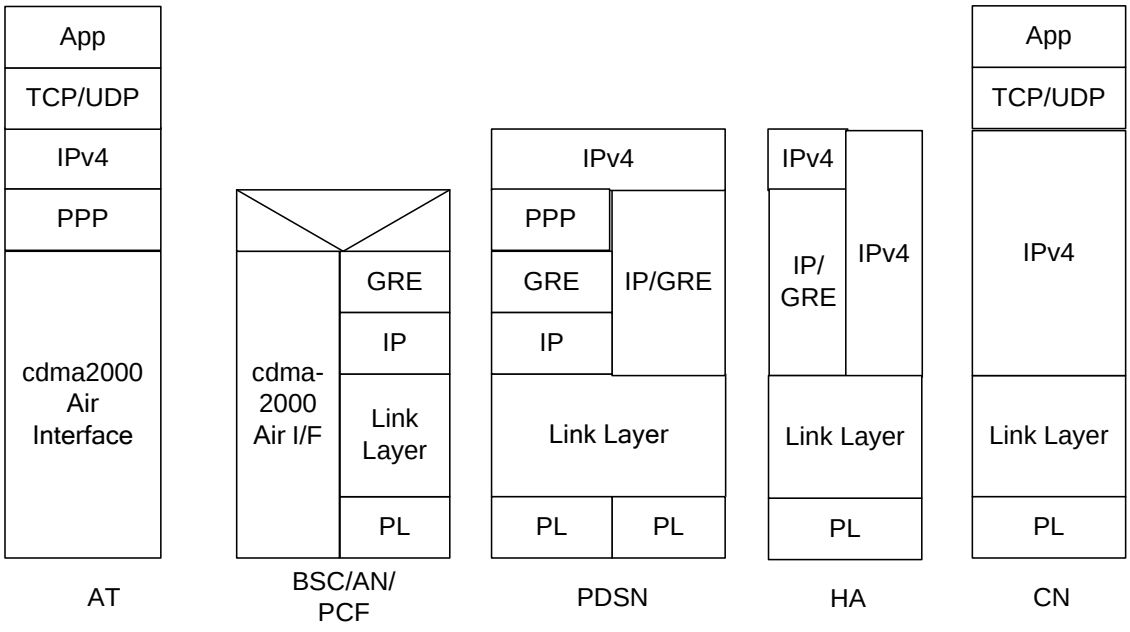

Figure 3 **PPP based (HDLC based) User Plane Protocol Stack for Simple IPv4 with PMIP4 Operation**

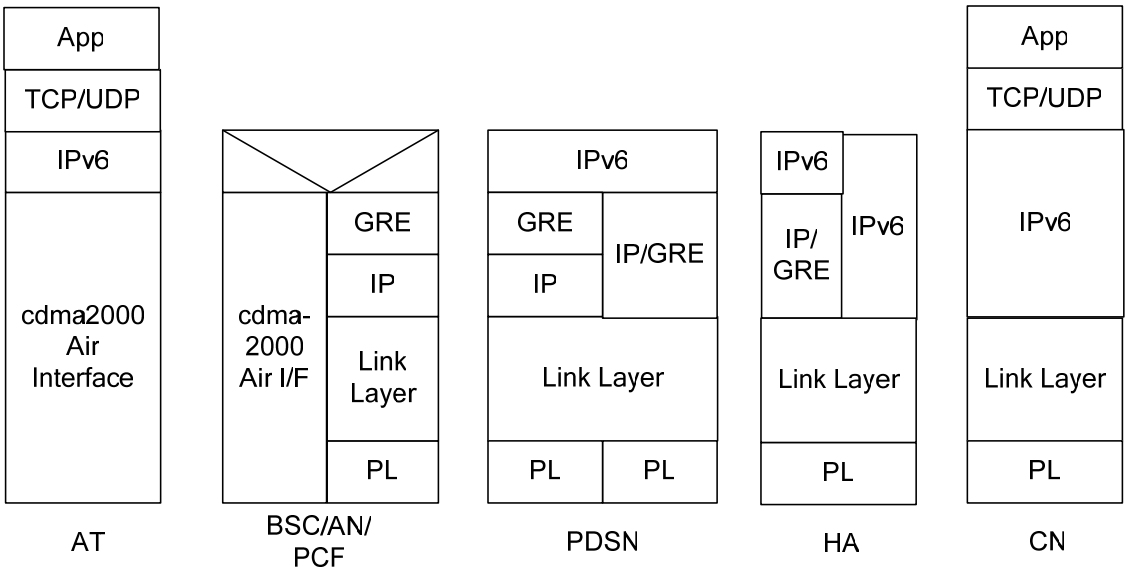

Figure 4 **PPP free (HDLC free) User Plane Protocol Stack for IPv6 with PMIP4 Operation**

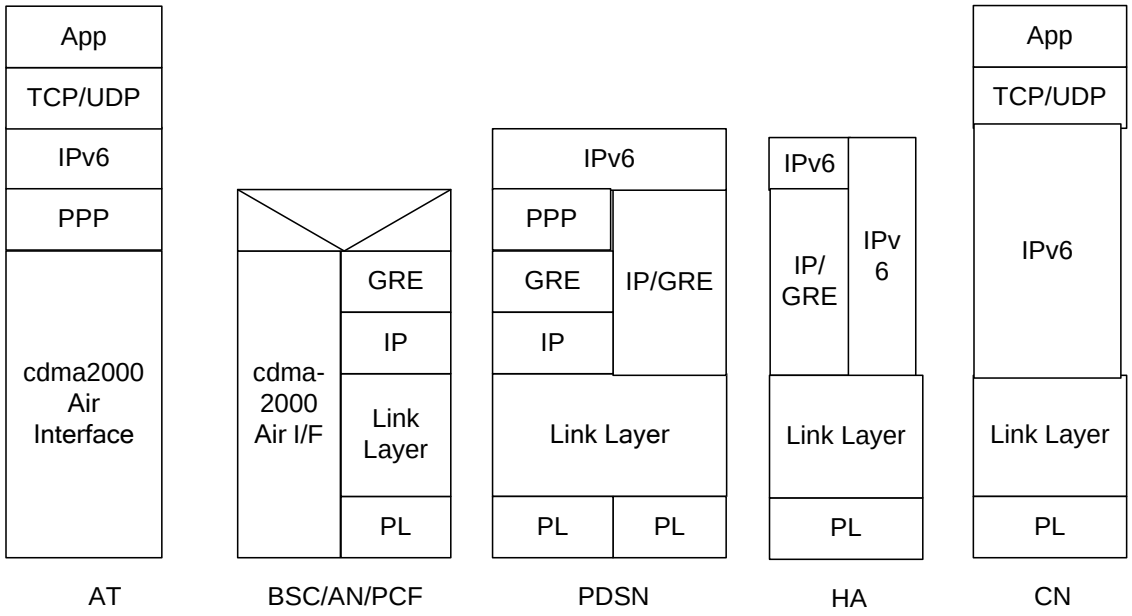

Figure 5 **PPP based (HDLC based) User Plane Protocol Stack for IPv6 with PMIP4 Operation**

3.2 PDSN Requirements

The PDSN may support PMIP4 operation as specified in this section.

3.2.1 Authentication and Authorization Support for PMIP Service

A PDSN supporting PMIP4 based mobility shall include in the Access-Request message sent to the HAAA during the access authentication and authorization procedures for an AT, the PMIP-Based-Mobility-Capability VSA to indicate to the HAAA that it supports PMIP4. If the visited network supports local HA assignment for PMIP, the PDSN may allocate an HA in the visited network and include the VAAA-Assigned-HA-IPv4-Service Subtype in PMIP-HA-Info-IPv4-Service VSA, or VAAA-Assigned-HA-IPv6-Service Subtype in PMIP-HA-Info-IPv6-Service VSA in the RADIUS Access-Request message sent to the HAAA during access authentication and authorization. See [21] for the definition of the RADIUS VSAs used for this purpose.

3.2.2 IP Address Assignment

3.2.2.1 IPv4 Addressing with IPCP

PDSN requirements for IP addressing with IPCP are specified in [15] with exceptions defined here.

- If the PDSN receives an IPCP Configure-Request message without including an IP Address Option from an AT that is authorized for PMIP4 based mobility then:
  - If the network prefers to grant PMIP4 based mobility to the AT based on the network policy, then the PDSN shall trigger PMIP4 procedures to acquire an IPv4 address and shall wait for PMIP4 signaling to finish before responding to the AT. If the PMIP4 registration is successful, then, the PDSN shall send IPCP Configure Nak including the IP Address Option to the AT.
  - Otherwise, the PDSN shall send IPCP Configure Ack without including the IP address option and shall follow the CMIP requirements specified in [15]
- If the PDSN receives an IPCP Configure-Request message containing an IP Address Option from an AT that is authorized for PMIP4 based mobility, then:
  - If the network prefers to grant PMIP4 based mobility to the AT, then the PDSN shall trigger PMIP4 procedures to acquire an IPv4 address and shall wait for PMIP4 signaling to finish before sending Configure-Nak/Configure-Ack to the AT. If the PDSN receives a notification from the HA indicating that the PMIP4 registration is successful, the PDSN shall set the IP Address Option of Configure-Nak/Configure-Ack message to the HoA received in the PMIP message.
  - Otherwise, the PDSN shall follow the procedures for Simple IPv4 operation as specified in [15].
- If the AT is not authorized for PMIP4 based mobility, the PDSN shall follow the procedures for Simple IPv4 or CMIPv4 operation as specified in [15].

The PDSN shall follow procedures defined in Section 3.2.3 for network PMIP4 tunnel establishment.

3.2.2.2 IPv6 Addressing with IPv6CP

PDSN requirements for IPv6 addressing with IPv6CP are specified in [15] with exceptions defined here.

If a PDSN supporting PMIP4 based mobility receives an IPv6CP Configure-Request message containing Interface-Identifier Configuration Option from the AT, and if Interface-Identifier Configuration Option in Configure-Request message was set to 0, the PDSN shall assign an interface ID to the AT before sending PMIP4 message to the HA. The PDSN shall wait for PMIP4 signaling to finish before sending Configure-Nak/Configure-Ack to the AT.

The PDSN shall wait for PMIP4 and IPv6CP procedures to finish before sending Router Advertisement to the AT. If the PDSN receives a PMIP4 RRP indicating that the registration with the HA was successful, the PDSN shall extract the HN-Prefix that is assigned to the AT in the PMIP4 message and send IPv6 Router Advertisement message to the AT including the assigned HN Prefix in the Prefix Information Option. The Valid Lifetime field of the Prefix Information Option shall be set to a value not larger than the PMIP4 Registration Lifetime.

The PDSN shall follow procedures defined in Section 3.2.3 for network PMIP4 tunnel establishmentIf the AT is not authorized for PMIP4 based mobility, or if the PMIP registration is not successful, then the PDSN shall follow the procedures for Simple IPv6 operation as specified in [15] .

If the PDSN receives DHCPv6 MIP6 bootstrapping message from an AT that is already granted a PMIP4 based mobility and is not allowed to use simultaneous PMIP4 and CMIPv6, then the PDSN shall fail the MIP6 bootstrapping procedures by not including the HA information in the DHCP reply to the AT.

3.2.3 PMIP4 Tunnel Management

The PDSN supporting Simple IP ATs with PMIP4 shall act as a Proxy Mobility Agent (PMA) as specified in [3] and [8].

Once PMIP4 is triggered, the PDSN shall send a Proxy Registration Request (PRRQ) to the HA as specified in [3]. The PDSN shall know the following information to be able to send the PRRQ:

- the user's Network PMIP NAI,
- mobility security information,
- the HA address.

This information is obtained during PPP authentication phase.

If the PDSN requests an IPv4 address from the HA for the AT, the PDSN shall set the Home Address (HoA) field in the PRRQ to 0.0.0.0. If the PDSN knows the AT's IPv4 address (e.g., the IP address specified as a hint in the IP Address option of IPCP Configuration Request message or the IPv4 address received as part of context transfer procedures), it shall set the IPv4 Home Address field to the known IPv4 home address. . In addition, if the AT is already assigned an IPv6 Prefix earlier for the same PMIP NAI and by the same HA, then the PDSN shall set the IPv6 Prefix Extension field in the PRRQ message to the IPv6 Prefix that is already assigned to the AT.

If the PDSN requests an IPv6 Prefix allocation from the HA for the AT, the PDSN shall set the IPv6 Prefix Extension field in the PRRQ to 0::/0. If the PDSN knows the AT's IPv6 prefix it shall set the IPv6 Prefix Extension to the known IPv6 Prefix. Optionally, the PDSN may include Interface ID Extension with AT's interface identifier negotiated during PPP NCP phase. In addition, if the AT is already assigned an IPv4 Home Address earlier for the same PMIP NAI and by the same HA, then the PDSN shall set the Home Address (HoA) field in the PRRQ message to the IPv4 Home Address that is already assigned to the AT.

Optionally, the PDSN may include the GRE key extension in the PRRQ message, with the value set as defined in [4].

If the PDSN wants to indicate its support for registration revocation to the HA, the PDSN shall include Mobile IP Revocation Support extension in the PRRQ sent to the HA. If the PDSN receives a PRRP that does not include Mobile IP Revocation Support extension, the PDSN shall assume that HA does not support registration revocation.

For securing the PRRQ, the PDSN shall compute the MN-HA Authentication Extension using the PMN-HA key received from HAAA during PPP authentication phase. The SPI field in MN-HA Authentication Extension is set to PMN-HA-SPI which is also received from HAAA during PPP authentication phase.

Upon receiving the PRRP, the PDSN shall verify that the PMN-HA-SPI received in the MN-HA Authentication Extension of the PRRP is associated with the stored value of PMN-HA key. If verification is successful, the PDSN shall use the PMN-HA key to validate the MN-HA Authentication Extension in the PRRP. Successfully authenticated PRRP shall indicate that the PDSN has established a security association with the HA.

Upon successful registration (e.g., reply code in PRRP is set to 0) the PDSN shall follow the procedures as specified in sections 3.2.2. . If the IP address assignment is not successful, and if the AT is already assigned either an IPv4 Home Address or an IPv6 Prefix prior to this registration and if the Home Address (HoA) field or IPv6 Prefix Extension field is included in the PRRP message, then, the address that is already assigned to the AT is not considered deregistered.

The PDSN shall send a PRRQ with lifetime = 0 to the HA if any of the following conditions are true:

- The PDSN determines that the HoA needs to be deregistered for an AT that has only HoA
- The PDSN determines that the IPv6 prefix needs to be deregistered for an AT that has only IPv6 prefix
- The PDSN determines that both the IPv6 prefix and HoA need to be deregistered for an AT that has both IPv6 prefix and HoA.

If the PDSN requests to release only an IPv4 HoA from the HA for the AT that has both IPv4 HoA and IPv6 Prefix, the PDSN shall not include the Home Address (HoA) field in the PRRQ message and shall set the IPv6 Prefix Extension field in the PRRQ message to the IPv6 Prefix that is already assigned to the AT.

If the PDSN determines to release only an IPv6 Prefix from the HA for the AT that has both IPv4 HoA and IPv6 Prefix, the PDSN shall not include the IPv6 Prefix Extension field in the PRRQ message and shall set the Home Address (HoA) field in the PRRQ message to the HoA that is already assigned to the AT.

If the PDSN determines that the PMIP Registration Lifetime needs to be extended, the PDSN shall follow the procedure defined in [3] to renew the PMIP Registration Lifetime with the HA.

If the PDSN receives the PMIP Registration Revocation message from the HA, and if the PDSN negotiated registration revocation support with the HA as specified above, the PDSN shall validate the message. Upon successful validation, the PDSN shall clean up the resources associated with the AT's IP address that is being revoked and send a PMIP Registration Revocation Acknowledgment message to the HA as specified in [3] and [8]. .

3.2.4 Ingress Address Filtering

The PDSN shall check the source IP address of every packet received from AT. Upon receiving packets from an AT with an invalid source IP address, except for IPCP packets with the IP address set to all 0s, the PDSN shall silently discard the packets.

3.3 HA Requirements

The HA supporting PMIP4 shall follow Mobile IPv4 procedures as specified in [3] and [8].

3.3.1 IP Address Assignment with PMIP4

If the GRE extension was included in the PRRQ, the HA shall process it in accordance with [4] and include a GRE key extension in the PRRP.

Upon receiving a PRRQ that includes Mobile IP Revocation Support extension, the HA supporting registration revocation shall include Mobile IP Revocation Support extension in the PRRP sent to the PDSN. Upon receiving a PRRQ that does not include Mobile IP Revocation Support extension, the HA shall assume that the PDSN does not support registration revocation.

If the HA has already assigned an IPv4 Home Address to the AT and that address does not match with the IPv4 Home address field, if present, in the PRRQ message, then the HA shall reject this registration by sending PRRP with the error code "Administratively prohibited (65)". If the HA has already assigned an IPv6 Prefix to the AT and that IPv6 Prefix does not match with the IPv6 Prefix Extension field, if present, in the PRRQ message, then the HA shall reject this registration by sending PRRP message with the error code "Administratively prohibited (65)".

Upon accepting a PRRQ request for extending the lifetime of a currently active registration, the HA shall update the lifetime for that binding and send a PRRP message to the PDSN.

3.3.1.1 IPv4 Address Assignment

If validation of the PRRQ is successful , the HA shall allocate an IPv4 address to the user if HoA in the PRRQ was set to 0.0.0.0 and the HA does not have a Mobility Binding Entry (MBE) associated with this NAI (e.g., initial connection setup). Otherwise, if HoA in the

PRRQ was set to all zeros and the HA has an MBE associated with this NAI with a valid IPv4 address or if PRRQ contains a non-zero HoA that is supported by this HA, the HA shall record the binding in the MBE. The HA shall send Proxy Registration Reply (PRRP) to the source address of the received PRRQ and include the HoA associated with the MBE. If PRRQ contains a non-zero HoA that is not supported by this HA or is not matching the HoA recorded in the MBE (if one exists) for this NAI, the HA shall reject this registration by sending PRRP with the error code "Administratively prohibited (65)". The HA shall secure the PRRP as specified in Section 8.2.4.3.

If this IPv4 HoA is assigned in addition to an IPv6 Prefix that is already assigned to the AT and if the IPv6 Prefix Extension field is included in the PRRQ message, then the HA shall set the IPv6 Prefix Extension field in the PRRP message to that IPv6 Prefix. If this IPv4 HoA is assigned in addition to an IPv6 Prefix that is already assigned to the AT and if the IPv6 Prefix Extension field is not included in the PRRQ message, then the HA shall delete the binding for the IPv6 Prefix and shall not include the IPv6 Prefix Extension field in the PRRP message.

3.3.1.2 IPv6 Address Assignment

If validation of the PRRQ is successful, the HA shall assign an IPv6 Prefix to the user if the IPv6 Prefix Extension in the PRRQ was set to 0::/0 and the HA does not have a Mobility Binding Entry (MBE) associated with this NAI (e.g., for initial connection setup). Otherwise, if IPv6 Prefix Extension in the PRRQ was set to 0::/0 and the HA has an MBE associated with this NAI with a valid IPv6 Prefix or if PRRQ contains a non-zero IPv6 Prefix Extension that is supported by this HA, the HA shall record the binding in the MBE. The HA shall send a Proxy Registration Reply (PRRP) to the source address of the received PRRQ. The PRRP shall include the IPv6 Code Extension. If the PRRQ contains a non-zero IPv6 Prefix that is not supported by this HA or is not matching the IPv6 Prefix recorded in the MBE (if one exists) for this NAI, the HA shall reject this registration by sending PRRP including IPv6 Prefix Code Extension with the error code "Administratively prohibited (9)". The HA shall secure the PRRP as specified in Section 3.3.3

If this IPv6 Prefix is assigned in addition to an IPv4 HoA that is already assigned to the AT and if the IPv4 HoA field is included in the PRRQ message, then the LMA shall set the IPv4 HoA field in the PRRP message to that IPv4 HoA. If this IPv6 Prefix is assigned in addition to an IPv4 HoA that is already assigned to the AT and if the IPv4 HoA field is not included in the PRRQ message, then the LMA shall delete the binding for the IPv4 HoA from its Binding Cache and shall not include the IPv4 HoA field in the PRRP message.

3.3.2 IP Address/HN Prefix Release with PMIP4

When the HA receives a PRRQ with lifetime = 0 from the PDSN associated with the MBE for that particular AT, the HA shall validate the authentication extension. If the validation is successful, the HA shall delete the MBE for that user. The HA shall respond back with a PRRP with lifetime=0 to confirm the successful IP address/HN prefix deregistration. Otherwise if the validation fails, the HA shall silently discard the PRRQ.

The HA may determine that the MBE for the user needs to be deregistered. In that case, if the HA supports registration revocation and had negotiated it with the PDSN during PMIP registration, the HA shall send a PMIP Registration Revocation message associated with the AT to the PDSN, as specified in [3] and [8]. Upon receiving Registration Revocation Acknowledgment message from the PDSN, the HA shall delete the AT's MBE.

3.3.3 PMIP4 Tunnel Management

3.3.3.1 RADIUS

Upon receiving PRRQ with the MN-HA Authentication extension, the HA shall check if the value of the PMN-HA-SPI received in the SPI field of the PRRQ is associated with any active security association for the current AT session. If HA finds the active SA for the AT with the same PMN-HA-SPI, the HA shall use the associated PMN-HA key to validate the received MN-HA Authentication Extension.

If the received PMN-HA-SPI does not match any currently active SA for this AT, the HA shall send RADIUS Access-Request to the HAAA, and include the User-Name attribute according to [15]. The HA shall include the PMN-HA-SPI value in the MN-HA SPI VSA. Upon receiving RADIUS Access-Accept, the HA shall use the PMN-HA key, received in the MN-HA Shared Key VSA, to validate the MN-HA Authentication Extension in the PRRQ and compute the MN-HA Authentication extension for the PRRP. In the MN-HA Authentication Extension of the PRRP, the HA shall set the SPI field to the PMN-HA SPI value received in the MN-HA SPI VSA of the RADIUS Access-Accept. For subsequent PMIP4 re-registrations, the HA shall use the PMN-HA key and PMN-HA-SPI to secure PRRP and verify the PRRQ.

3.4 AT Requirements

AT shall follow requirements specified in [15], with the following exceptions:

If an AT is using IPv4 and if the AT wants to use IP mobility, then the AT shall follow the procedures for MIP4 operation specified in [4] except for the following procedures:

- The AT shall perform access authentication (e.g., CHAP/PAP) during establishment of PPP session.

- If the AT obtains IPCP-Configure-Nak message with IP Address Option in response to IPCP-Configure Req message with no IP Address Option sent by the AT, then the access terminal shall initiate the simple-IP procedure operation specified in [4]

3.5 VAAA Requirements

3.5.1 RADIUS

During the PDSN authentication of a roaming AT, if the VAAA receives Access-Request from the PDSN with PMIP-Based-Mobility-Capability VSA included, the VAAA may perform one of the following for IPv4 services before sending the RADIUS Access-Request message to the HAAA:

- Include the PMIP-HA-Info-IPv4-Service VSA with the VAAA-Assigned-HA-IPv4-Service Subtype, if the PMIP-HA-Info-IPv4-Service VSA was not received from the PDSN;

- Replace HA IP address received in the VAAA-Assigned-HA-IPv4-Service Subtype with another HA IP address in the visited network, if the PMIP-HA-Info-IPv4-Service VSA was received from the PDSN;

- Forward the PMIP-HA-Info-IPv4-Service VSA without modifications, if received from the PDSN.

During the PDSN authentication of a roaming AT, if the VAAA receives Access-Request from the PDSN with PMIP-Based-Mobility-Capability VSA included, the VAAA may perform one of the following for IPv6 services before sending the RADIUS Access-Request message to the HAAA:

- Include the PMIP-HA-Info-IPv6-Service VSA with the VAAA-Assigned-HA-IPv6-Service Subtype, if the PMIP-HA-Info-IPv6-Service VSA was not received from the PDSN;

- Replace HA IP address received in the VAAA-Assigned-HA-IPv6-Service Subtype with another HA IP address in the visited network, if the PMIP-HA-Info-IPv6-Service VSA was received from the PDSN;

- Forward the PMIP-HA-Info-IPv6-Service VSA without modifications, if received from the PDSN.

The VAAA shall not modify the PMIP-HA-Info-IPv4-Service VSA and/or PMIP-HA-Info-IPv6-Service VSA in the RADIUS Access-Accept message received from the HAAA.

3.6 HAAA Requirements

3.6.1 Network PMIP4 Key Management

Upon successful initial Access Authentication, for the given user the HAAA shall generate a random unique value for the PMN-HA key and select a unique value that is greater than 255 for PMN-HA-SPI .

3.6.2 RADIUS

During PDSN Authentication, upon receiving a RADIUS Access-Request containing the PMIP-Based-Mobility-Capability VSA, if the AT is authorized for IPv4 with PMIP4 the HAAA shall perform one of the following before sending the RADIUS Access-Accept message:

- If the RADIUS Access-Request message contains PMIP-HA-Info-IPv4-Service VSA with VAAA-Assigned-HA-IPv4-Service Subtype, and if the HAAA authorizes the visited network to assign a local HA, the HAAA shall include PMIP-HA-Info-IPv4-Service VSA with received VAAA-Assigned-HA-IPv4-Service Subtype as well as associated PMN-HA key Subtype and PMN-HA-SPI Subtype, in the RADIUS Access-Accept message. The HAAA shall not include the HAAA-Assigned-HA-IPv4-Service Subtype in PMIP-HA-Info-IPv4-Service VSA in the RADIUS Access-Accept message.

- If the RADIUS Access-Request message contains PMIP-HA-Info-IPv4-Service VSA with VAAA-Assigned-HA-IPv4-Service Subtype, and if the HAAA decides to assign an HA, the HAAA shall not include VAAA-Assigned-HA-IPv4-Service Subtype in the RADIUS Access-Accept message and shall include PMIP-HA-Info-IPv4-Service VSA with the HAAA-Assigned-HA-IPv4-Service Subtype which contains the address of an HA assigned by the HAAA. The HAAA shall also include associated PMN-HA key Subtype and PMN-HA-SPI Subtype in PMIP-HA-Info-IPv4-Service VSA in the RADIUS Access-Accept message.

- If the RADIUS Access-Request message does not contain PMIP-HA-Info-IPv4-Service VSA with VAAA-Assigned-HA-IPv4-Service Subtype, the HAAA shall include PMIP-HA-Info-IPv4-Service VSA with HAAA-Assigned-HA-IPv4-Service Subtype as well as associated PMN-HA key Subtype and PMN-HA-SPI Subtype in the RADIUS Access-Accept message.

If the AT is not authorized for IPv4 with PMIP4, the HAAA shall not include PMIP-HA-Info-IPv4-Service VSA in the RADIUS Access-Accept message.

During PDSN Authentication, upon receiving a RADIUS Access-Request containing the PMIP-Based-Mobility-Capability VSA, if the AT is authorized for IPv6 with PMIP4 the HAAA shall perform one of the following before sending the RADIUS Access-Accept message:

- If the RADIUS Access-Request message contains PMIP-HA-Info-IPv6-Service VSA with VAAA-Assigned-HA-IPv6-Service Subtype, and if the HAAA authorizes the visited network to assign a local HA, the HAAA shall include PMIP-HA-Info-IPv6-Service VSA with received VAAA-Assigned-HA-IPv6-Service Subtype as well as associated PMN-HA key Subtype and PMN-HA-SPI Subtype, in the RADIUS Access-Accept message. The HAAA shall not include the HAAA-Assigned-HA-IPv6-Service Subtype in PMIP-HA-Info-IPv6-Service VSA in the RADIUS Access-Accept message.

- If the RADIUS Access-Request message contains PMIP-HA-Info-IPv6-Service VSA with VAAA-Assigned-HA-IPv6-Service Subtype, and if the HAAA decides to assign an HA, the HAAA shall not include VAAA-Assigned-HA-IPv6-Service Subtype in the RADIUS Access-Accept message and shall include PMIP-HA-Info-IPv6-Service VSA with the HAAA-Assigned-HA-IPv6-Service Subtype which contains the address of an HA assigned by the HAAA. The HAAA shall also include associated PMN-HA key Subtype and PMN-HA-SPI Subtype in PMIP-HA-Info-IPv6-Service VSA in the RADIUS Access-Accept message.

- If the RADIUS Access-Request message does not contain PMIP-HA-Info-IPv6-Service VSA with VAAA-Assigned-HA-IPv6-Service Subtype, the HAAA shall include PMIP-HA-Info-IPv6-Service VSA with HAAA-Assigned-HA-IPv6-Service Subtype as well as associated PMN-HA key Subtype and PMN-HA-SPI Subtype in the RADIUS Access-Accept message.

If the AT is not authorized for IPv6 with PMIP, the HAAA shall not include PMIP-HA-Info-IPv6-Service VSA in the RADIUS Access-Accept message.

During the initial PMIP4 registration, upon receiving a RADIUS Access-Request from an HA, which contains the MN-HA-SPI VSA, the HAAA shall retrieve the PMN-HA key

associated with the value of PMN-HA-SPI received in the MN-HA SPI VSA. The HAAA shall include the MN-HA Shared Key VSA (containing the PMN-HA key) and the MN-HA SPI VSA (containing the PMN-HA-SPI) in the RADIUS Access-Accept sent to the HA. The keys shall be derived as specified in Section 3.6.1.

Table 1provides a list of additional RADIUS Attributes exchanged between an PDSN and AAA Server during Access Authentication and Authorization for support of Simple IP with network PMIP4.

Table 1 **Additional RADIUS Attributes exchanged between PDSN and AAA during Access Authentication and Authorization for Supporting Network PMIP for IP Services**

Attribute Name	Type	Access-Request	Access-Accept	Interface(s)
Network-PMIP-NAI	26/192	0	0-1	PDSN <-> HAAA
PMIP-Based-Mobility-Capability	26/193	0-1	0-1	PDSN <-> HAAA
PMIP-HA-Info-IPv4-Service	26/194	0-1	0-1	PDSN<->HAAA
PMIP-HA-Info-IPv6-Service	26/195	0-1	0-1	PDSN<->HAAA

Table 2 provides a list of RADIUS Attributes exchanged between HA and AAA for support of network PMIP4.

Table 2 **RADIUS Attributes exchanged between HA and AAA for Supporting PMIP4**

Attribute Name	Type	Access-Request	Access-Accept	Interface(s)
MN-HA-SPI	26/57	1	1	HA <-> AAA
MN-HA Shared Key	26/58	0	1	HA <- AAA
Network-PMIP-NAI	26/192	1	0	HA -> AAA

4 PMIPv6 Operation

This section specifies the requirements for PMIPv6 Operation.

4.1 Protocol Stack

Figure 6 shows the protocol reference model for Simple IPv4/Simple IPv6 with PMIP6 signaling data between the PDSN and the LMA. Figure 7 shows the protocol reference model for HDLC free user data for Simple IPv4 with PMIPv6 between the AT and CN. Figure 8 shows the protocol reference model for HDLC based user data for Simple IPv4 with PMIPv6 between the AT and CN. Figure 9 shows the protocol reference model for HDLC based user data for Simple IPv6 with PMIPv6 between the AT and CN. Figure 10 shows the protocol reference model for HDLC based user data for Simple IPv6 with PMIPv6 between the AT and CN.

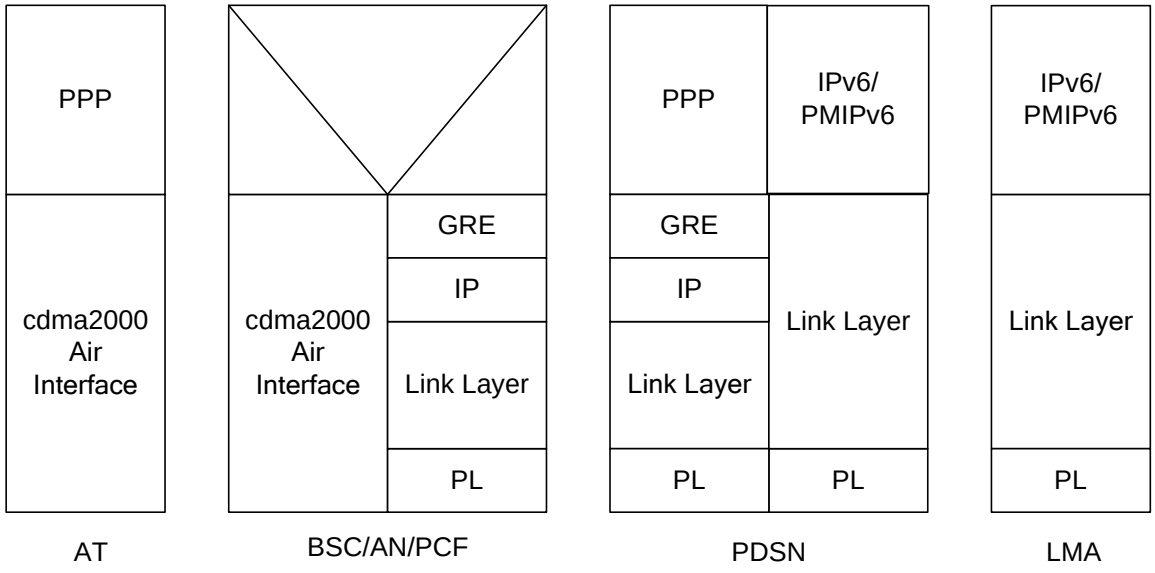

Figure 6 **Control Plane Protocol Stack for Simple IPv4/Simple IPv6 with PMIPv6 Operation**

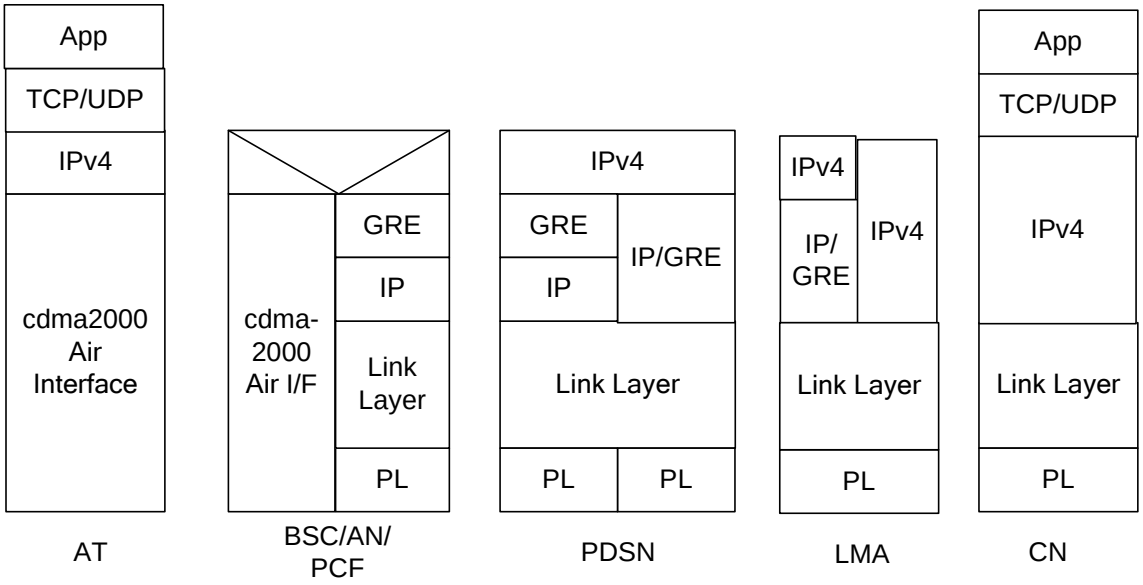

Figure 7 **PPP free(HDLC free) User Plane Protocol Stack for Simple IPv4 with PMIP6 Operation**

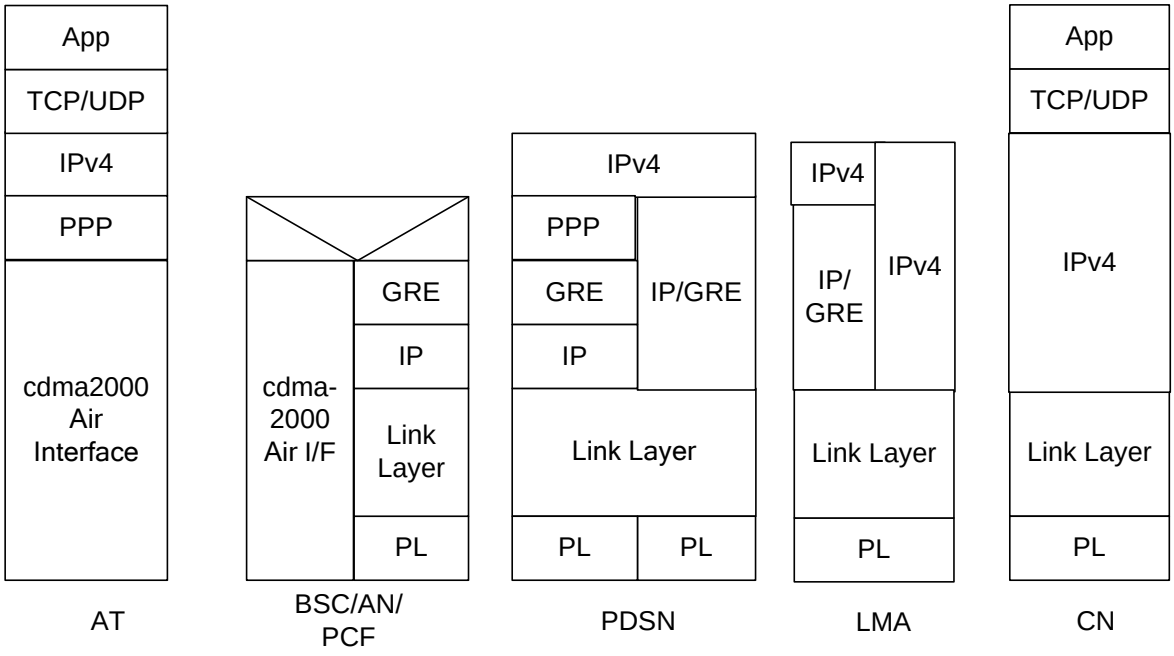

Figure 8 **PPP based (HDLC based) User Plane Protocol Stack for Simple IPv4 with PMIP6 Operation**

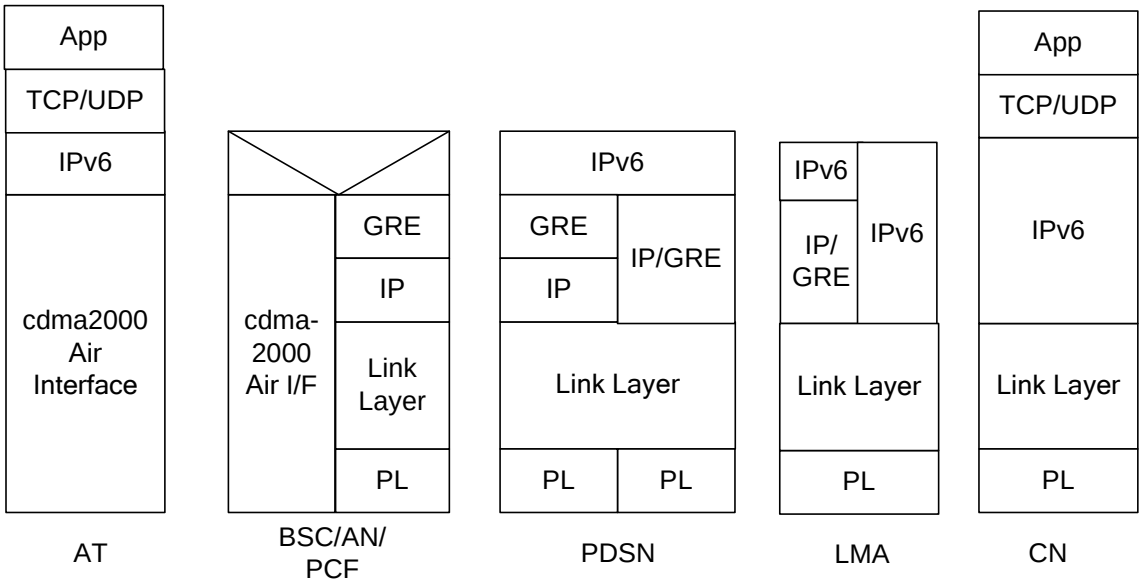

Figure 9 **PPP free(HDLC free) User Plane Protocol Stack for Simple IPv6 with PMIP6 Operation**

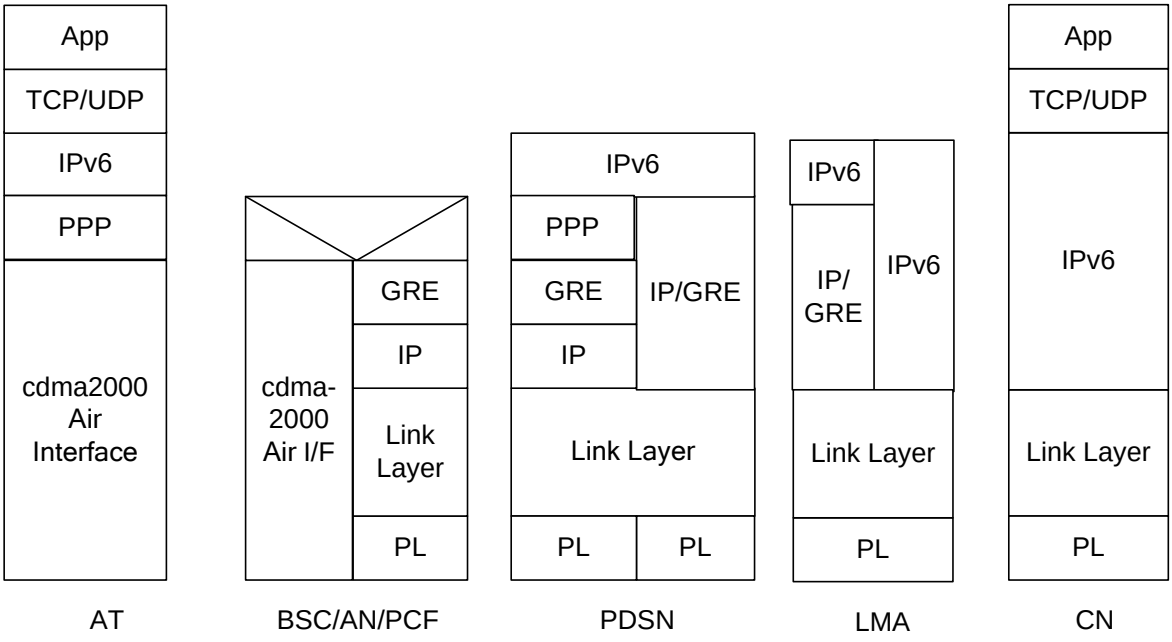

Figure 10 **PPP based (HDLC based) User Plane Protocol Stack for Simple IPv6 with PMIP6 Operation**

4.2 PDSN Requirements

The PDSN may support the MAG functionality for PMIP6 operation as specified in this section.

4.2.1 Authentication and Authorization Support for PMIP6 Service

A PDSN supporting PMIP6 based mobility shall include in the Access-Request message sent to the HAAA during the access authentication and authorization procedures for an AT, the PMIP-Based-Mobility-Capability VSA to indicate to the HAAA that it supports PMIP6. If the visited network supports local LMA assignment for PMIP6, the PDSN may allocate an LMA from the visited network and include either the VAAA-Assigned-LMA-IPv4-Service Subtype in PMIP-HA-Info-IPv4-Service VSA, or VAAA-Assigned-LMA-IPv6-Service Subtype in PMIP-HA-Info-IPv6-Service VSA or both in the RADIUS Access-Request message sent to the HAAA during access authentication and authorization. See [21] for the definition of the RADIUS VSAs used for this purpose.

4.2.2 IP Address Assignment

4.2.2.1 IPv4 Addressing with IPCP

PDSN requirements for IP addressing with IPCP are specified in [X.S0011-002-D] with exceptions defined here.

- If the PDSN receives an IPCP Configure-Request message without including an IP Address Option from an AT that is authorized for PMIP6 based mobility then,
  - if the network prefers to grant PMIP6 based mobility to that AT based on the network policy, then the PDSN shall trigger PMIP6 procedures to acquire an IPv4 address and shall wait for PMIP signaling to finish before responding to the AT. If the PMIP6 registration is successful, then, the PDSN shall send IPCP Configure Nak including the IP Address Option to the AT.
  - Otherwise, the PDSN shall send IPCP Configure Ack without including the IP address option and shall follow the CMIP requirements specified in [4]
- If the PDSN receives an IPCP Configure-Request message containing an IP Address Option from the AT that is authorized for PMIP6 based mobility, then:
  - If the network prefers to grant PMIP6 based mobility to the AT, then the PDSN shall trigger PMIP6 procedures to acquire an IPv4 address and shall wait for PMIP6 signaling to finish before sending Configure-Nak/Configure-Ack to the AT. If the PDSN receives a notification from the LMA indicating that the PMIP6 registration is successful, the PDSN shall set the IP Address Option of Configure-Nak/Configure-Ack message to the HoA received in the PMIP6 message.
  - Otherwise, the PDSN shall follow the procedures for Simple IPv4 operation as specified in [4].
- If the AT is not authorized for PMIP6 based mobility, the PDSN shall follow the procedures for Simple IPv4 or CMIPv4 operation as specified in [4].

The PDSN shall follow procedures defined in Section 4.2.2 for network PMIP6 tunnel establishment

4.2.2.2 IPv6 Addressing with IPv6CP

PDSN requirements for IPv6 addressing with IPv6CP are specified in [X.S0011-002-D] with exceptions defined here.

If a PDSN supporting PMIP6 based mobility receives an IPv6CP Configure-Request message containing Interface-Identifier Configuration Option from the AT, and if Interface-Identifier Configuration Option in Configure-Request message was set to 0, the PDSN shall assign an interface ID to the AT before sending PMIP6 message to the LMA. The PDSN shall wait for PMIP6 signaling to finish before sending Configure-Nak/Configure-Ack to the AT.

The PDSN shall wait for PMIP6 and IPv6CP procedures to finish before sending Router Advertisement to the AT. If the PDSN receives a PMIP6 BA indicating that the registration with the LMA was successful, the PDSN shall extract the HN-Prefix that is assigned to the AT in the PMIP6 message and send IPv6 Router Advertisement message to the AT including the assigned HN Prefix in the Prefix Information Option. The Valid Lifetime field of the Prefix Information Option shall be set to a value not larger than the PMIP6 Registration Lifetime.

The PDSN shall follow procedures defined in Section 4.2.2 for network PMIP6 tunnel establishment

If the AT is not authorized for PMIP6 based mobility, or if the PMIP6 registration is not successful, then the PDSN shall follow the procedures for Simple IPv6 operation as specified in[15].

If the PDSN receives DHCPv6 MIP6 bootstrapping message from an AT that is already granted a PMIP6 based mobility and is not allowed to use simultaneous PMIP6 and CMIPv6, then the PDSN shall fail the MIP6 bootstrapping procedures by not including the HA information in the DHCP reply to the AT.

4.2.3 PMIP6 Tunnel Management

The PDSN supporting Simple IP ATs with PMIP6 shall act as a Mobile Access Gateway (MAG) as specified in [18], [19] and [17].

Once PMIP6 is triggered, the PDSN shall send a Proxy Binding Update (PBU) to the LMA with the Proxy Registration Flag set to 1. The PDSN shall know the following information to be able to send the PBU:

- the user's PMIP NAI,
- the LMA address.

This information is obtained during PPP authentication phase.

If the PDSN requests an IPv4 address from the LMA for the AT, the PDSN shall include the IPv4 Home Address Option and PMIP6 NAI Option in the Proxy Binding Update. If the PDSN needs to request an IPv4 address allocation from the LMA, it shall set the Home Address field in the PBU to 0.0.0.0. If the PDSN knows the IPv4 address, it shall set the IPv4 Home Address field to the known IPv4 address. In addition, if the AT is already assigned a Home Network Prefix earlier for the same PMIP NAI and by the same LMA, then the PDSN

shall set the Home Network Prefix option in the PBU message to the Home Network Prefix that is already assigned to the AT.

If the PDSN requests an IPv6 address from the LMA for the AT, the PDSN shall include the Home Network Prefix Option and NAI Option. If the PDSN needs to request an HN Prefix allocation from the LMA, it shall set the HN Prefix Option field in the PBU to set 0::/0. If the PDSN knows the HN Prefix, it shall set the HN Prefix Option field to the known HN Prefix. Optionally, the PDSN may include Mobile Node Interface Identifier Option with AT's interface identifier negotiated during PPP NCP phase. . In addition, if the AT is already assigned an IPv4 address earlier for the same PMIP NAI and by the same LMA, then the PDSN shall set the IPv4 Home Address field in the PBU message to the IPv4 address that is already assigned to the AT.

Upon receiving a Proxy Binding Acknowledgment (PBA), the PDSN shall inspect the PBA for security verification. Upon successful security verification, the PDSN shall inspect PBA for status codes. If registration is successful, the PDSN shall extract the HoA/HN Prefix from the PBA, and shall follow the procedures as specified in sections 4.2.2. If the IP address assignment is not successful, and if the AT is already assigned either an IPv4 address or an IPv6 address prior to this registration and if the IPv4 Home Address field or Home Network Prefix option is included respectively in the PBA message, then, the address that is already assigned to the AT is not considered deregistered.

If the PDSN determines that the IP address/HN Prefix needs to be deregistered, the PDSN shall send a PBU with lifetime = 0 to the LMA.

The PDSN shall send a PBU with lifetime = 0 to LMA if any of the following conditions are true:

- The PDSN determines that the IPv4 Home Address needs to be deregistered for an AT that has only IPv4 Home Address.
- The PDSN determines that the HN prefix needs to be deregistered for an AT that has only IPv6 address.
- The PDSN determines that both the HN prefix and IPv4 Home Address need to be deregistered for an AT that has both IPv6 address and HoA.

If the PDSN requests to release only an IPv4 address from the LMA for the AT that has both IPv4 Home Address and IPv6 Home Network Prefix, the PDSN shall not include the IPv4 Home Address option in the PBU message and shall set the Home Network Prefix option in the PBU message to the Home Network Prefix that is already assigned to the AT.

If the PDSN requests to release only Home Network Prefix from the HA for the AT that has both IPv4 Home Address and IPv6 Home Network Prefix, the PDSN shall not include the IPv6 Prefix Extension field in the PRRQ message and shall set the Home Address (HoA) field in the PRRQ message to the HoA that is already assigned to the AT.

If the PDSN receives the PMIPv6 Registration Revocation Request message from the LMA, the PDSN shall clean up the resources associated with the AT's IP address that is being revoked and send a PMIPv6 Registration Revocation Ack message to the LMA as specified in [17].

4.2.3.1 PMIP6 Signaling Protection

The PMIPv6 signaling messages between the PDSN and the LMA shall be protected.

4.2.3.1.1 Authentication Protocol Support

If the HAAA returns PMN-LMA Key and PMN-LMA-SPI to the PDSN during PPP authentication phase, the PDSN shall compute the MN-HA Mobility Message Authentication Option in PBU using the PMN-LMA key received from HAAA during PPP authentication phase. The SPI field in MN-HA Mobility Message Authentication Option of PBU is set to PMN-LMA-SPI which is also received from HAAA during PPP authentication phase.

Upon receiving the PBA, the PDSN shall verify that the PMN-LMA-SPI received in the MN-HA Mobility Message Authentication Option of the PBA is associated with the stored value of PMN-LMA key. If verification is successful, the PDSN shall use the PMN-LMA key to validate the MN-HA Mobility Message Authentication Option of the PBA. Successfully authenticated PBA shall indicate that the PDSN has established a security association with the LMA.

4.2.3.1.2 IPsec Support

In case the interface between the PDSN and the LMA is not trusted, IPSec shall be used for the link protection. When the PMIPv6 signaling messages exchanged between the PDSN and the LMA are protected using IPsec via the established security association between them, then IKEv2 is used to setup security associations between the PDSN/MAG and the LMA to protect the Proxy Binding Update and Proxy Binding Acknowledgment messages.

4.2.4 Ingress Address Filtering

The PDSN shall check the source IP address of every packet received from AT. Upon receiving packets from an AT with an invalid source IP address, except for IPCP packets with the IP address set to all 0s, the PDSN shall silently discard the packets.

4.3 LMA Requirements

The LMA supporting PMIP6 shall act as a Local Mobility Anchor as specified in [18], [19] and [17].

4.3.1 IP Address Assignment with PMIP6

Upon receiving a Proxy Binding Update message from the PDSN on behalf of an AT, the LMA shall process the request as defined in [18]. If the LMA has already assigned an IPv4 address to the AT and if that address does not match with the IPv4 Home address field, if present, in the PBU message, then the LMA shall reject this registration by sending PBA message with the error code “Administratively prohibited (129)”. If the LMA has already assigned a Home Network Prefix to the AT and that Home Network Prefix does not match with the Home Network Prefix option, if present, in the PBU message, then the LMA shall reject this registration by sending PBA message with the error code “Administratively prohibited (129)”.

4.3.1.1 IPv4 Address Assignment

Upon receiving a Proxy Binding Update (PBU) message from the PDSN on behalf of the AT, the LMA shall process the request as defined in [18] and [19]. The LMA before accepting a Proxy Binding Update containing the IPv4 Home Address Option shall check if the AT is configured for IPv4 home address mobility service as defined in [19]. If the LMA determines that the AT is configured for IPv4 home address mobility service, and if the value of the IPv4 Home Address Option is set to 0.0.0.0 and the LMA has no binding cache entry associated with this NAI, the LMA shall assign an IPv4 address to the AT. Otherwise, if the Home Address Option in the PBU was set to all zeros and LMA has a binding cache entry associated with this NAI with assigned IPv4 address or if PBU contains a non-zero Home Address Option, the LMA needs to ensure that the AT is authorized to use the specified IPv4 address. If that is the case, the LMA shall accept the binding and create the binding cache entry. The LMA shall also send the Proxy Binding Acknowledgment (PBA) message to the PDSN. The PBA message shall include an IPv4 Address Acknowledgment Option in the mobility header and the assigned HoA. If the PBU contains a non-zero Home Address Option that is not supported by this LMA or is not matching the IPv4 address recorded in the binding cache entry (if one exists) for this NAI, the LMA shall reject this registration by sending PBA with the error code "Administratively prohibited (129)".

If this IPv4 address is assigned in addition to an HN Prefix that is already assigned to the AT and if the HN Prefix option is included in the PBU message, then the LMA shall set the HN Prefix Option in the PBA message to that HN Prefix. If this IPv4 address is assigned in addition to an IPv6 HN Prefix that is already assigned to the AT and if the HN Prefix option is not included in the PBU message, then the LMA shall delete the binding for the HN Prefix from its Binding Cache and shall not include the HN Prefix option in the PBA message.

4.3.1.2 IPv6 Address Assignment

If the HN Prefix in the PBU message is set to 0::/0 and the LMA has no binding cache entry associated with this NAI, the LMA shall allocate a prefix for the AT. Otherwise, if the HN Prefix in the PBU was set to 0::/0 and the LMA has a binding cache entry associated with this NAI with an assigned prefix, or if PBU contains a non-zero HN Prefix, the LMA shall ensure that the AT is authorized to use the specified HN prefix. If that is the case, the LMA shall accept the binding and update the binding cache entry. The LMA will also send the Proxy Binding Acknowledgment (PBA) message to the PDSN. The PBA message will include an HN Prefix Option in the mobility header containing the assigned HN Prefix. If PBU contains a non-zero HN Prefix that is not supported by this LMA or is not matching the HN Prefix recorded in the binding cache entry (if one exists) for this NAI, the LMA will reject this registration by sending a PBA with the error code "Administratively prohibited (129)".

If this HN Prefix is assigned in addition to an IPv4 Home address that is already assigned to the AT and if the IPv4 Home address field is included in the PBU message, then the LMA shall set the IPv4 Home address field in the PBA message to that IPv4 Home address. If this HN Prefix is assigned in addition to an IPv4 Home address that is already assigned to the AT and if the IPv4 Home address field is not included in the PBU message, then the LMA shall delete the binding for the IPv4 Home address from its Binding Cache and shall not include the IPv4 Home address field in the PBA message.

Upon accepting the PBU request for extending the lifetime of a currently active binding, the LMA shall update the lifetime for that binding and send a PBA message to the PDSN

4.3.2 IP Address/HN Prefix Release with PMIP6

Upon accepting the PBU request sent with the lifetime =0, the LMA shall delete the binding from its Binding Cache. The LMA shall send a PBA to the PDSN to acknowledge successful IP address/HN Prefix deregistration.

If the LMA determines that the MBE for the user needs to be deregistered, the LMA may send a PMIPv6 Registration Revocation Request message associated with the AT to the PDSN, as specified in [17].

4.3.3 Authentication Protocol Support

If the LMA is configured to support Authentication Protocol [22], the LMA shall follow the procedures specified in this section.

4.3.3.1 RADIUS

Upon receiving PBU with the MN-HA Mobility Message Authentication Option, the LMA shall check if the value of the PMN-LMA-SPI received in the SPI field of the PBU is associated with any active security association for the current AT session. If LMA finds the active SA for the AT with the same PMN-LMA-SPI, the LMA shall use the associated PMN-LMA key to validate the received MN-HA Mobility Message Authentication Option.

If the received PMN-LMA-SPI does not match any currently active SA for this AT, the LMA shall send RADIUS Access-Request to the HAAA, and include the User-Name attribute according to [19]. The LMA shall include the PMN-LMA-SPI value in the MN-HA SPI VSA. Upon receiving RADIUS Access-Accept, the LMA shall use the PMN-LMA key, received in the MN-HA Shared Key VSA, to validate the MN-HA Mobility Message Authentication Option in the PBU and compute the MN-HA Authentication extension for the PBA. In the MN-HA Mobility Message Authentication Option of the PBA, the LMA shall set the SPI field to the PMN-LMA SPI value received in the MN-HA SPI VSA of the RADIUS Access-Accept message. For subsequent PMIP6 re-registrations, the LMA shall use the PMN-LMA key and PMN-LMA-SPI to secure PBA and verify the PBU.

4.4 AT Requirements

The AT shall follow requirements specified in 3.4 of this document.

4.5 VAAA Requirements

During the PDSN authentication of a roaming AT, if the VAAA receives Access-Request from the PDSN with PMIP-Based-Mobility-Capability VSA included, the VAAA may perform one of the following for IPv4 services before sending the RADIUS Access-Request message to the HAAA:

- Include the PMIP-HA-Info-IPv4-Service VSA with the VAAA-Assigned-LMA-IPv4-Service Subtype, if the PMIP-HA-Info-IPv4-Service VSA was not received from the PDSN;

- Replace LMA IP address received in the VAAA-Assigned-LMA-IPv4-Service Subtype with another LMA IP address in the visited network, if the PMIP-HA-Info-IPv4-Service VSA was received from the PDSN;

- Forward the PMIP-HA-Info-IPv4-Service VSA without modifications, if received from the PDSN.

During the PDSN authentication of a roaming AT, if the VAAA receives Access-Request from the PDSN with PMIP-Based-Mobility-Capability VSA included, the VAAA may perform one of the following for IPv6 services before sending the RADIUS Access-Request message to the HAAA:

- Include the PMIP-HA-Info-IPv6-Service VSA with the VAAA-Assigned-LMA-IPv6-Service Subtype, if the PMIP-LMA-Info-IPv6-Service VSA was not received from the PDSN;

- Replace LMA IP address received in the VAAA-Assigned-LMA-IPv4-Service Subtype with another LMA IP address in the visited network, if the PMIP-HA-Info-IPv6-Service VSA was received from the PDSN;

- Forward the PMIP-HA-Info-IPv6-Service VSA without modifications, if received from the PDSN.

The VAAA shall not modify the PMIP-HA-Info-IPv4-Service VSA and/or PMIP-HA-Info-IPv6-Service VSA in the RADIUS Access-Accept message received from the HAAA.

The VAAA shall follow the requirements specified in [20].

4.6 HAAA Requirements

The HAAA shall follow the requirements specified in [20].

4.6.1 Network PMIP6 Key Management

Upon successful initial Access Authentication, for the given user the HAAA shall generate a random unique value for the PMN-LMA key and select a unique value that is greater than 255 for PMN-LMA-SPI if HAAA determines that Authentication Protocol needs to be used for this user.

4.6.2 RADIUS

During PDSN Authentication, upon receiving a RADIUS Access-Request containing the PMIP-Based-Mobility-Capability VSA, if the AT is authorized for IPv4 with PMIP6 the HAAA shall perform one of the following before sending the RADIUS Access-Accept message:

- If the RADIUS Access-Request message contains PMIP-HA-Info-IPv4-Service VSA with VAAA-Assigned-LMA-IPv4-Service Subtype, and if the HAAA authorizes the visited network to assign a local LMA, the HAAA shall include PMIP-HA-Info-IPv4-Service VSA with received VAAA-Assigned-LMA-IPv4-Service Subtype, in the RADIUS Access-Accept message. The HAAA shall not include the HAAA-Assigned-LMA-IPv4-Service Subtype in PMIP-HA-Info-IPv4-Service VSA in the RADIUS Access-Accept message.

- If the RADIUS Access-Request message contains PMIP-HA-Info-IPv4-Service VSA with VAAA-Assigned-LMA-IPv4-Service Subtype, and if the HAAA decides to assign an HA, the HAAA shall not include VAAA-Assigned-LMA-IPv4-Service Subtype in the RADIUS Access-Accept message and shall include PMIP-HA-Info-IPv4-Service VSA with the HAAA-Assigned-LMA-IPv4-Service Subtype which contains the address of an LMA assigned by the HAAA.

- If the RADIUS Access-Request message does not contain PMIP-HA-Info-IPv4-Service VSA with VAAA-Assigned-LMA-IPv4-Service Subtype, the HAAA shall include PMIP-HA-Info-IPv4-Service VSA with HAAA-Assigned-LMA-IPv4-Service Subtype.

If the AT is not authorized for IPv4 with PMIP6, the HAAA shall not includePMIP-HA-Info-IPv4-Service VSA in the RADIUS Access-Accept message.

During PDSN Authentication, upon receiving a RADIUS Access-Request containing the PMIP-Based-Mobility-Capability VSA, if the AT is authorized for IPv6 with PMIP6 the HAAA shall perform one of the following before sending the RADIUS Access-Accept message:

- If the RADIUS Access-Request message contains PMIP-HA-Info-IPv6-Service VSA with VAAA-Assigned-LMA-IPv6-Service Subtype, and if the HAAA authorizes the visited network to assign a local LMA, the HAAA shall include PMIP-HA-Info-IPv6-Service VSA with received VAAA-Assigned-LMA-IPv6-Service Subtype, in the RADIUS Access-Accept message. The HAAA shall not include the HAAA-Assigned-LMA-IPv6-Service Subtype in PMIP-HA-Info-IPv6-Service VSA in the RADIUS Access-Accept message.

- If the RADIUS Access-Request message contains PMIP-HA-Info-IPv6-Service VSA with VAAA-Assigned-LMA-IPv6-Service Subtype, and if the HAAA decides to assign an HA, the HAAA shall not include VAAA-Assigned-LMA-IPv6-Service Subtype in the RADIUS Access-Accept message and shall include PMIP-HA-Info-IPv6-Service VSA with the HAAA-Assigned-LMA-IPv6-Service Subtype which contains the address of an LMA assigned by the HAAA.

- If the RADIUS Access-Request message does not contain PMIP-HA-Info-IPv6-Service VSA with VAAA-Assigned-LMA-IPv6-Service Subtype, the HAAA shall include PMIP-HA-Info-IPv6-Service VSA with HAAA-Assigned-LMA-IPv6-Service Subtype.

If the AT is not authorized for IPv6 with PMIP6, the HAAA shall not includePMIP-HA-Info-IPv6-Service VSA in the RADIUS Access-Accept message.

Table 1 provides a list of additional RADIUS Attributes exchanged between an PDSN and AAA Server during Access Authentication and Authorization for support of Simple IP with network PMIP6.

During the initial PMIP6 registration, upon receiving a RADIUS Access-Request from an LMA, which contains the MN-HA-SPI VSA, the HAAA shall retrieve the PMN-LMA key associated with the value of PMN-LMA-SPI received in the MN-HA SPI VSA. The HAAA shall include the MN-HA Shared Key VSA (containing the PMN-LMA key) and the MN-HA

SPI VSA (containing the PMN-LMA-SPI) in the RADIUS Access-Accept sent to the LMA. The keys shall be derived as specified in Section 3.6.1.

Table 1 provides a list of RADIUS Attributes exchanged between a PDSN and AAA Server during Access Authentication and Authorization. For support of Authentication Protocol, PMIP-HA-Info-IPv4-Service VSA and PMIP-HA-Info-IPv6-Service VSA [X.S0054-910] are both appended with the following two sub-types.

Sub-Type (7)	Length	PMN-LMA key
…		PMN-LMA key
Sub-Type (8)	Length	PMN-LMA-SPI
…		PMN-LMA-SPI

Sub-Type (7): Sub-Type for the PMN-LMA key

Length: 34

the PMN-LMA key: 256 bits value of network PMIP MN-HA key.

Sub-Type (8): Sub-Type for the PMN-LMA-SPI

Length: 6

PMN-LMA-SPI: 32 bits value of network PMIP MN-HA SPI value.

One occurrence of Sub-Type (7) and Sub-Type (8) shall be present.

Table 3 provides a list of RADIUS Attributes exchanged between LMA and AAA for support of Authentication Protocol for network PMIP6.

Table 3 RADIUS Attributes exchanged between LMA and AAA for support of Authentication Protocol for network PMIP6.

Network-PMIP-NAI	26/192	1	0	HA -> AAA
PMIP-HA-Info-IPv4-Service	26/194	0-1	0-1	PDSN<->HAAA
PMIP-HA-Info-IPv6-Service	26/195	0-1	0-1	PDSN<->HAAA

5 Call Flows

5.1 Address Assignment: Simple IPv4 with PMIPv4

Figure 11 illustrates an example call flow for Simple IPv4 address assignment using IPCP.

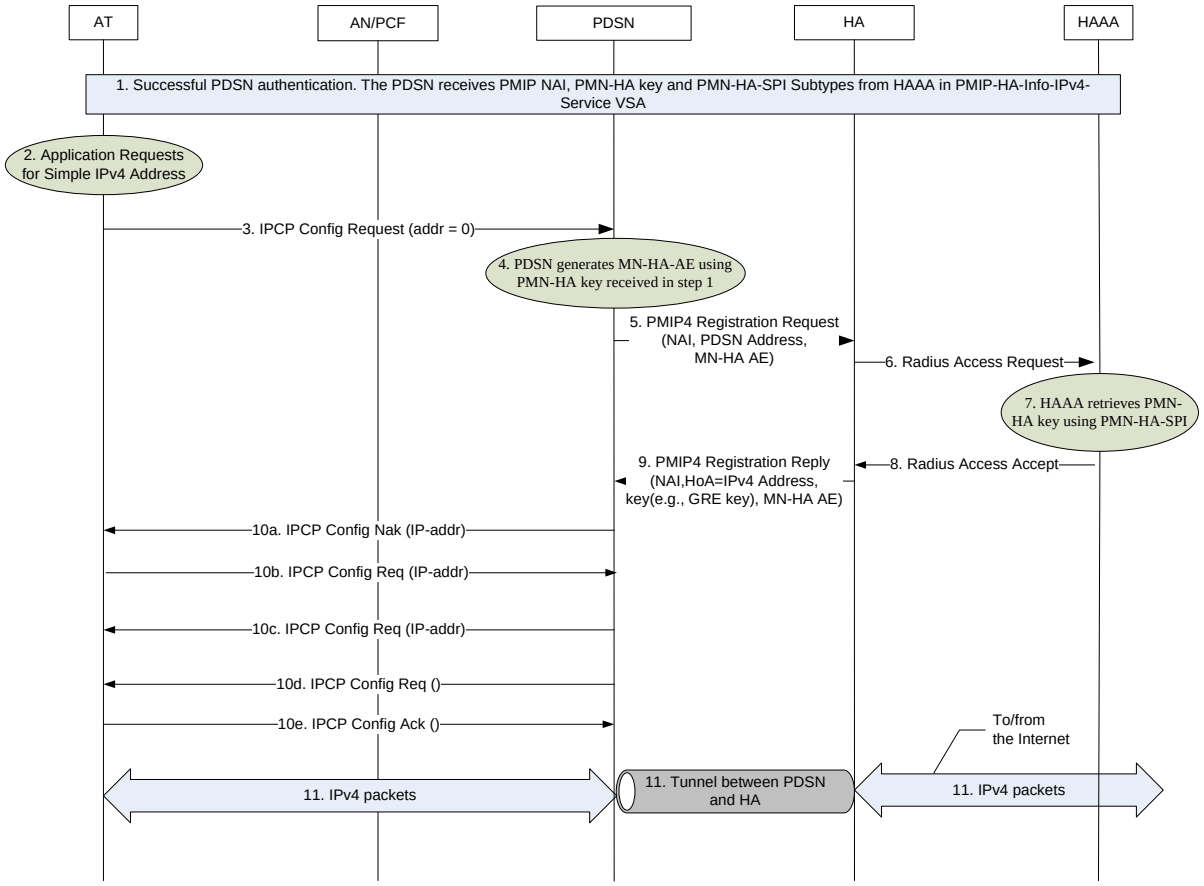

Figure 11 **Simple IPv4 Address Assignment with PMIP4**

The steps in Figure 11 are described below.

1. The AT performs a successful authentication. In this step, the Home AAA indicates the HA address of the AT to the PDSN. The PDSN receives Network-PMIP-NAI, PMN-HA key and PMN-HA-SPI from the Home AAA. Successful PDSN authentication. The PDSN receives PMIP NAI, PMN-HA key and PMN-HA-SPI Subtypes from HAAA in PMIP-HA-Info-IPv4-Service VSA

2. AT's application requests a simple IPv4 address. Step 2 may occur during step 1.

3. The AT sends IP-Config-request message to the PDSN.

4. The PDSN generates a MN-HA Authentication Extension for establishing PMIP4 tunnel between the PDSN and the HA.

5. The PDSN sends a PMIP4 Registration Request message to the HA. The Proxy MIP Registration Request message includes an NAI extension [10]. PDSN may also include the GRE Key Extension in the PRRQ message (see [4]).

6. The HA sends an Access Request to the Home AAA to verify the received PMIP RRQ.

7. The Home AAA retrieves the PMN-HA key using the PMN-HA-SPI.

8. The Home AAA sends the Access Accept to the HA. The PMN-HA key and PMN-HA SPI are included.

9. If the GRE Key extension was included in the PRRQ message, the HA selects a key (e.g., GRE key) associated with this NAI and includes it in the GRE Key extension (see [4]) in the PMIP4 Registration Reply message sent to the PDSN. The HA also includes the NAI extension and the HoA in the PMIPv4 Registration Reply message. The HA assures that the AT's IPv4 address is unique and controls the routing and filter table with full 32 bits. The SPI in MN-HA Authentication Extension is set to the PMN-HA-SPI received in step 8. The PDSN uses the PMN-HA key to verify the MN-HA Authentication Extension in the PRRP message.

10. a. The PDSN sends a IPCP-Configure-Nak message that includes an assigned IP address received in PRRP in the IP-address field to the AT.

    b. The AT sends IPCP-Configure-Req accepting the IP address proposed by the PDSN

    c. The PDSN responds with IPCP-Configure-Ack in response to IPCP-Configure-Req from the AT.

    d. The PDSN sends IPCP-Configure-Req to complete the IPCP negotiation procedure

    e. The AT sends IPCP-Configure-Ack in response to the IPCP-Configure-Ack obtained from PDSN

11. AT sends/receives IPv4 packets to/from the Internet. The tunnel between PDSN and HA can be GRE tunnel or IP-in-IP tunnel.

5.2 Address Assignment: Simple IPv6 with PMIP4

Figure 12 illustrates an example call flow for Simple IPv6 address assignment.

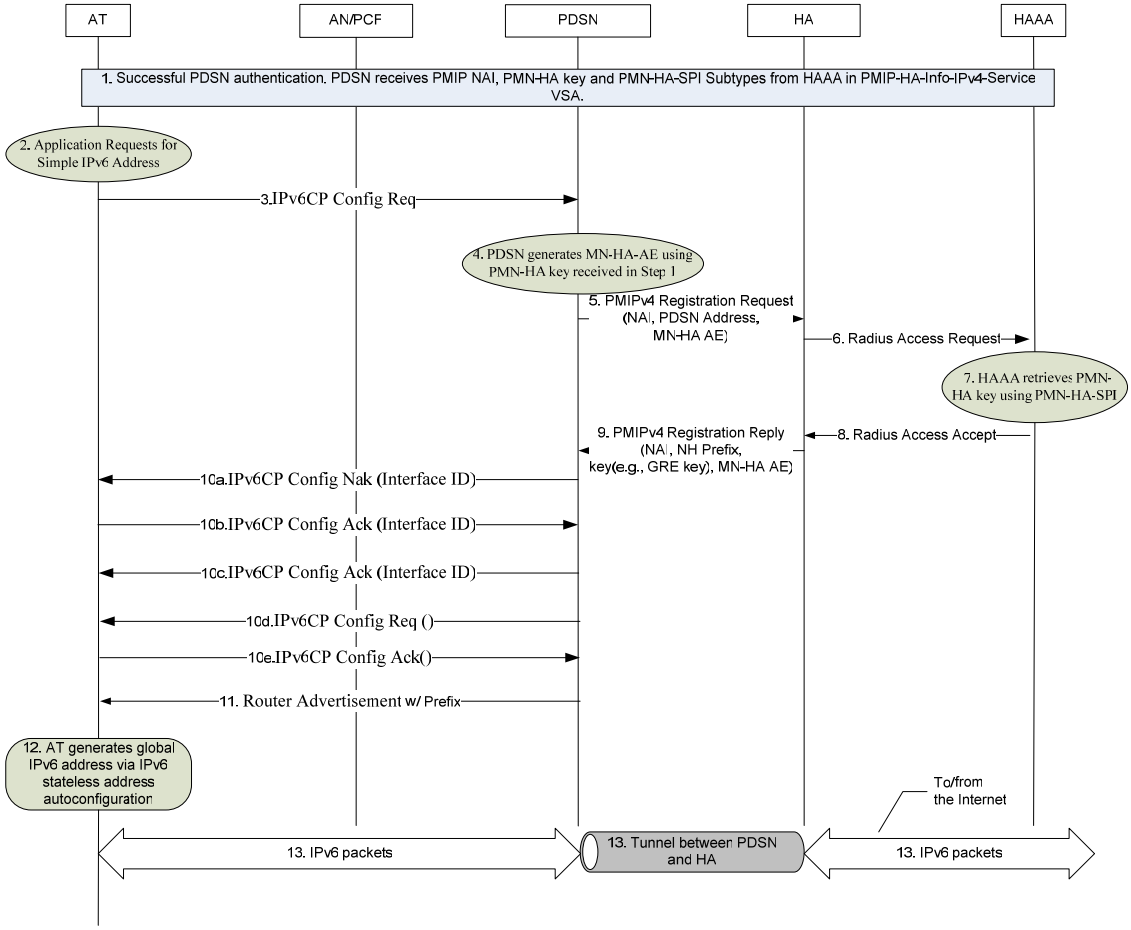

Figure 12 **Simple IPv6 Address Assignment with PMIP4**

The steps in Figure 12 are described below.

1. The AT performs a successful authentication. In this step, the Home AAA indicates the HA address of the AT to the PDSN. The PDSN receives Network-PMIP-NAI, PMN-HA key and PMN-HA-SPI from the Home AAA.

2. AT's application requests a simple IPv6 address. Step 2 may occur during step 1.

3. The AT sends a IPv6CP Configure Request message to negotiate interface identifier with the PDSN [RFC 2472]

4. The PDSN generates PMN-HA Authentication Extension for establishing PMIP4 tunnel between PDSN and HA.

5. The PDSN sends a PMIP4 Registration Request message to the HA. The PMIP4 Registration Request message includes an NAI extension [10] and Home Network Prefix. For integrity protection, the MN-HA Authentication Extension computed using the PMN-HA key is also included. PDSN may also include the GRE Key Extension in the PRRQ message (see [4]).

6. The HA sends an Access Request to the Home AAA requesting the PMN-HA key to verify the received PMIP RRQ.

7. The Home AAA retrieves the PMN-HA using the PMN-HA-SPI

8. The Home AAA sends the Access Accept to the HA. The PMN-HA key and PMN-HA-SPI are included.

9. If the GRE Key extension was included in the PRRQ message, the HA selects a key (e.g., GRE key) associated with this NAI and includes it in the GRE Key extension (see [4]) in the PMIP4 Registration Reply message sent to the PDSN. The HA also includes an NAI extension and per-AT Home Network Prefix in the PMIP4 Registration Reply message. The HA also assures that the AT's prefix is unique and controls the routing and filter table with 64 bits of the prefix. For integrity protection, the MN-HA Authentication Extension computed using the PMN-HA key is also included. The SPI in the MN-HA Authentication Extension is set to the PMN-HA-SPI received in step 8. The PDSN uses the PMN-HA key to verify the MN-HA Authentication Extension in the PRRP message.

10. a. The PDSN sends a IPv6CP Configure Nak message that includes an interface identifier to the AT.

    b. The AT sends IPv6CP-Configure-Req accepting the IP address proposed by the PDSN

    c. The PDSN responds with IPv6CP-Configure-Ack in response to IPCP-Configure-Req from the AT.

    d. The PDSN sends IPv6CP-Configure-Req to complete the IPv6CP negotiation procedure

    e. The AT sends IPCP-Configure-Ack in response to the IPv6CP-Configure-Ack obtained from PDSN

11. The PDSN sends a Router Advertisement message [13] to the AT with the source IP address set to its link local IP address and destination address set to all-routers multicast address or the AT's link local IP address [16]. The Router Advertisement message contains the AT's unique home network prefix. The prefix length can be configured based on operator's policy.

12. The AT generates an IPv6 global unicast address via IPv6 stateless address autoconfiguration [11].

13. The AT sends/receives IPv6 packets to/from the Internet. The tunnel between PDSN and HA can be GRE tunnel or IP-in-IP tunnel.

5.3 Address Assignment: Simple IPv4 with PMIPv6

Figure 13 illustrates an example call flow for Simple IPv4 address assignment while PMIP6.

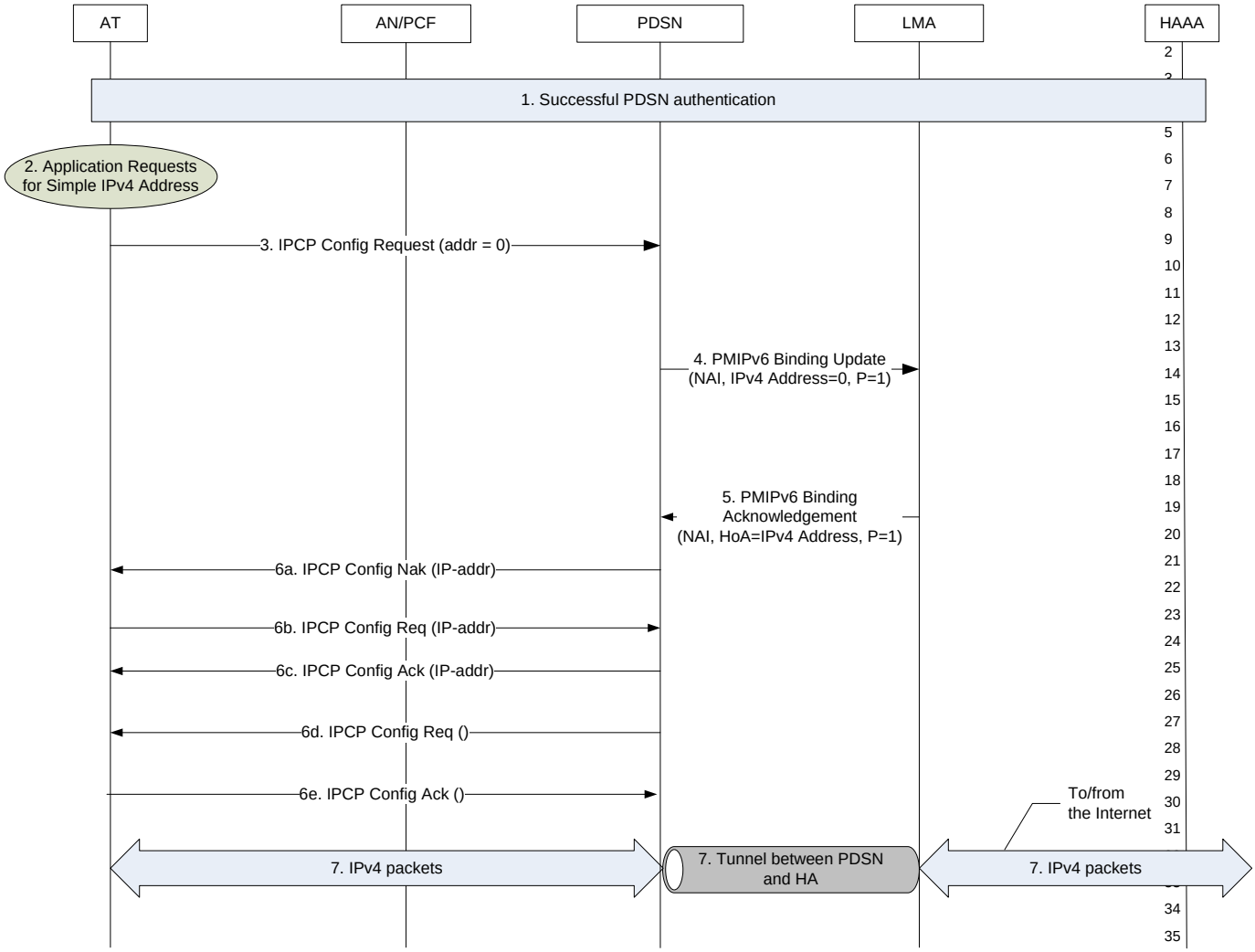

Figure 13 **Simple IPv4 Address Assignment with PMIP6**

The steps in Figure 13 are described below.

1. The AT performs a successful authentication. In this step, the Home AAA can indicate the LMA address of the AT to the PDSN.

2. AT's application requests a simple IPv4 address. Step 2 may occur during step 1.

3. The AT sends IP-Config-request message to the PDSN.

4. The PDSN sends PMIPv6 Binding Update message to the LMA. The PMIPv6 Binding Update message includes an NAI extension [13], and a Home Network Prefix extension. The HN Prefix is set to 0, indicating to the LMA that it needs to assign a per-AT HN Prefix. A flag indicating that it is a PMIPv6 Binding Update is set. After this step, the selected LMA may inform the Home AAA of the LMA address. If the LMA address is already known by the Home AAA by other means, this step can be avoided.

5. The LMA assigns a per-AT HN Prefix and sends a PMIPv6 Binding Acknowledgement message including an HN Prefix extension (see [5][) as well as NAI extension. The LMA sets a flag in PMIPv6 Binding Acknowledgement indicating that it is a PMIPv6 Binding Acknowledgement. The LMA also ensures that the AT's prefix is unique and controls the routing and filter table with 64 bits of the prefix.

6. a. The PDSN sends a IPCP-Configure-Nak message that includes an assigned IP address received in PRRP in the IP-address field to the AT

   b. The AT sends IPCP-Configure-Req accepting the IP address proposed by the PDSN

   c. The PDSN responds with IPCP-Configure-Ack in response to IPCP-Configure-Req from the AT.

   d. The PDSN sends IPCP-Configure-Req to complete the IPCP negotiation procedure

   e. The AT sends IPCP-Configure-Ack in response to the IPCP-Configure-Ack obtained from PDSN

7. AT sends/receives IPv4 packets to/from the Internet.

5.4 Address Assignment: Simple IPv6 with PMIPv6

Figure 14 illustrates an example call flow for Simple IPv6 address assignment.

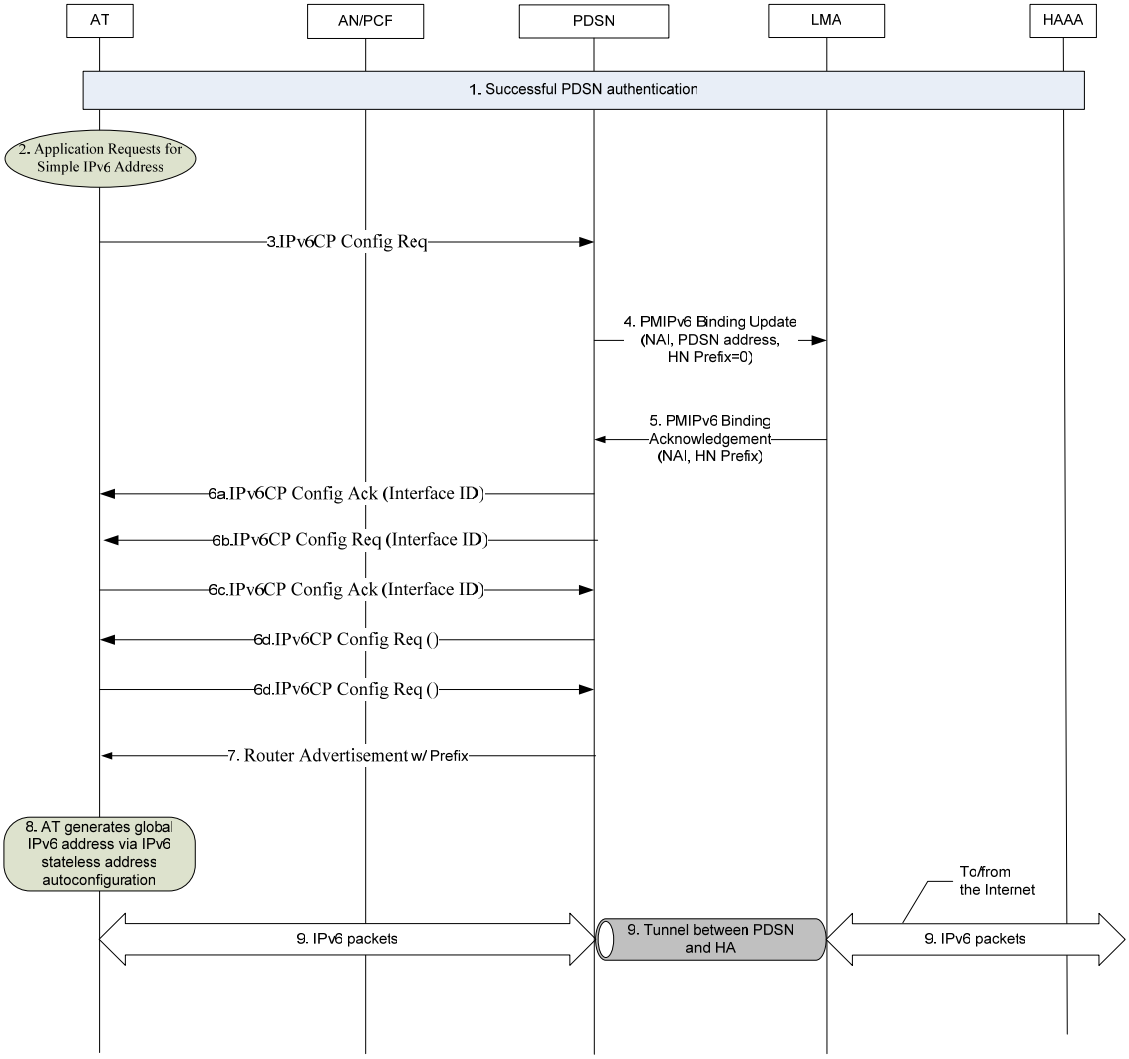

Figure 14 **Simple IPv6 Address Assignment with PMIP6**

The steps in Figure 14 are described below.

1. The AT performs a successful authentication. In this step, the Home AAA can indicate the LMA address of the AT to the PDSN.

2. AT's application requests for simple IPv6 address. Step 2 may occur during step 1.

3. The AT sends a IPv6CP Configure Request message to negotiate interface identifier with the PDSN [RFC 2472]

4. The PDSN sends PMIPv6 Binding Update message to the LMA. The PMIPv6 Binding Update message includes an NAI extension[13], and a Home Network Prefix extension. The HN Prefix is set to 0, indicating to the LMA that it needs to assign a per-AT HN Prefix. A flag indicating that it is a PMIPv6 Binding Update is set. After this step, the selected HA/LMA may inform the Home AAA of the HA/LMA address. If the HA/LMA address is already known by the Home AAA by other means, this step can be avoided.

The PDSN shall skip this step for an AT that is authorized to use only simple IP based on the profile, and go to step 7.

5. The LMA assigns a per-AT HN Prefix and sends a PMIPv6 Binding Acknowledgement message including an HN Prefix extension (see [5]) as well as NAI extension. The LMA sets a flag in PMIPv6 Binding Acknowledgement indicating that it is a PMIPv6 Binding Acknowledgement. The LMA also ensures that the AT's prefix is unique and controls the routing and filter table with 64 bits of the prefix.

6. a. The PDSN sends an IPv6 Configure Nak message that includes an interface identifier to the AT.

   b. The AT sends IPv6CP-Configure-Req accepting the IP address proposed by the PDSN

   c. The PDSN responds with IPv6CP-Configure-Ack in response to IPCP-Configure-Req from the AT.

   d. The PDSN sends IPv6CP-Configure-Req to complete the IPv6CP negotiation procedure

   e. The AT sends IPCP-Configure-Ack in response to the IPv6CP-Configure-Ack obtained from PDSN

7. The PDSN sends a Router Advertisement message to the AT with the source IP address set to its link local IP address and destination address set to all-routers multicast address or AT's link local IP address. The Router Advertisement message contains the per-AT HN prefix.

8. The AT generates an IPv6 global unicast address via IPv6 stateless address autoconfiguration[14].

9. The AT sends/receives IPv6 packets to/from the Internet through the tunnel between the PDSN and the LMA.