

3GPP2 X.S0054-220-0

Version 2.0

Date: August 29, 2008



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

Network PMIP Support

COPYRIGHT

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

This page is left blank intentionally.

Network PMIP Support

CONTENTS

1	Introduction.....	1	
2	1.1 Scope.....	1	
3	2	References.....	2
4	2.1	Normative References.....	2
5	2.2	Informative References.....	3
6	3	Simple IPv4 with PMIP Operation.....	4
7	3.1	Protocol Stack.....	4
8	3.2	AGW Requirements.....	5
9	3.2.1	Authentication and Authorization Support for PMIP Service	5
10	3.2.2	IP Address Assignment	5
11	3.2.3	IP Address Release	6
12	3.2.4	PMIP4 Tunnel Management.....	6
13	3.2.5	DHCPv4 Support.....	7
14	3.2.6	Ingress Address Filtering.....	7
15	3.3	HA Requirements	8
16	3.3.1	IP Address Assignment with PMIP4	8
17	3.3.2	IP Address Release with PMIP4.....	8
18	3.3.3	PMIP4 Tunnel Management.....	8
19	3.4	AT Requirements.....	9
20	3.5	VAAA Requirements.....	9
21	3.5.1	RADIUS	9
22	3.6	HAAA Requirements.....	9
23	3.6.1	Network PMIP4 Key Management for simple IPv4 Services	9
24	3.6.2	RADIUS	10
25	4	Simple IPv6 with PMIP Operation.....	12
26	4.1	Protocol Stack.....	12
27	4.2	AGW Requirements.....	13
28	4.2.1	Authentication and Authorization Support for PMIP Service	13
29	4.2.2	IPv6 Address Assignment.....	13
30	4.2.3	IPv6 Address Release	13
31	4.2.4	PMIP4 Tunnel Management.....	14
32	4.2.5	Stateless DHCPv6 Support.....	15
33	4.2.6	Ingress Address Filtering.....	15
34	4.3	HA Requirements	15
35	4.3.1	IP Address Assignment with PMIP4	15
36	4.3.2	IP Address Release with PMIP4.....	15
37	4.3.3	PMIP4 Tunnel Management.....	16
38	4.4	AT Requirements.....	16
39	4.5	VAAA Requirements.....	16

4.5.1	RADIUS	16	1
4.6	HAAA Requirements.....	17	2
4.6.1	Network PMIP4 Key Management for Simple IPv6 Service	17	3
4.6.2	RADIUS	17	4
			5
5	PMIP Based Inter-AGW Handoff	19	6
			7
5.1	AGW Requirements.....	20	8
5.2	HA Requirements.....	20	9
			10
5.3	eBS Behavior	21	11
5.4	SRNC Requirements	21	12
5.5	AT Requirements	21	13
			14
5.6	HAAA Requirements.....	21	15
			16
6	Call Flows	22	17
			18
6.1	Simple IPv4 with PMIP4 Addressing using DHCP Rapid Commit Option.....	22	19
6.2	Simple IPv4 with PMIPv4 Addressing using DHCP	23	20
6.3	Simple IPv6 with PMIP4 Call Flow.....	25	21
			22
6.4	PMIP Based inter-AGW Active Handoff.....	27	23
			24
			25
			26
			27
			28
			29
			30
			31
			32
			33
			34
			35
			36
			37
			38
			39
			40
			41
			42
			43
			44
			45
			46
			47
			48
			49
			50
			51
			52
			53
			54
			55
			56
			57
			58
			59
			60

LIST OF FIGURES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

<i>Figure 1</i>	Control Plane Protocol Stack for Simple IPv4 with PMIP4 Operation	4
<i>Figure 2</i>	User Plane Protocol Stack for Simple IPv4 with PMIP4 Operation	5
<i>Figure 3</i>	Control Plane Protocol Stack for Simple IPv6 with PMIP4 Operation	12
<i>Figure 4</i>	User Plane Protocol Stack for Simple IPv6 with PMIP4 Operation	12
<i>Figure 5</i>	Illustration of PMIP Based Inter-AGW Active Handoff	20
<i>Figure 6</i>	Simple IPv4 Address Assignment using DHCPv4 Rapid Commit Option.....	22
<i>Figure 7</i>	Simple IPv4 with PMIP Address Assignment using DHCP	24
<i>Figure 8</i>	Simple IPv6 Address Assignment	26
<i>Figure 9</i>	PMIP Based Inter-AGW Active Handoff	28

LIST OF TABLES

<i>Table 1</i>	Additional RADIUS Attributes exchanged between AGW and AAA during Access Authentication and Authorization for Supporting Network PMIP4 for IPv4 Services.....	11
<i>Table 2</i>	RADIUS Attributes exchanged between HA and AAA for Supporting PMIP4.....	11
<i>Table 3</i>	Additional RADIUS Attributes Exchanged between AGW and AAA during Access Authentication and Authorization for Supporting Network PMIP4 for IPv6 Services.....	18

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

REVISION HISTORY

Revision	Date	Remarks
0 v1.0	December, 2007	Initial release
0 v2.0	August, 2008	Bug fix release for the initial release

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

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 part of a multi-part document consisting of multiple parts that together describes Converged Access Network.

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.S0054-220-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 AGW and HA. This document describes PMIP based Simple IP address assignment and PMIP based inter-AGW handoff.

The solution for PMIP based inter-AGW handoff in this release involves invoking IP address assignment procedures (DHCP procedures for Simple IPv4 or Router Solicitation/Router Advertisement for Simple IPv6) every time there is an inter-AGW handoff. Other solutions that do not require invocation of IP address assignment procedures are for further study in subsequent releases of this document or other parts in this series of documents. Inter AGW handoff specified in this document should not prevent these other solutions.

1.1 Scope

This document is part of a multi-part document consisting of multiple parts that together describes Converged Access Network operation.

The scope of this document covers support for PMIP between AGW and HA, called network PMIP. It includes network PMIP based Simple IP address assignment and network PMIP based inter-AGW mobility.

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.S0084-0 v2.0, “Ultra Mobile Broadband (UMB) Air Interface”, September 2007.
- [2] 3GPP2: A.S0020-0 v1.0, “Interoperability Specification (IOS) for Ultra Mobile Broadband (UMB) Radio Access Network Interfaces”, November 2007.
- [3] 3GPP2: X.S0054-100-0 v2.0, “Basic IP Services for Converged Access Network Specification”, August 2008.
- [4] 3GPP2: X.S0054-110-0 v2.0, “MIPv4 Specification in Converged Access Network Specification”, August 2008.
- [5] 3GPP2: X.S0054-210-0 v1.0, “CMIP based Inter-AGW Handoff”, December 2007.
- [6] 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.

- [7] 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.

- [8] IETF: draft-ietf-mip4-dsmipv4

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.

- [9] IETF: RFC 2131, Dromi, “Dynamic Host Configuration Protocol”, March 1997.
- [10] IETF: RFC3046, Patrik, “DHCP Relay Agent Information Option”, January 2001.
- [11] IETF: RFC4039, Park, et.al., “Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)”, March 2005.
- [12] IETF: RFC3543, Glass, et.al., “Registration Revocation in Mobile IPv4”, August 2003.
- [13] IETF: RFC 3775, D. Johnson, et.al., “Mobility Support in IPv6”, June 2004.
- [14] IETF: RFC2794, Calhoun, et.al., “Mobile IP Network Access Identifier Extension for IPv4”, March 2000.

- 1 [15] IETF: RFC4862, Thomson, et. al., “IPv6 Stateless Address
2 Autoconfiguration”, September 2007.
- 3 [16] IETF: RFC3041, Narten, et.al., “Privacy Extensions for Stateless Address
4 Autoconfiguration in IPv6”, January 2001.
- 5 [17] IETF: RFC4861, Narten, et.al., “Neighbor Discovery for IP Version 6
6 (IPv6)”, September 2007.
- 7 [18] IETF: RFC3012, Parkins, et.al., “Mobile IPv4 Challenge/Response
8 Extensions”, November 2000.
- 9 [19] 3GPP2: X.S0011-002-D, “cdma2000 Wireless IP Network Standard:
10 Simple IP and Mobile IP Access Service”, March 2006.
- 11 [20] 3GPP2: X.S0054-400-0 v1.0, “Converged Access Network Accounting
12 Specification”, December 2007.
- 13 [21] 3GPP2: X.S0054-910-0 v2.0, “CAN Data Dictionary”, August 2008.
- 14 [22] IETF: RFC4861, Narten, et.al., “Neighbor Discovery for IP Version 6
15 (IPv6)”, September 2007.
- 16
17
18
19
20
21
22

2.2 Informative References

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

- 25 <1> 3GPP2: X.S0054-000-0 v2.0, “CAN Wireless IP Network Overview and
26 List of Parts”, August 2008.
- 27 <2> 3GPP2: X.S0054-102-0 v2.0, “Multiple-Authentication and Legacy
28 Authentication Support for CAN”, August 2008.
- 29 <3> 3GPP2: X.S0054-300-0 v1.0, “QoS Support for Converged Access Network
30 Specification”, December 2007.
- 31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

3 Simple IPv4 with PMIP Operation

This section specifies the requirements for Simple IPv4 with PMIP Operation

3.1 Protocol Stack

Figure 1 shows the protocol reference model for Simple IPv4 with PMIP4 signaling data between the AGW and the HA. Figure 2 shows the protocol reference model for Simple IPv4 with PMIP4 user data between the AT and CN.

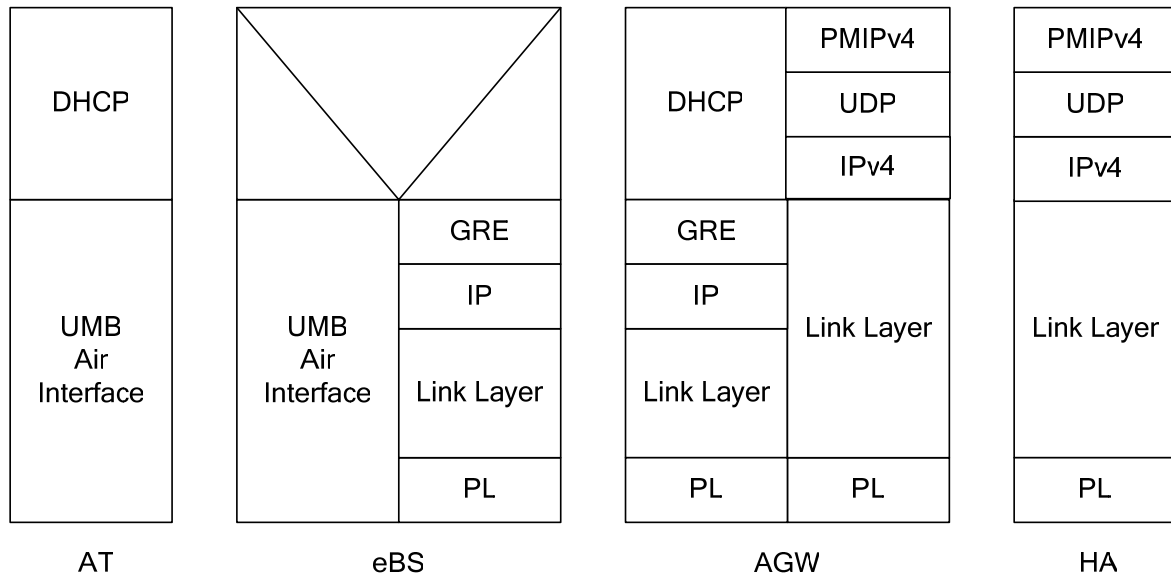


Figure 1 Control Plane Protocol Stack for Simple IPv4 with PMIP4 Operation

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

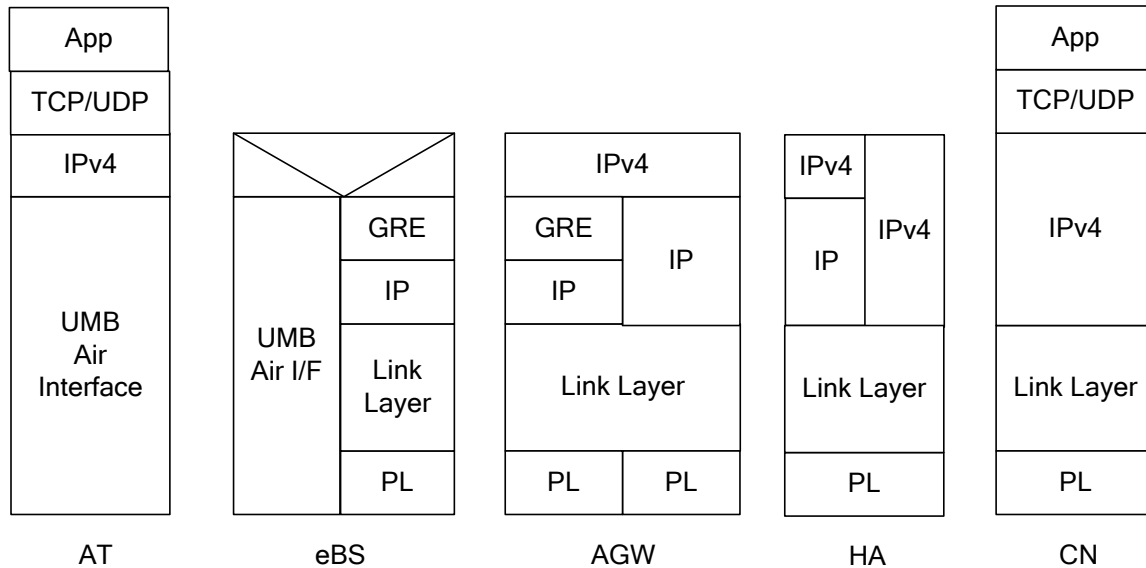


Figure 2 User Plane Protocol Stack for Simple IPv4 with PMIP4 Operation

3.2 AGW Requirements

The AGW may support PMIP4 operation as specified in this section. If the AGW operates in network PMIPv4, the AGW shall identify packets received from the eBS belonging to a Level 2 IP interface (encapsulated in odd GRE keys) and apply PMIP4 operations on them. On forward link, the AGW shall process PMIP4 packets received from the HA and encapsulate them in appropriate odd GRE keys corresponding to the AT's Level 2 IP interface.

3.2.1 Authentication and Authorization Support for PMIP Service

An AGW supporting PMIP4 based mobility shall include in the Access-Request message sent to the HAAA during the EAP access authentication and authorization procedures for an AT [3] 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 AGW may allocate an HA in the visited network and include the VAAA-Assigned-HA-IPv4-Service Subtype in PMIP-HA-Info-IPv4-Service VSA in the RADIUS Access-Request message sent to the HAAA during EAP access authentication and authorization. See [21] for the definition of the RADIUS VSAs used for this purpose.

3.2.2 IP Address Assignment

Upon receiving a DHCP message from the AT requesting IP address assignment, if the AT is authorized for PMIP based mobility, and if the DHCP message is associated with a Level 2 IP interface, i.e., it is encapsulated with GRE key associated with Level 2 IP interface, an AGW supporting PMIP based mobility shall trigger PMIP procedures to acquire an IPv4 address and hold the DHCP message until PMIPv4 signaling completes. The AGW shall follow procedures defined in Section 3.2.4 for network PMIP tunnel establishment. If the AT is not authorized for PMIP based mobility, the AGW shall follow the procedures for Simple IPv4 operation as specified in [3].

If the AGW receives a PMIP RRP indicating that the registration is successful (see Section 3.2.4), the AGW shall set the 'yiaddr' field to the HoA received in the PRRP, Server IP address field to the IP address of the AGW and the IP Address Lease Time field to a value not

larger than the value of the PMIP Registration Lifetime. The AGW shall follow the rest of procedures as specified in [3].

If the AGW receives a PRRP indicating that the registration is successful, and the same IP address has been assigned to the AT for a different IP session, the AGW shall follow the procedures specified in [3]. In addition the AGW shall deregister the IPv4 address with the HA as specified in 3.2.4.

If the AGW receives an indication that the registration was unsuccessful, the AGW shall follow the procedures as defined in [3] for Simple IPv4 operation.

For subsequent DHCPREQUEST with the assigned IPv4 address (e.g., to extend the lease on the AT's IP address), the AGW shall verify that the IP address in the 'ciaddr' field in the DHCPREQUEST is identical to the IP address that is associated with the RAN PMIP tunnel through which the AGW received the DHCPREQUEST message. If this is the case, and if the IP Address Lease Time extends beyond the PMIP Registration Lifetime, the AGW shall send PRRQ to the HA to extend the PMIP Registration Lifetime as specified in Section 3.2.4 and follow the rest of procedures as specified in [3]. If the IP addresses do not match, the AGW shall silently discard the DHCPREQUEST message.

3.2.3 IP Address Release

If the AGW receives a DHCPRELEASE message from the AT before the IP address lease time expires, the AGW shall verify that the IP address in the 'ciaddr' field in the DHCPRELEASE is identical to the IP address that is associated with the Level 2 GRE key in the tunnel through which the AGW received the DHCPRELEASE message. If the IP addresses are the same, the AGW shall trigger the PMIP procedures to deregister the IPv4 address with the HA. If the IP addresses do not match, the AGW shall silently discard the DHCPRELEASE message.

If the AGW receives a RADIUS Disconnect-Request message from the HAAA, the AGW shall follow procedures defined in [3]. In addition, the AGW shall trigger the PMIP4 procedures to deregister the IPv4 address with the HA as specified in Section 3.2.4.

3.2.4 PMIP4 Tunnel Management

The AGW supporting mobility for Simple IPv4 ATs with PMIP4 shall act as a Proxy Mobility Agent (PMA) as specified in [6] and [12].

Upon receiving a DHCP message requesting IP address assignment (e.g., DHCPDISCOVER), encapsulated with the GRE key associated with Level 2 IP interface, the AGW shall send a Proxy Registration Request (PRRQ) to the HA as specified in [6]. The AGW shall know the following information to be able to send the PRRQ:

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

This information is obtained during access authentication and authorization [3]. If the AGW requests an IPv4 address from the HA, the AGW shall set the Home Address (HoA) field in the PRRQ to 0.0.0.0. If the AGW knows the AT's IPv4 address (e.g., the IP address specified as a hint in the 'requested IP address' option of the DHCP message), it shall set the IPv4

1 Home Address field to the known IPv4 home address. Optionally, the AGW may send the
2 GRE key extension in the PRRQ message, with the value set as defined in [7].

3
4 To establish and preserve the AGW-HA security, the AGW receives the PMN-HA key and
5 associated PMN-HA-SPI from the Home AAA during Access Authentication.

6
7 For securing the PRRQ, the AGW shall compute the MN-HA Authentication Extension using
8 the PMN-HA key. The SPI field in MN-HA Authentication Extension is set to PMN-HA-SPI.

9
10 Upon receiving the PRRP, the AGW shall verify that the PMN-HA-SPI received in the MN-
11 HA Authentication Extension of the PRRP is associated with the stored value of PMN-HA
12 key. If verification is successful, the AGW shall use the PMN-HA key to validate the MN-HA
13 Authentication Extension in the PRRP. Successfully authenticated PRRP shall indicate that
14 the AGW has established an SA to the HA.

15
16 If the AGW wants to indicate its support for registration revocation to the HA, the AGW shall
17 include Mobile IP Revocation Support extension in the PRRQ sent to the HA. If the AGW
18 receives a PRRP that does not include Mobile IP Revocation Support extension, the AGW
19 shall assume that HA does not support registration revocation.

20
21 Upon successful registration (e.g., reply code in PRRP is set to 0) the AGW shall follow the
22 IP address assignment procedures as specified in section 3.2.2. However, before responding to
23 the AT, the AGW may perform another DHCP request (encapsulated in PMIP tunnel) with
24 the Level 2 DHCP server to learn DHCP configuration information. The AGW shall set the
25 configuration parameters in the DHCP response to the AT based on the DHCP response it
26 receives from the server. The AGW shall wait for this DHCP exchange to complete before
27 responding to the AT.

28
29 If the AGW determines that the IPv4 address needs to be deregistered, the AGW shall send a
30 PRRQ with lifetime = 0 to the HA.

31
32 If the AGW determines that the PMIP Registration Lifetime needs to be extended, the AGW
33 shall follow the procedure defined in [6] to renew the PMIP Registration Lifetime with the
34 HA.

35
36 If the AGW receives the PMIP Registration Revocation message from the HA, and if the
37 AGW negotiated registration revocation support with the HA as specified above, the AGW
38 shall validate the message. Upon successful validation, the AGW shall clean up the resources
39 associated with the AT's IP address that is being revoked and send a PMIP Registration
40 Revocation Acknowledgment message to the HA as specified in [6] and [12].

41 42 43 44 **3.2.5 DHCPv4 Support**

45 The AGW shall support DHCP Server functionality as defined in [9] and [11].

46 47 48 **3.2.6 Ingress Address Filtering**

49 The AGW shall check the source IP address of every packet received on per AT tunnels
50 between the eBS and AGW. Upon receiving packets from an AT with an invalid source IP
51 address, except for DHCP packets with the IP address set to all 0s, the AGW shall silently
52 discard the packets.

3.3 HA Requirements

The HA supporting PMIP4 shall follow Mobile IPv4 procedures as specified in [6] and [12].

3.3.1 IP Address Assignment with PMIP4

If validation of the PRRQ is successful (for details refer to Section 3.3.3), 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, 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 3.3.3.

If the GRE extension was included in the PRRQ, the HA shall process it in accordance with [7] 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 AGW. Upon receiving a PRRQ that does not include Mobile IP Revocation Support extension, the HA shall assume that the AGW does not support registration revocation.

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 AGW.

3.3.2 IP Address Release with PMIP4

When the HA receives a PRRQ with lifetime = 0 from the AGW 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 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 AGW during PMIP registration, the HA shall send a PMIP Registration Revocation message associated with the AT to the AGW, as specified in [6] and [12]. Upon receiving Registration Revocation Acknowledgment message from the AGW, 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.

1 If the received PMN-HA-SPI does not match any currently active SA for this AT, the HA
 2 shall send RADIUS Access-Request to the HAAA, and include the User-Name attribute
 3 according to [19]. The HA shall include the PMN-HA-SPI value in the MN-HA SPI VSA.
 4 Upon receiving RADIUS Access-Accept, the HA shall use the PMN-HA key, received in the
 5 MN-HA Shared Key VSA, to validate the MN-HA Authentication Extension in the PRRQ
 6 and compute the MN-HA Authentication extension for the PRRP. In the MN-HA
 7 Authentication Extension of the PRRP, the HA shall set the SPI field to the PMN-HA SPI
 8 value received in the MN-HA SPI VSA of the RADIUS Access-Accept. For subsequent
 9 PMIP4 re-registrations, the HA shall use the PMN-HA key and PMN-HA-SPI to secure
 10 PRRP and verify the PRRQ.
 11

12 3.4 AT Requirements

13 AT requirements are specified in [3]. For simple IPv4 associated with Level 2 IP interface, the
 14 AT shall perform all its simple IPv4 operations on that IP interface.
 15

16 3.5 VAAA Requirements

17 3.5.1 RADIUS

18 During the EAP access authentication of a roaming AT, if the VAAA receives Access-
 19 Request from the AGW with PMIP-Based-Mobility-Capability VSA included, the VAAA
 20 may perform one of the following before sending the RADIUS Access-Request message to
 21 the HAAA:
 22

- 23 • Include the PMIP-HA-Info-IPv4-Service VSA with the VAAA-Assigned-HA-IPv4-
 24 Service Subtype, if the PMIP-HA-Info-IPv4-Service VSA was not received from the
 25 AGW;
- 26 • Replace HA IP address received in the VAAA-Assigned-HA-IPv4-Service Subtype
 27 with another HA IP address in the visited network, if the PMIP-HA-Info-IPv4-
 28 Service VSA was received from the AGW;
- 29 • Forward the PMIP-HA-Info-IPv4-Service VSA without modifications, if received
 30 from the AGW.
 31

32 The VAAA shall not modify the PMIP-HA-Info-IPv4-Service VSA and/or PMIP-HA-Info-
 33 IPv6-Service VSA (see Section 4) in the RADIUS Access-Accept message received from the
 34 HAAA.
 35

36 3.6 HAAA Requirements

37 3.6.1 Network PMIP4 Key Management for simple IPv4 Services

38 Upon successful initial Access Authentication, the HAAA shall generate the random unique
 39 value for the PMN-HA key and PMN-HA-SPI for the user. The HAAA may derive the PMN-
 40 HA key and PMN-HA-SPI from the EMSK as follows.
 41

42 The HAAA generates the PMN-HA-RK key from the EMSK:
 43

PMN-HA-RK key = HMAC-SHA-256 (EMSK, “IPv4-Service-PMN-HA-RK key@3gpp2.org”)

From the PMN-HA-RK, the PMN-HA key and its associated PMN-HA-SPI shall be derived as follows:

PMN-HA key = HMAC-SHA-256 (PMN-HA-RK, “PMN-HA key@3gpp2.org”, AGW IP address | HA IP address)

PMN-HA-SPI = HMAC-SHA-256 (PMN-HA-RK, “3GPP2-PMN-HA-SPI@3gpp2.org”),

where the HA IP address is the IP address included by the HAAA in either the VAAA-Assigned-HA-IPv4-Service Subtype or the HAAA-Assigned-HA-IPv4-Service Subtype of the PMIP-HA-Info-IPv4-Service VSA, depending whether assignment of the HA in the visited network or the home network is authorized by the HAAA.

The PMN-HA-SPI indicates the specific security association between AGW and HAAA and algorithm used in computation of the MN-HA Authentication Extension. If the value of this computed PMN-HA-SPI is equal to or smaller than 255, then an integer value of 256 shall be added to the computed value. If the PMN-HA-SPI collides with another SPI value already allocated for the AT, then the SPI value shall be monotonically incremented until the SPI value has no collision for that AT.

3.6.2 RADIUS

During EAP Access 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 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 1 provides a list of additional RADIUS Attributes exchanged between an AGW and AAA Server during Access Authentication and Authorization for support of Simple IPv4 with network PMIP4.

Table 1 Additional RADIUS Attributes exchanged between AGW and AAA during Access Authentication and Authorization for Supporting Network PMIP4 for IPv4 Services

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

4.1 Protocol Stack

Figure 3 shows the protocol reference model for Simple IPv6 with PMIPv4 signaling data between the AGW and the HA. Figure 4 shows the protocol reference model for Simple IPv6 with PMIPv4 user data between the AT and CN.

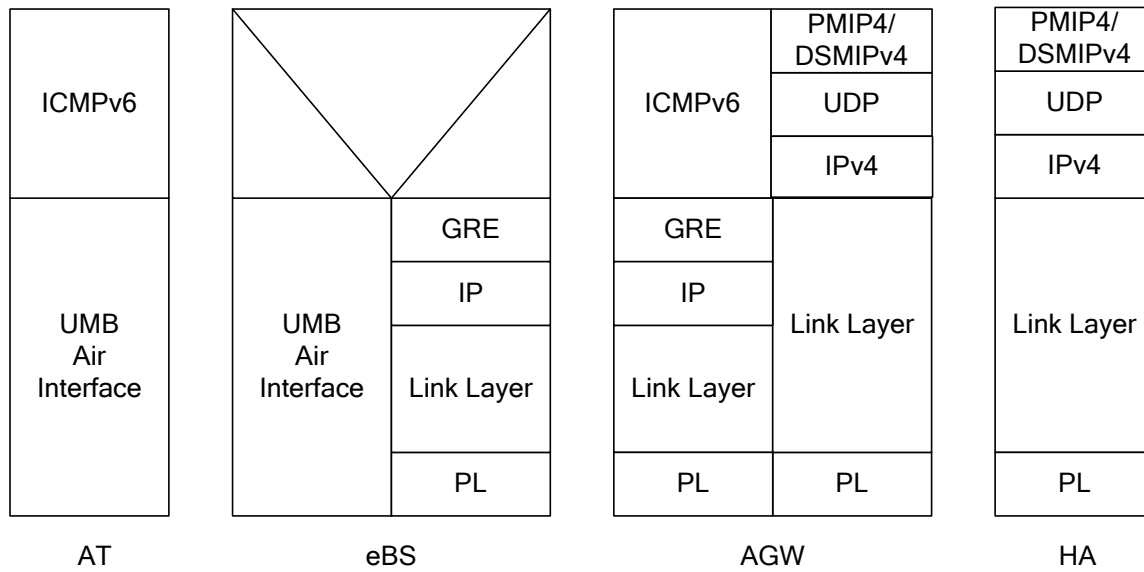


Figure 3 Control Plane Protocol Stack for Simple IPv6 with PMIPv4 Operation

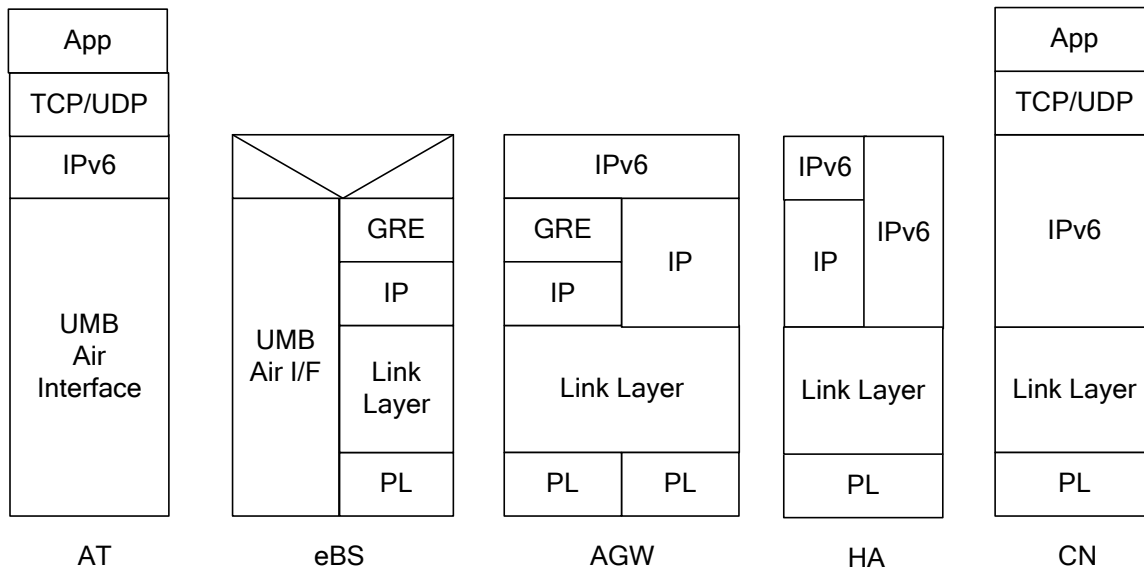


Figure 4 User Plane Protocol Stack for Simple IPv6 with PMIPv4 Operation

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

4.2 AGW Requirements

4.2.1 Authentication and Authorization Support for PMIP Service

An AGW supporting PMIP4 based mobility shall include in the Access-Request message sent to the HAAA during the EAP access authentication and authorization procedures for an AT [3] 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 AGW may allocate an HA from the visited network and include the VAAA-Assigned-HA-IPv6-Service Subtype in PMIP-HA-Info-IPv6-Service VSA in the in the RADIUS Access-Request message sent to the HAAA during for EAP access authentication and authorization. See [21] for the definition of the RADIUS VSAs used for this purpose.

4.2.2 IPv6 Address Assignment

The AGW shall act as an IPv6 default router as defined in [3].

If the AGW receives a Router Solicitation message from the AT, and if the AT is authorized for PMIP based mobility, an AGW supporting PMIP based mobility shall trigger PMIP procedures to acquire an IPv6 address and hold the Router Solicitation message until PMIPv4 signaling completes. The AGW shall follow procedures defined in Section 4.2.4 for network PMIP tunnel establishment. If the AT is not authorized for PMIP based mobility, the AGW shall follow the procedures for Simple IPv6 operation as specified in [3].

If the AGW receives a PMIP RRP indicating that the registration with the HA was successful, the AGW shall extract the HN-Prefix that is assigned to the AT in the PRRP and respond back to the AT with the IPv6 Router Advertisement message 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 PMIP Registration Lifetime. The AGW shall follow the rest of the procedures as specified in [3]. Otherwise, if the AGW receives PMIP RRP indicating that the registration failed, the AGW shall follow the procedures as defined in [3] for Simple IPv6 operation.

If the AGW receives a PRRP indicating that the registration is successful, and the same IP address has been assigned to the AT for a different IP session, the AGW shall follow the procedures specified in [3]. In addition the AGW shall deregister the IPv6 address with the HA as specified in Section 4.2.4.

If the AGW receives the Router Solicitation message before the Prefix Valid Life time expires, the AGW shall follow the procedures defined in Section 4.2.4 and [3].

4.2.3 IPv6 Address Release

If the Prefix Valid Lifetime expires, the AGW shall release the assigned IPv6 Prefix for the AT and deregister the network PMIP tunnel with the HA.

If the AGW receives a RADIUS Disconnect-Request message the AGW shall follow procedures defined in [3]. Additionally, the AGW shall trigger the PMIP4 procedures to deregister the IPv6 Prefix with the HA as specified in Section 4.2.4.

4.2.4 PMIP4 Tunnel Management

The AGW supporting mobility for Simple IPv6 mobiles with PMIP4 shall act as a Proxy Mobility Agent (PMA) as specified in [6], [8] and [12].

Upon receiving a Router Solicitation message the AGW shall send a Proxy Registration Request (PRRQ) to the HA. The AGW shall know the following information to be able to send a PRRQ:

- the user's Network PMIP NAI,
- Mobility Security Information
- and the HA address.

This information is obtained during access authentication and authorization [3]. If the AGW requests an IPv6 Prefix allocation from the HA, it shall set the IPv6 Prefix Extension in the PRRQ to 0::/0. If the AGW knows the IPv6 Prefix, it shall set the IPv6 Prefix Extension to the known IPv6 Prefix. The AGW may send the GRE key extension in the PRRQ message, with the value set as defined in [7].

To establish and preserve the AGW-HA security, the AGW receives the PMN-HA key and associated PMN-HA-SPI from the Home AAA during Access Authentication and Authorization.

For securing the PRRQ, the AGW shall compute the MN-HA Authentication Extension using the PMN-HA key. The SPI field in MN-HA Authentication Extension is set to PMN-HA-SPI.

Upon receiving the PRRP, the AGW 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 AGW shall use the PMN-HA key to validate the MN-HA Authentication Extension in the PRRP. Successfully authenticated PRRP shall indicate that the AGW has established an SA to the HA.

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

If authentication is successful, the AGW shall inspect the PRRP for error codes. If registration is successful (e.g., reply code is set to 0), the AGW shall follow the procedures as specified in Section 4.2.2. If the AGW determines that the IPv6 address needs to be deregistered, the AGW shall send a PRRQ to the HA with lifetime = 0.

If the AGW determines that the PMIP Registration Lifetime needs to be extended, the AGW shall follow the procedure defined in [6] to renew the PMIP Registration Lifetime with the HA.

If the AGW receives the PMIP Registration Revocation message from the HA and if the AGW negotiated registration revocation support with the HA as specified above, the AGW shall validate the message. Upon successful validation, the AGW 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 [6] and [12].

4.2.5 Stateless DHCPv6 Support

The AGW shall act either as a DHCPv6 Relay Agent or a Stateless DHCPv6 server. For details refer to [3].

4.2.6 Ingress Address Filtering

The AGW checks the prefix of the source IP address of every packet received on the per AT tunnels between the eBS and AGW. Details can be found in [3].

4.3 HA Requirements

4.3.1 IP Address Assignment with PMIP4

The HA supporting PMIP4 shall follow the Mobile IP procedures as specified in [6] and [8].

If validation of the PRRQ is successful (for details refer to Section 4.3.3), 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 [8] 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 [8]. If the PRRQ contains a non-zero IPv6 Prefix that is not supported by this HA, 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 4.3.3.

If the GRE extension was included in the PRRQ, the HA shall process it in accordance with [7] 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 AGW. Upon receiving a PRRQ that does not include Mobile IP Revocation Support extension, the HA shall assume that the AGW does not support registration revocation.

Upon accepting the 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 AGW.

4.3.2 IP Address Release with PMIP4

When the HA receives a PRRQ with lifetime = 0, the HA shall validate the authentication extension. If the validation is successful, the HA shall remove the MBE for that user. The HA shall respond back with a PRRP with lifetime=0 to confirm the successful 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 AGW during PMIP registration, the HA shall send a PMIP Registration Revocation message associated with the AT to the AGW, as specified in [6] and [12]. Upon receiving Registration Revocation Acknowledgment message from the AGW, the HA shall delete the AT’s MBE.

4.3.3 PMIP4 Tunnel Management

4.3.3.1 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 any. 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 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 a RADIUS Access-Request to the H-AAA, which includes the User-Name attribute according to [19]. 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-registration, the HA shall use the PMN-HA key and PMN-HA-SPI to secure PRRP and verify the PRRQ.

4.4 AT Requirements

AT requirements are specified in [3]. For simple IPv6 associated with Level 2 IP interface, the AT shall perform all its simple IPv6 operations on that IP interface.

4.5 VAAA Requirements

4.5.1 RADIUS

During the EAP access authentication of a roaming AT, if the VAAA receives Access request from the AGW with PMIP-Based-Mobility-Capability VSA included, the VAAA may perform one of the following 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 is not received from the AGW;
- 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 AGW;
- Forward the PMIP-HA-Info-IPv6-Service VSA without modifications, if received from the AGW.

The VAAA shall not modify the PMIP-HA-Info-IPv4-Service (see section 3) and/or PMIP-HA-Info-IPv6-Service VSA in the RADIUS Access-Accept message received from the HAAA.

4.6 HAAA Requirements

4.6.1 Network PMIP4 Key Management for Simple IPv6 Service

Upon successful initial Access Authentication, the HAAA shall generate the random unique value for the PMN-HA key and PMN-HA-SPI for the user. The HAAA may derive the PMN-HA key and PLM-HA-SPI from the EMSK as follows.

First, the HAAA generates the PMN-HA-RK key from the EMSK

PMN-HA-RK key = HMAC-SHA-256 (EMSK, “IPv6-Service-PMN-HA-RK@3gpp2.org”)

From the PMN-HA-RK, the PMN-HA key and its associated PMN-HA-SPI shall be derived as follows:

PMN-HA key = HMAC-SHA-256 (PMN-HA-RK, “PMN-HA key@3gpp2.org”, AGW IP address | HA IP address)

PMN-LM -SPI = HMAC-SHA-256 (PMN-HA-RK, “3GPP2-PMN-HA-SPI@3gpp2.org”),

where the HA IP address is the IP address included by the HAAA in either the VAAA-Assigned-HA-IPv6-Service Subtype or the HAAA-Assigned-HA-IPv6-Service Subtype of the PMIP-HA-Info-IPv6-Service VSA, depending whether assignment of the HA in the visited network or the home network is authorized by the HAAA.

The PMN-HA-SPI indicates the specific security association between the AGW and the HA and algorithm used in computation of the MN-HA Authentication Extension. If the value of this computed PMN-HA-SPI is equal to or smaller than 255, then an integer value of 256 shall be added to the computed value. If the PMN-HA-SPI collides with another SPI value already allocated for the AT, then the SPI value shall be monotonically incremented until the SPI value has no collision for that AT.

4.6.2 RADIUS

During the EAP Access Authentication, upon receiving 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 the received VAAA-Assigned-HA-IPv6-Service VSA Subtype as well as associated PMN-HA key Subtype and PMN-HA-SPI Subtype in the RADIUS Access-Accept message and shall not include the HAAA-Assigned-HA-IPv6-Service Subtype in the 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, 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 the PMIP-HA-Info-IPv6-Service VSA with 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 PMIP4, the HAAA shall not include PMIP-HA-Info-IPv6-Service VSA in the RADIUS Access-Accept message.

During the initial PMIP4 registration, upon receiving 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 detail of key derivation is defined in Section 4.6.1.

Table 3 provides a list of additional RADIUS Attributes exchanged between an AGW and AAA Server during Access Authentication and Authorization for support of Simple IPv6 with network PMIP4. A list of RADIUS Attributes exchanged between HA and AAA for support of network PMIP4 is provided in Table 2.

Table 3 Additional RADIUS Attributes Exchanged between AGW and AAA during Access Authentication and Authorization for Supporting Network PMIP4 for IPv6 Services

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

¹ This attribute is only included once in the RADIUS Access-Request message if both PMIP4 for IPv4 Service and PMIP4 for IPv6 Service capabilities are supported.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

5 PMIP Based Inter-AGW Handoff

In some cases, inter-AGW handoff occurs when the AT is in an active session and a newly added eBS needs to connect with a different AGW from the original AGW. Document [5] addresses this scenario based on CMIP procedures (e.g., AT is CMIPv4). This document addresses the scenario in which mobility is provided utilizing PMIP between an AGW and an HA.

In this scenario, a different LinkID (which represents the new AGW) belonging to the same level is presented to the AT when the new eBS that is connected to a new AGW is added in the Route Set and after EAP Access Authentication and Authorization is performed successfully. Once a RAN Primary PMIP tunnel is established between the new eBS and new AGW (target AGW) the AT presents the new IP interface to upper layers. Details can be found in [2].

A different LinkID at the same level also triggers IP address assignment procedures. In particular, a DHCP (alternatively Router Solicitation) message is sent from the AT to the new AGW through the newly established RAN PMIP tunnel. Subsequently, a PMIP tunnel is established between the new AGW and HA. The HA assigns the same IPv4 address (alternatively IPv6 prefix) to the AT.

The primary RAN PMIP tunnel from the previous DAP to the previous AGW is kept alive until the primary PMIP lifetime expires or the Source AGW receives PMIP RRQ with lifetime set to 0. The reverse link only bindings (if any) to the previous AGW are also kept alive until one of the following occurs:

- The individual reverse link PMIP binding lifetimes expire,
- Source AGW receives PMIP RRQ with lifetime set to 0, or
- The primary RAN PMIP Tunnel is released.

Figure 5 shows an example of inter-AGW active handoff based on PMIP. In the figure, eBS0 and eBS1 are connected to AGW1 and associated with LinkID1, and eBS2 and eBS3 are connected to AGW2 and associated with LinkID2. PMIPv4 is used for inter AGW handoff. The AT has been in communication with eBS1 connected to AGW1. The AT has just added eBS2 to the Route Set. Due to radio conditions, the Forward Link Serving eBS (FLSE)/Reverse Link Serving eBS (RLSE) is switched to eBS2.

On the forward-link, before PMIP re-registration is performed, the HA sends data to the Source AGW. The Source AGW sends packets to eBS1 which is the DAP for the Source AGW (AGW1). When the eBS1 receives a packet for the AT from AGW1 (and the FLSE is eBS2 under AGW2), it uses its route (Route 1) to send the packet to the eBS2 via Link-Layer tunneling protocol. Once the packet is transmitted from eBS2 to the AT, the AT processes the IP packet on the IP interface associated with Route 1 (IP interface 1 in Figure 5). After network PMIP re-registration is performed, the HA starts sending data to AGW2 (the target AGW), which forwards packets to eBS2 (DAP under AGW2). When the eBS2 receives an IP packet for the AT from AGW2 (and the FLSE is eBS2), the eBS2 uses its route (Route 2) to send the IP packet to the AT. Upon receipt of the packet, the AT uses the associated IP interface with Route 2 (i.e., IP interface 2) to process the packet.

On the reverse link, when the application in the AT generates data, the data is sent to the IP interface 1 associated with the LinkID 1 (which is associated with AGW1, called the Source AGW). Since eBS2 is not associated with LinkID1, the AT sends the packets to Route 1,

5.3 eBS Behavior

During inter-AGW handoff, the RAN PMIP tunnel between the source DAP and source AGW and the RAN PMIP tunnel between the target DAP and target AGW are maintained simultaneously. The detailed requirements for the eBS are specified in [2].

5.4 SRNC Requirements

The SRNC shall trigger EAP authentication by sending EAP-Request Identity to the AT. When the SRNC sends AAA message to the AGW, it shall include AAA-Session-ID in the AAA message as specified in [3]. The detailed requirements for the SRNC are specified in [2].

5.5 AT Requirements

The AT shall support multiple IP interfaces as specified in 0. When the AT is presented a new IP interface, the AT shall follow the requirement as specified in 0 and [3].

5.6 HAAA Requirements

If the HAAA receives a AAA-Session-ID during EAP Access Authentication procedures from a new AGW, the HAAA determines the CAN Access session has not been terminated. Since the session is continued with the new AGW, the HAAA shall return the same AAA-Session-ID and the same HA address to the AGW in the AAA messages specified in [3] during Access Authentication and authorization procedures. The HAAA shall generate a new PMN-HA key and PMN-HA-SPI using the new AGW IP address and the previous HA IP address. The HAAA shall return the new values of PMN-HA key and associated PMN-HA-SPI to the AGW during Access Authentication and Authorization procedures.

6 Call Flows

6.1 Simple IPv4 with PMIP4 Addressing using DHCP Rapid Commit Option

Figure 6 illustrates an example call flow for Simple IPv4 address assignment using DHCPv4 Rapid Commit option (see [11]).

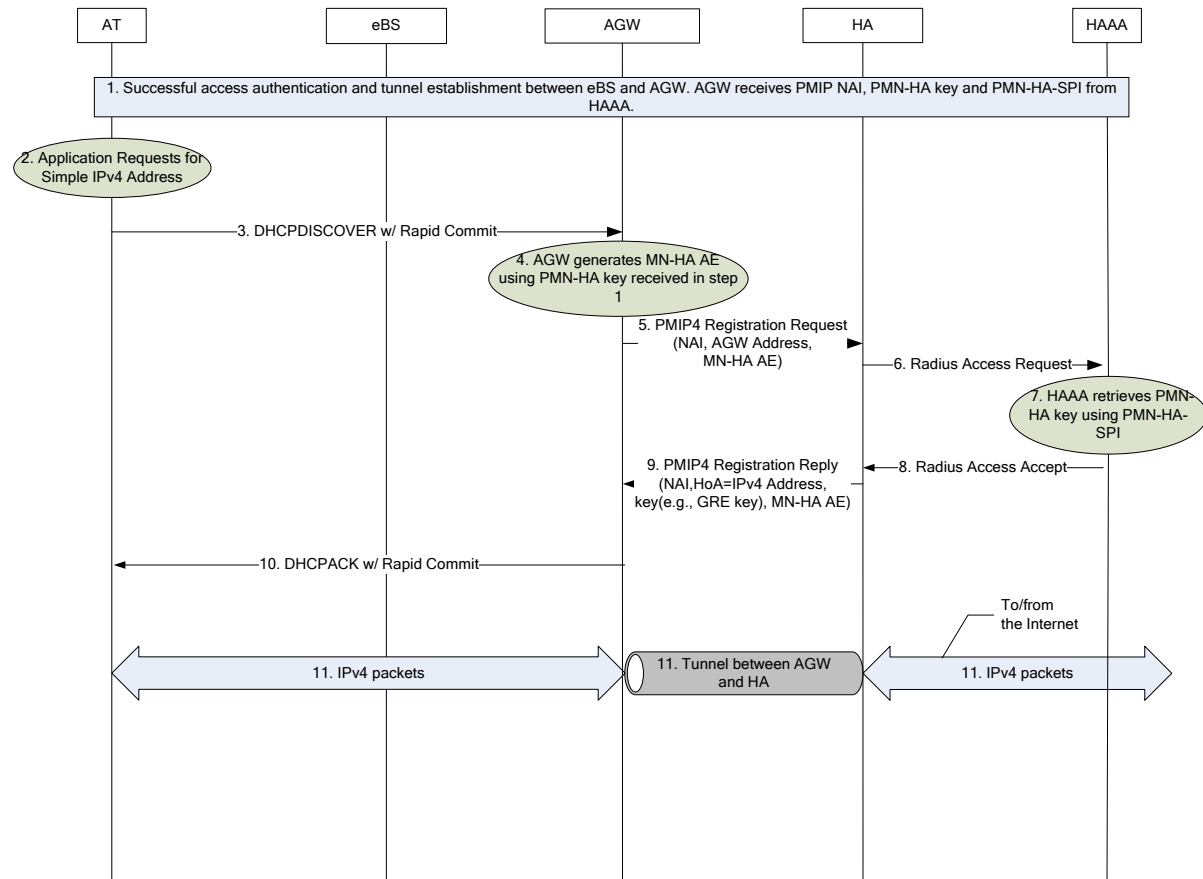


Figure 6 Simple IPv4 Address Assignment using DHCPv4 Rapid Commit Option

The steps in Figure 6 are described below.

- The AT performs a successful authentication and the primary per AT RAN PMIP tunnel is established between the eBS and AGW. In this step, the Home AAA indicates the HA address of the AT to the AGW. The AGW receives Network-PMIP-NAI, PMN-HA key and PMN-HA-SPI from the Home AAA.
- AT's application requests a simple IPv4 address. Step 2 may occur during step 1.
- The AT broadcasts a DHCPDISCOVER message with the Rapid Commit option to the eBS. The message is sent to the AGW through the RAN PMIP tunnel between

1 the eBS and AGW. The AT uses the DHCPv4 Rapid Commit option [11] in order to
2 obtain an IPv4 address and configuration information using a 2-message exchange
3 rather than the usual 4-message exchange.

- 4 4. The AGW generates a MN-HA Authentication Extension for establishing PMIP4
5 tunnel between the AGW and the HA.
- 6 5. The AGW sends a PMIP4 Registration Request message to the HA. The Proxy MIP
7 Registration Request message includes an NAI extension [14]. AGW may also
8 include the GRE Key Extension in the PRRQ message (see [7]).
- 9 6. The HA sends a RADIUS Access-Request to the Home AAA to verify the received
10 PMIP RRQ.
- 11 7. The Home AAA retrieves the PMN-HA key using the PMN-HA-SPI.
- 12 8. The Home AAA sends the RADIUS Access-Accept to the HA. The PMN-HA key
13 and PMN-HA SPI are included.
- 14 9. If the GRE Key extension was included in the PRRQ message, the HA selects a key
15 (e.g., GRE key) associated with this NAI and includes it in the GRE Key extension
16 (see [7]) in the PMIP4 Registration Reply message sent to the AGW. The HA also
17 includes the NAI extension and the HoA in the PMIP4 Registration Reply message.
18 The HA assures that the AT's IPv4 address is unique and controls the routing and
19 filter table with full 32 bits. The SPI in MN-HA Authentication Extension is set to
20 the PMN-HA-SPI received in step 8.
- 21 10. The AGW uses the PMN-HA key to verify the MN-HA Authentication Extension in
22 the PRRP message. The AGW sends a DHCPACK message with the Rapid Commit
23 option to the AT through the tunnel between the eBS and AGW.
- 24 11. AT sends/receives IPv4 packets to/from the Internet.

35 6.2 Simple IPv4 with PMIPv4 Addressing using DHCP

36 Figure 7 illustrates an example call flow for Simple IPv4 address assignment using DHCPv4.
37

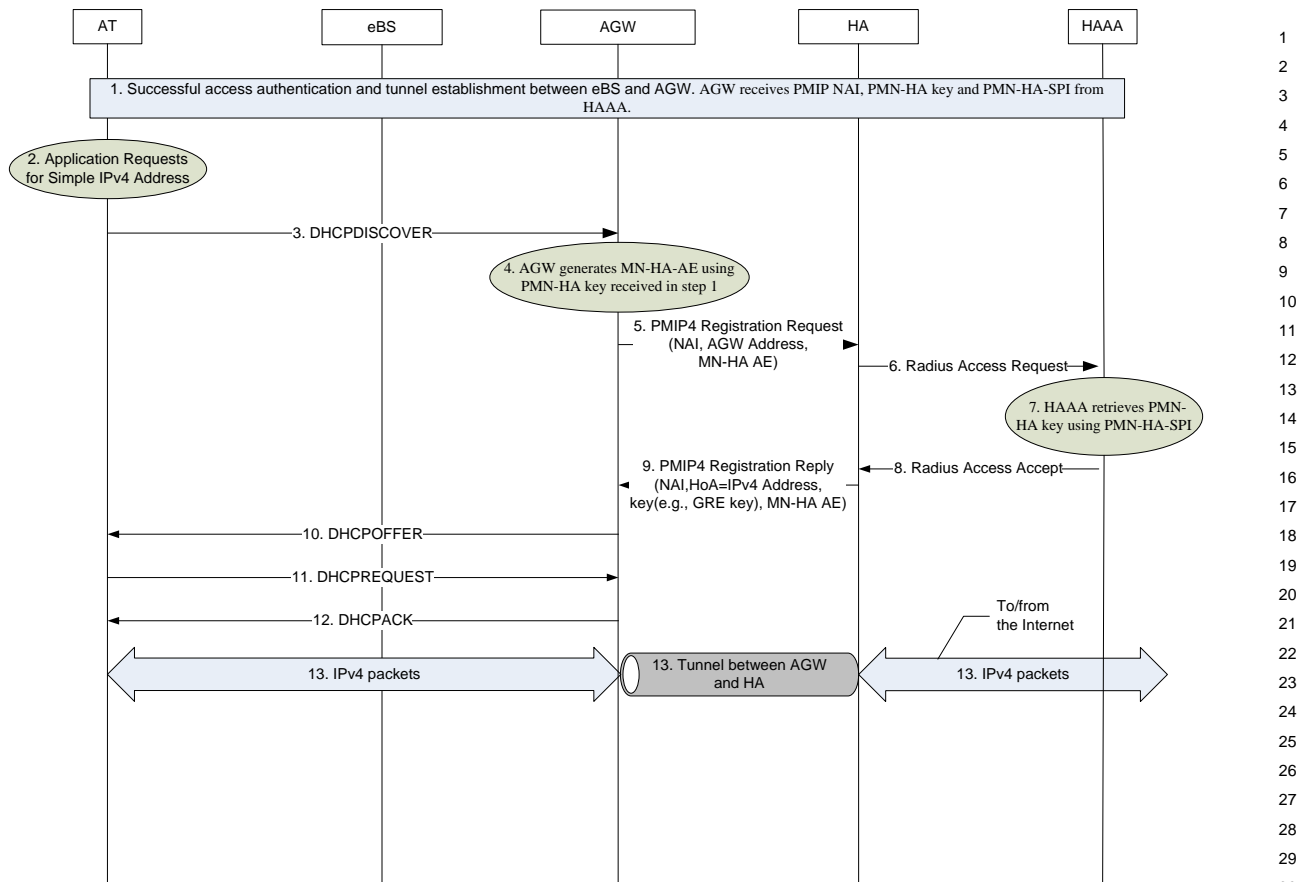


Figure 7 Simple IPv4 with PMIP Address Assignment using DHCP

The steps in Figure 7 are described below.

1. The AT performs a successful authentication and the primary per AT RAN PMIP tunnel is established between the eBS and AGW. In this step, the Home AAA indicates the HA address of the AT to the AGW. The AGW receives Network-PMIP-NAI, PMN-HA key and PMN-HA-SPI from the Home AAA.
2. AT's application requests a simple IPv4 address. Step 2 may occur during step 1.
3. The AT broadcasts a DHCPDISCOVER message to the eBS. The message is sent to the AGW through the RAN PMIP tunnel between the eBS and AGW.
4. The AGW generates a MN-HA Authenticating Extension for establishing PMIP4 tunnel between the AGW and the HA.
5. The AGW sends a PMP4 Registration Request message to the HA. The Proxy MIP Registration Request message includes an NAI extension [14]. AGW may also include the GRE Key Extension in the PRRQ message (see [7]).
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.

- 1 8. The Home AAA sends the Access Accept to the HA. The PMN-HA key and PMN-
2 HA SPI are included.
- 3 9. If the GRE Key extension was included in the PRRQ message, the HA selects a key
4 (e.g., GRE key) associated with this NAI and includes it in the GRE Key extension
5 (see [7]) in the PMIP4 Registration Reply message sent to the AGW. The HA also
6 includes the NAI extension and the HoA in the PMIPv4 Registration Reply message.
7 The HA assures that the AT's IPv4 address is unique and controls the routing and
8 filter table with full 32 bits. The SPI in MN-HA Authentication Extension is set to
9 the PMN-HA-SPI received in step 8.
- 10 10. The AGW uses the PMN-HA key to verify the MN-HA Authentication Extension in
11 the PRRP message. The AGW sends a DHCPOFFER message that includes an
12 assigned IP address received in PRRP in the 'yiaddr' field to the AT through the
13 tunnel between the eBS and AGW.
- 14 11. The AT broadcasts a DHCPREQUEST message through the tunnel between the eBS
15 and AGW. The DHCPREQUEST message includes the 'server identifier' option and
16 may include other options specifying desired configuration values. The 'requested IP
17 address' option is set to the value of 'yiaddr' of the DHCPOFFER message received
18 from the AGW. DHCPREQUEST in this case (e.g., generated during selecting state
19 [9]) does not trigger PMIP procedures.
- 20 12. The AGW sends a DHCPACK message to the AT through the tunnel between the
21 eBS and AGW
- 22 13. AT sends/receives IPv4 packets to/from the Internet.

23 24 25 26 27 28 29 30 31 32 **6.3 Simple IPv6 with PMIP4 Call Flow**

33 Figure 8 illustrates an example call flow for Simple IPv6 address assignment.
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

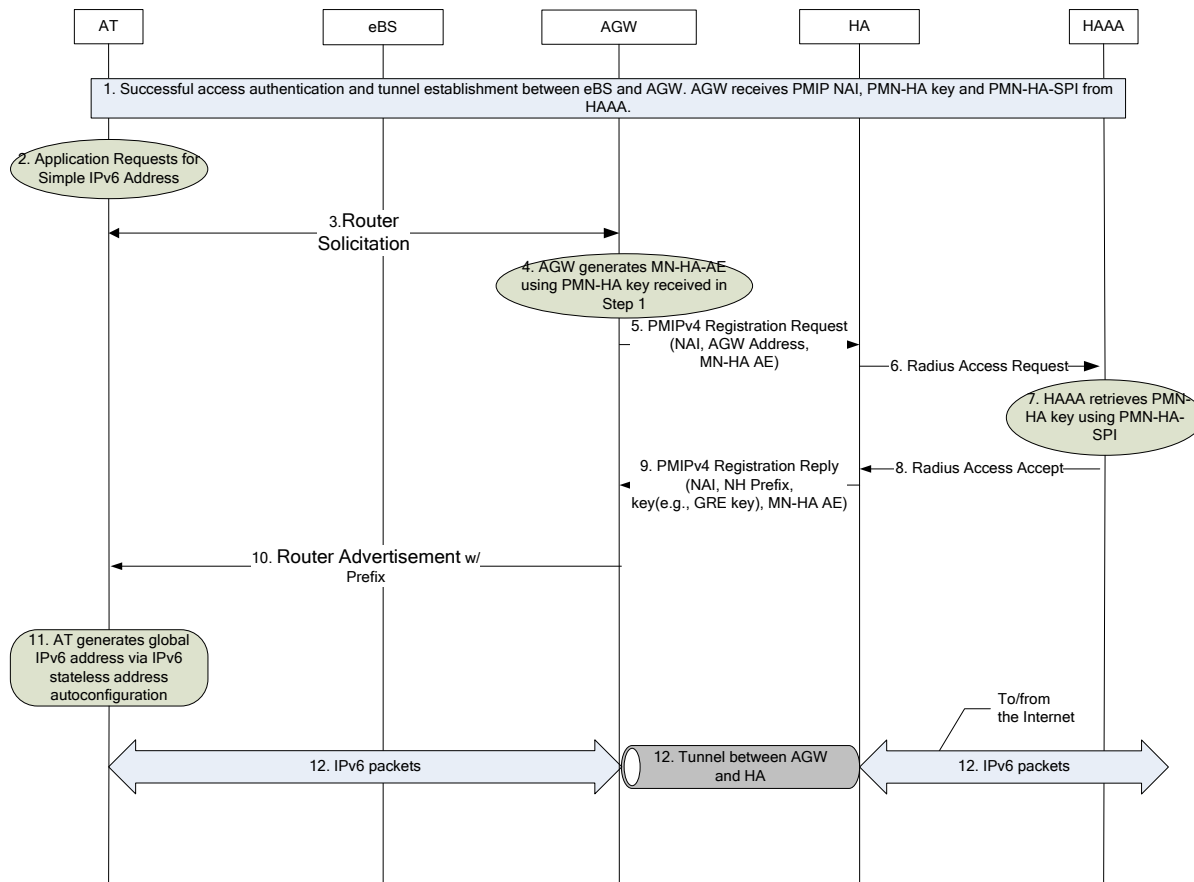


Figure 8 Simple IPv6 Address Assignment

The steps in Figure 8 are described below.

- The AT performs a successful authentication and the primary per AT tunnel is established between the eBS and AGW. In this step, the Home AAA indicates the HA address of the AT to the AGW. The AGW receives Network-PMIP-NAI, PMN-HA key and PMN-HA-SPI from the Home AAA.
- AT's application requests a simple IPv6 address. Step 2 may occur during step 1.
- The AT sends a Router Solicitation message with the source IP address set to its link local IP address and destination address set to all-routers multicast address [17]. The Router Solicitation message is sent to the AGW through the GRE tunnel between the eBS and AGW.
- The AGW generates PMN-HA Authentication Extension for establishing PMIP4 tunnel between AGW and HA.
- The AGW sends a PMIP4 Registration Request message to the HA. The PMIP4 Registration Request message includes an NAI extension [14] and Home Network Prefix. For integrity protection, the MN-HA Authentication Extension computed using the PMN-HA key is also included. AGW may also include the GRE Key Extension in the PRRQ message (see [7]).

- 1 6. The HA sends an Access Request to the Home AAA requesting the PMN-HA key to
2 verify the received PMIP RRQ.
- 3 7. The Home AAA retrieves the PMN-HA using the PMN-HA-SPI
- 4 8. The Home AAA sends the Access Accept to the HA. The PMN-HA key and PMN-
5 HA-SPI are included.
- 6 9. If the GRE Key extension was included in the PRRQ message, the HA selects a key
7 (e.g., GRE key) associated with this NAI and includes it in the GRE Key extension
8 (see [7]) in the PMIP4 Registration Reply message sent to the AGW. The HA also
9 includes an NAI extension and per-AT Home Network Prefix in the PMIP4
10 Registration Reply message. The HA also assures that the AT's prefix is unique and
11 controls the routing and filter table with 64 bits of the prefix. For integrity protection,
12 the MN-HA Authentication Extension computed using the PMN-HA key is also
13 included. The SPI in the MN-HA Authentication Extension is set to the PMN-HA-
14 SPI received in step 8.
- 15 10. The AGW uses the PMN-HA key to validate the PRRP message. The AGW sends a
16 Router Advertisement message [17] to the AT with the source IP address set to its
17 link local IP address and destination address set to all-routers multicast address or the
18 AT's link local IP address [22]. The Router Advertisement message, tunneled
19 through the eBS, contains the AT's unique home network prefix. The prefix length
20 can be configured based on operator's policy.
- 21 11. The AT generates an IPv6 global unicast address via IPv6 stateless address
22 autoconfiguration [15].
- 23 12. The AT sends/receives IPv6 packets to/from the Internet.
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32

33 6.4 PMIP Based inter-AGW Active Handoff

34 Figure 9 illustrates an example call flow for PMIP based inter-AGW active handoff.

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

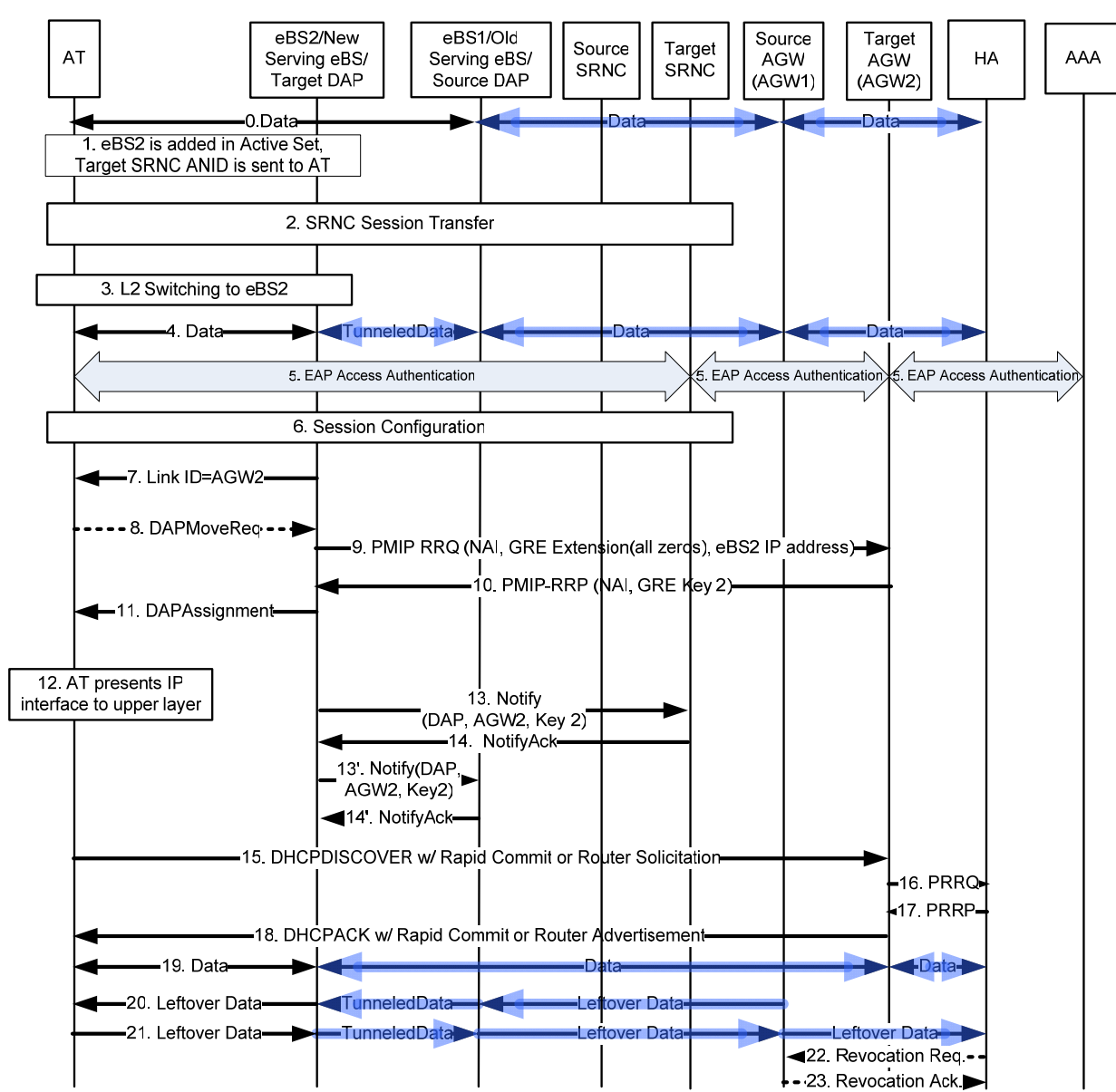


Figure 9 PMIP Based Inter-AGW Active Handoff

The steps in Figure 9 are described below.

- 0. The AT sends/receives IP packets to/from the HA through the PMIP tunnel between the HA and source AGW (AGW1) and the RAN PMIP tunnel between eBS1 (that serves as both Serving AN and DAP) and AGW1.
- 1. The AT requests to add eBS2 in the Route Set. In this example, eBS2 is connected to AGW2 and the target SRNC. The target SRNC ANID is sent to the AT.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

2. SRNC session transfer is performed. The target SRNC assigns a new UATI to the AT. As a part of UATI assignment, the target SRNC fetches session information from the source SRNC. See [2] for the details.
3. The AT performs L2 fast switching to eBS2.
4. The AT sends/receives IP packets to/from the HA through the PMIP tunnel between the HA and source AGW (AGW1), the GRE tunnel between eBS1 (that serves as both Serving AN and DAP) and AGW1, and the L2 tunnel between eBS1 and eBS2/DAP.
5. The target SRNC triggers full EAP Access Authentication and Authorization. (See [3] on Access Authentication and Authorization call flow.).
6. Target SRNC, eBS2 and AT perform session configuration. Target SRNC sends session information to eBS2 through IOS signaling in which AGW2 ID, the user's NAI, and the PMN-AN-HA1 key are sent to eBS2. (See [2] for the details.)
7. eBS2 presents new link ID to the AT. The link ID represents the IP interface that the AT creates to talk to IP layer.
8. This step is optional. . The AT sends DAPMoveReq message to the eBS2 [2].
9. Since eBS2 does not have a GRE key associated with AGW2, eBS2 sends PMIP RRQ [6] to the AGW2 which includes NAI (formatted as AAA-Session-ID@Realm, where AAA-Session-ID is received from SRNC at step 6, and Realm is the Realm portion of User Name received from SRNC at step 6), eBS2 IP address and MN-HA authentication extension calculated by using PMN-AN-HA1. AGW2's IP address and the PMN-AN-HA1 key are received in step 6.
10. AGW2 selects a GRE key 2 associated with this NAI and includes it through a GRE extension [7] in the PMIP RRP sent to eBS2.
11. eBS2 sends a DAP Assignment to the AT.
12. The AT presents the link ID to the upper IP layer. The upper IP layer compares the link ID with its current link ID. Since it is different from its current link ID, it triggers IP Address assignment procedures.
13. eBS2 notifies other Route Set members (SRNC, eBS1) about AGW2's IP address and GRE key 2 through IOS signaling (see [2] for the details.).
14. The target SRNC and eBS1 sends Notify Ack back to the eBS2.
15. Triggered by step 12, the AT sends a DHCPDISCOVER message with the Rapid Commit option or a Router Solicitation message to AGW2. The message is sent to AGW2 through the tunnel between eBS2 and AGW2.
16. AGW2 sends a PMIP RRQ message to the HA with NAI included.
17. The HA updates the binding cache entry and sends PMIP RRP message to AGW2 including the same IP address or IPv6 prefix for the AT.
18. AGW2 sends a DHCPACK message with the Rapid Commit option or Router Advertisement message to the AT through the tunnel between eBS2 and AGW2.

19. Now the AT sends/receives IP packets to/from the HA through the PMIP tunnel between the HA and target AGW (AGW2) and the tunnel between eBS2 (that serves as both Serving AN and DAP) and AGW 2.
20. On the forward link, if there is leftover data intended for the AT, that data is sent from the source AGW (AGW1) to eBS1 through the tunnel between AGW 1 and the source DAP and the tunnel between eBS1 and eBS2.
21. On reverse link, if there is leftover data sent from the AT's eBS1 route to the HA, this data will be sent through the tunnel between eBS1 and eBS2, the tunnel between eBS1 and AGW1, and the PMIP tunnel between AGW1 and HA. During this period of time, the HA may be receiving the data from both AGW1 and AGW2.
22. This step is optional. The HA may send a Registration Revocation message to the AGW1 if the bi-receiving mode is not supported in the HA.
23. AGW1 sends a Registration Revocation Acknowledgment message to the HA.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60