3GPP2 X.S0054-100-0
Version 2.0
Date: August 29, 2008

Basic IP Service for Converged Access Network Specification

This page is left blank intentionally.

Basic IP Services for Converged Access Network Specification

CONTENTS

LIST OF FIGURES

LIST OF TABLES

REVISION HISTORY

Revision	Date	Remarks
0 v1.0	December 2007	Initial release
0 v2.0	August 2008	Bug fix release for the 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 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.S0054-100-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.

This page is left blank intentionally.

1 Introduction

This document defines the stage-2 and stage-3 requirements for Simple IP access to the Converged Access Network supporting Ultra Mobile Broadband™ (UMB™) [1] Wireless access.

1.1 Scope

This document is part of a multi-part document. The multi-part document together describes IP Network operation for the Converged Access Network.

The scope of this document covers support for access authentication and authorization, RAN PMIP4 tunnel management, and IP address assignment for the CAN reference model [40].

[1] Ultra Mobile Broadband™ and (UMB™) are trade and service marks owned by the CDMA Development Group (CDG).

2 References

2.1 Normative References

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

[1] IETF: RFC 3748, Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, “Extensible Authentication Protocol (EAP)”, June 2004.

[2] IETF: RFC 4187, J. Arkko, “Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)”, January 2006.

[3] 3GPP2: C.S0084-0 v2.0, “Ultra Mobile Broadband (UMB) Air Interface”, September 2007.

[4] 3GPP2: A.S0020-0 v1.0, “Interoperability Specification (IOS) for Ultra Mobile Broadband (UMB) Radio Access Network Interfaces”, November 2007.

[5] IETF: RFC 2865, Rigney, C., Willens, S., Rubens, A. and W. Simpson, “Remote Authentication Dial in User Service (RADIUS)”, June 2000.

[6] IETF: RFC 3579, Aboba, B. and P. Calhoun, “RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)”, September 2003.

[7] IETF: RFC 2548, Zorn, G., “Microsoft Vendor-specific RADIUS Attributes”, March 1999.

[8] IETF: RFC 3588, Calhoun, et al., “Diameter Base Protocol”, September 2003.

[9] IETF: RFC 4005, Calhoun, et al., “Diameter Network Access Server Application”, August 2005.

[10] IETF: RFC 4072, Eronen, et al, “Diameter Extensible Authentication Protocol (EAP) Application”, August 2005.

[11] IETF: RFC 4301, Kent, S. and K. Seo, “Security Architecture for the Internet Protocol”, December 2005.

[12] IETF: RFC 4303, Kent, S., “IP Encapsulating Security Payload (ESP),” December 2005.

[13] IETF: RFC 4306, Kaufman, C., “Internet Key Exchange (IKEv2) Protocol”, December 2005.

[14] 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.]

[15] 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.]

[16] IETF: RFC3344, Perkins, "IP Mobility Support for IPv4", August 2002.

[17] IETF: RFC3543, Glass, et al., "Registration Revocation in Mobile IPv4", August 2003.

[18] IETF: RFC 2131, Dorms, "Dynamic Host Configuration Protocol", March 1997.

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

[20] IETF: RFC1542, Wimer, "Clarifications and Extensions for the Bootstrap Protocol", October 1993.

[21] IETF: RFC3046, Patrik, "DHCP Relay Agent Information Option", January 2001.

[22] IETF: RFC3527, Kinnear, et al., "Link Selection sub-option for the Relay Agent Information Option for DHCPv4", April 2003.

[23] 3GPP2: S.S0078-B, "Common Security Algorithms", February 2008

[24] IETF: RFC3587, Hinden, et al., "IPv6 Global Unicast Address Format", August 2003.

[25] IETF: RFC2460, Deering, et al., "Internet Protocol, Version 6 (IPv6) Specification", December 1998.

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

[27] IETF: RFC4862, Thomson, et al., "IPv6 Stateless Address Autoconfiguration", September 2007.

[28] IETF: RFC2463, Conta, et al., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", December 1998.

[29] IETF: RFC3513, Hinden, et al., "Internet Protocol Version 6 (IPv6) Addressing Architecture", April 2003.

[30] IETF: RFC3315, Droms, et al., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", July 2003.

[31] IETF: RFC3736, Droms, "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", April 2004.

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

[33] IETF: RFC4282, Aboba, "The Network Access Identifier", December 2005.

[34] IETF: RFC3576, Chiba, et al., "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", July 2003.

[35] IETF: draft-zorn-radius-logoff

[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.]

[36] IETF: draft-ietf-mip4-generic-notification-message.

[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.]

[37] IETF: RFC 5296, Narayanan and Dondeti, "EAP Extensions for EAP Re-authentication Protocol (ERP)", July 2008.

[38] IETF: draft-gaonkar-radext-erp-attrs

[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.]

[39] IETF: RFC 5295, Salowey, et al., "Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)", August 2008.sk-hierarchy

[40] 3GPP2: X.S0054-000-0 v2.0, "CAN Wireless IP Network Overview and List of Parts", August 2008.

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

[42] 3GPP2: X.S0054-910-0 v2.0, "CAN Data Dictionary", August 2008.

[43] IETF: RFC3056, Carpenter, et al., "Connection of IPv6 Domains via IPv4 Clouds", February 2001.

[44] 3GPP2: C.S0023-C, "Removable User Identity Module for Spread Spectrum Systems", June 2006.

[45] 3GPP2: C.S0065, "cdma2000 Application on UICC for Spread Spectrum Systems", June 2006.

[46] IETF: RFC2104, H. Krawczyk, et al., "HMAC: Keyed-Hashing for Message Authentication", February 1997.

[47] IETF: dondeti-dime-erp-diameter.

[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.]

[48] IETF: RFC3203, T'Joens, et al., 'DHCP reconfigure extension', December 2001.

[49] 3GPP2: X.S0054-220-0 v2.0, "Network PMIP Support", August 2008.

2.2 Informative References

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

<1> 3GPP2: X.S0054-102-0 v2.0, "Multiple Authentication and Legacy Authentication Support for CAN", August 2008.

<2> 3GPP2: X.S0054-110-0 v2.0, “MIPv4 Specification in Converged Access Network Specification”, August 2008.

<3> 3GPP2: X.S0054-210-0 v1.0, “CMIP based Inter-AGW Handoff”, December 2007.

<4> 3GPP2: X.S0054-300-0 v1.0, “QoS Support for Converged Access Network Specification”, December 2007.

<5> 3GPP2: X.S0054-400-0 v1.0, “Converged Access Network Accounting Specification”, December 2007.

3 Access Authentication and Authorization

This section specifies the network access authentication and authorization procedures in Converged Access Networks (CAN). The Extensible Authentication Protocol (EAP) [1] is used for access authentication; the Session Reference Network Controller (SRNC) is the EAP authenticator and the HAAA server is the authentication server.

EAP-AKA is the authentication method described in this document; the AT and the HAAA mutually authenticate using the EAP-AKA procedures. Upon successful authentication, if the AT is authorized to access the network, the HAAA checks policy and sends the Master Session Key (MSK) to the SRNC through the AGW. The HAAA also sends other parameters to the AGW/SRNC as specified in this part and other parts of the document.

3.1 Protocol Stack

Figure 1 and Figure 2 below illustrate the protocol stack diagram for EAP authentication. The EAP Pass Through Model is used (see 0). The AT serves as EAP Peer. The SRNC serves as EAP Authenticator. The AGW serves as Proxy AAA server. The HAAA serves as EAP Authentication server. The EAP method runs between the AT and the HAAA. The SRNC is the authenticator and thus processes the EAP packet and sends it to the AGW; the EAP packet in the visited network is AAA-routed through the appropriate AAA hops, AGW and VAAA, shown in the figure.

The SRNC may support RADIUS [5], Diameter [8], or both based on operator's local policy. The AGW and AAA may support RADIUS, Diameter, or both based on operator's policy and the roaming agreement. The translation between RADIUS and Diameter is outside the scope of this document.

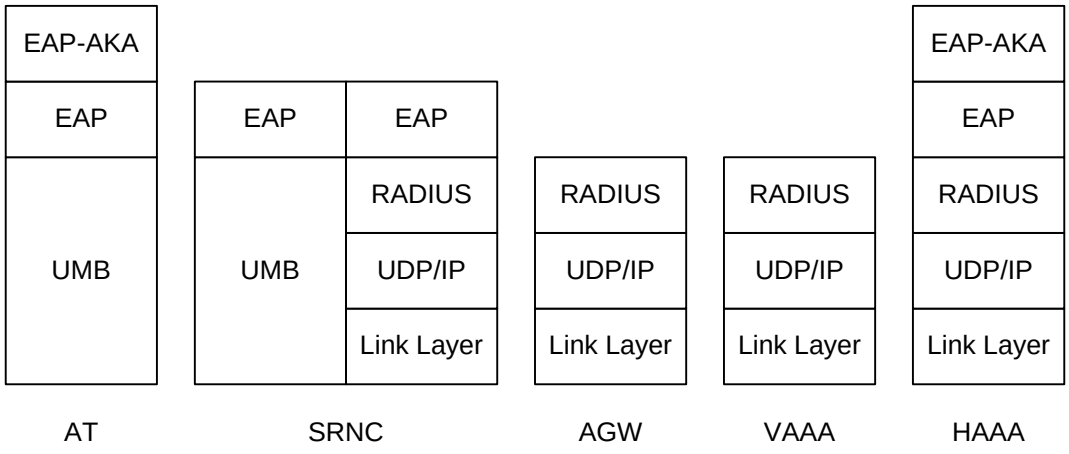


Figure 1. **EAP-AAA Protocol Stack for RADIUS**

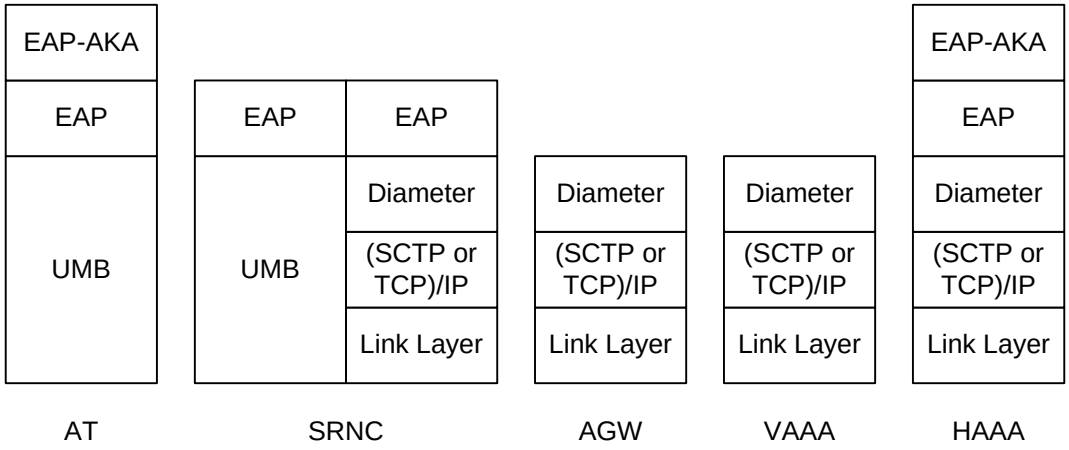


Figure 2. **EAP-AAA Protocol Stack for Diameter**

The AGW represents itself as the NAS (Network Access Server) to the HAAA and receives the parameters from the HAAA as specified in this part and other parts of X.S0054. The SRNC receives the MSK and a subset of the parameters as specified in this part and other parts of X.S0054 from the AGW.

3.2 Authentication Method and Key Management

EAP-AKA is the authentication method used. An MSK and an EMSK are derived as part of the EAP method execution, as specified in [2]. The MSK is delivered to the EAP authenticator, i.e., the SRNC. The EMSK is held securely at the HAAA and the AT.

3.2.1 MSK Derivation

The derivedMSK is computed from the MSK as follows:

T1 = EHMAC-SHA-256(MSK, “DerivedMSK”, 0x01, RouteCounter),

T2 = EHMAC-SHA-256(MSK, T1, “DerivedMSK”, 0x02, RouteCounter),

derviedMSK = T1 | T2

where the RouteCounter is defined in [3]. The RouteCounter is sent by the AT as part of the RouteOpen message and verified by the SRNC. The key label “DerivedMSK” is set to ASCII strings without NULL termination.

3.2.2 PMK Derivation

The PMK is derived from the MSK of the route as follows:

PMK = EHMAC-SHA-256(MSK, “PMK”),

where the key label “PMK” is set to ASCII strings without NULL termination.

3.3 AT Requirements

The AT shall support the following RFCs:

- RFC 3748, Extensible Authentication Protocol (EAP),
- RFC 4187, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA),

AKA long-term credentials corresponding to the AT's NAI are pre-configured in the AT. After successful EAP authentication via the SRNC, the AT shall derive the MSK from the EAP-AKA method as specified in [2]. The AT shall use the procedure of section 3.2.2 to derive the PMK for that SRNC.

When the AT adds an eBS or Target SRNC to the Route Set and if the EAP re-authentication protocol is not used, the AT shall derive a derivedMSK from the MSK of the current SRNC route, as specified in section 3.2.1. The AT shall use the RouteCounter (as specified in [4]) in the corresponding RouteOpenRequest message in the derivation. The AT shall use the derivedMSK as the MSK of the eBS route for PMK derivation. The AT shall use the procedure of section 3.2.2 to derive the PMK.

When an existing eBS in the Route Set becomes the SRNC or when a target SRNC is added to the Route Set, the AT shall set the MSK to the current derivedMSK of the eBS or target SRNC respectively and use it in future derivedMSK key derivations.

When an AT closes a route to an eBS, the AT shall delete all the keys it shares with that eBS. When an AT closes a connection (See C.S0084), the AT shall delete all the keys it shares with the SRNC except the most recent MSK. An AT may choose to keep the most recent MSK that it shares with the SRNC in its non-volatile memory for later use.

EAP-AKA does not support Master Session Key (MSK) lifetime negotiation. The AT relies on the SRNC (EAP Authenticator), to initiate EAP authentication prior to MSK expiry.

3.3.1 R-UIM/CSIM Support Requirements

The R-UIMs are the R-UIMs that support AKA [44]. CSIM (cdma2000®[1] SIM application) is an application that resides on the UICC as specified in [45]. CSIMs also support AKA functionality. When the AKA algorithms used for the EAP access authentication are terminated at such an R-UIM/CSIM, the requirements specified in this section apply to the ME part of the AT.

After the successful AKA authentication, the CK (Cipher Key) and the IK (Integrity Key) are sent from the R-UIM/CSIM to the ME. The ME uses the CK and the IK to derive EAP keys such as MSK, EMSK (see [2]). The ME shall delete the CK, IK, and any other keys (such as MSK, EMSK, etc.) derived from them from its memory after power-off as well as after removal of the R-UIM/UICC. However, the ME may store the identity of the R-UIM/UICC that was last used by it. Upon the ME powering on, if the R-UIM/UICC identity stored at the ME is same as the currently inserted R-UIM/UICC identity, the ME may request the CK and IK from the R-UIM/UICC without performing the EAP access authentication with network and generate other keys from them as needed. Otherwise, the ME shall not use the CK, IK from the R-UIM/CSIM and shall request the SRNC to initiate an EAP access authentication to obtain new keys.

[1] cdma2000® is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.

3.4 SRNC/eBS Requirements

The SRNC shall support the following RFCs:

- RFC 3748, Extensible Authentication Protocol (EAP).

The SRNC shall be the EAP authenticator in the CAN. From the AT point of view the SRNC is the authenticator and the entity that receives the MSK from the HAAA after EAP authentication.

When the AT adds an eBS to the Route Set, the eBS fetches AT's session from the SRNC. The SRNC shall verify the freshness of the RouteCounter, compute the derivedMSK from its MSK as specified in section 3.2.1 and send it to the eBS. If the EAP re-authentication protocol is not used or not enabled, the eBS shall use derivedMSK received from the SRNC as its MSK for PMK computation.

When an eBS in the Route Set becomes an SRNC, it shall continue using its current MSK for PMK computation and subsequent derivedMSK computations, using the procedures specified in section 3.2.2 and section 3.2.1, respectively.

If the SRNC was the entity performing the EAP authentication for the AT, then the SRNC shall use the MSK received from the HAAA after EAP authentication for PMK computation and subsequent derivedMSK computations, using the procedures specified in section 3.2.2 and section 3.2.1, respectively. In case of an SRNC transfer, the target SRNC shall use the derivedMSK received from the source SRNC as the MSK for PMK computation and subsequent derivedMSK computations.

If the EAP access re-authentication is performed, the SRNC shall use the keys derived from the most recent MSK (i.e., the MSK that was obtained in the most recent EAP access authentication) for procedures that make use of "derived MSK" (e.g., session get or update, see [4]) and "PMK" (e.g., KEP, see [3]).

If the EAP access re-authentication is performed, the eBS shall use the keys derived from the most recent MSK (i.e., the MSK that was obtained most recently from the SRNC) for procedures that make use of MSK and PMK (e.g., KEP, see [3]).

3.4.1 RADIUS

If RADIUS protocol is used, the SRNC shall support the following RFCs:

- RFC 2865, Remote Authentication Dial in User Service (RADIUS)
- RFC 3579, RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP),
- RFC 2548, Microsoft Vendor-specific RADIUS Attributes.

The SRNC shall send an EAP-Request/Identity over UMB Air Interface (see [3]) to the AT. Upon receiving the EAP-Response/Identity from the AT, the SRNC shall initiate the RADIUS Access-Request messages to the HAAA through the AGW. The NAS-Identifier shall contain the SRNC's own identity. The NAS-IP-address, if present, shall be set to the SRNC's IP address.

When the Session-Timeout attribute is present in a RADIUS Access-Accept message, the SRNC shall use it to set the EAP session lifetime. The SRNC shall initiate EAP authentication some time before the EAP session expires; if a non fatal error occurred during that

authentication attempt, the SRNC shall initiate another EAP authentication some time later before the lifetime expires.

The Message-Authenticator, if present, shall be computed using the HMAC-SHA-256 algorithm [23]over the entire RADIUS packet as specified in [6]. The message length is kept the same, and hence the first 16 octets of the output of the HMAC-SHA-256 function shall be used as the Message-Authenticator value.

The SRNC should use IPsec [11], [12] and IKEv2 [13] for hop-by-hop protection of RADIUS packets.

The SRNC receives the MSK via the RADIUS Access-Accept message. The first half of the MSK shall be encoded in the MS-MPPE-Recv-Key and the second half of the MSK shall be encoded in the MS-MPPE-Send-Key specified in [7].

The SRNC also receives AAA-Session-ID [42] and other parameters as specified in Table 1 in the RADIUS Access-Accept message. If one or more fields of the RADIUS Access-Accept message that are listed as mandatory attributes are not present, the SRNC shall send an EAP Failure to the AT and delete the EAP session and perform packet data session release procedure (see [4]).

Upon receiving the Access Accept message from the AGW with an Error Cause (Type 101, [34],) set to 506 “Resources Unavailable”, the SRNC shall treat the access authentication as unsuccessful. If the Access Accept message includes a vendor specific VSA (AGW-Redirect) containing an IP Address of an AGW, the SRNC may send the EAP-Request/Identity to the AT or may initiate the RADIUS Access-Request messages to the redirected AGW and follow the rest of procedures specified above in this section.

3.4.2 Diameter

If the Diameter protocol is used, the SRNC shall support the following RFCs:

- RFC 3588, Diameter Base Protocol.
- RFC 4005, Diameter Network Access Server Application
- RFC 4072, Diameter Extensible Authentication Protocol (EAP) Application

The SRNC shall send an EAP-Request/Identity over UMB Air Interface (see [3]) to the AT. Upon receiving the EAP-Response/Identity from the AT, the SRNC shall initiate a Diameter-EAP-Request command to the AGW. The NAS-Identifier shall contain the SRNC’s own identity. The NAS-IP-address, if present, shall be set to the SRNC’s IP address.

When the Session-Timeout AVP is present in a Diameter-EAP-Answer command, the SRNC shall use it to set the EAP session lifetime. The SRNC shall initiate EAP authentication some time before the EAP session expires; if a non fatal error occurred during that authentication attempt, the SRNC shall initiate another EAP authentication some time later before the lifetime expires.

IPsec with IKEv2 for key management shall be used to protect the Diameter commands on a hop-by-hop basis.

Diameter AVPs are as specified in Table 3. If the mandatory AVPs are not present, the SRNC shall send an EAP Failure to the AT and delete the EAP session and perform packet data session release procedure (see [4]).

3.5 AGW Requirements

The AGW shall construct one or two unique LinkIDs as specified in section 9. The Level 1 LinkID represents the IP interface terminating at the AGW if simple IP is supported and the Level 2 LinkID represents the IP interface terminating at the LMA/HA if the network PMIP is supported (see [49]). LinkID is specified using the RADIUS LinkID attribute or DIAMETER LinkID AVP. If both levels of LinkID are used, the AGW shall include two instances of RADIUS LinkID attribute or DIAMETER LinkID AVP.

3.5.1 RADIUS

If the RADIUS protocol is used, the AGW shall support the following RFCs:

- RFC 2865, Remote Authentication Dial in User Service (RADIUS)
- RFC 3579, RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP),

The AGW shall act as a RADIUS client in accordance with [5], and shall communicate EAP authentication information to the Home or Visited RADIUS server in a RADIUS Access-Request message. An AGW upon receiving a RADIUS Access-Request message from an SRNC to initiate authentication, may return a RADIUS Access-Accept message to the SRNC with an Error Cause (Type 101, [34],) set to 506 “Resources Unavailable” with or without a vendor specific VSA (AGW-Redirect) containing an IP Address of an AGW to which the SRNC is being redirected. The RADIUS Access-Accept message shall not contain any other attributes. Otherwise upon receipt of the RADIUS Access-Request message from the SRNC, the AGW shall create a RADIUS Access-Request message in accordance with Table 2. The AGW shall serve as the NAS from the HAAA perspective by replacing the NAS-Identifier with its own NAS-Identity and replacing NAS-IP-Address or NAS-IPv6-Address fields with its own IP address. If the AGW receives a RADIUS Access-Accept message containing a AAA-Session-ID, the MSK and additional information from the HAAA after successful authentication, it shall forward them to the SRNC as specified in Table 1. The AGW shall also derive a PMN-AN-RK1 from the randomly generated PMN-AN-RK, and send PMN-AN-RK1 to the SRNC for RAN PMIP4 signaling message protection (see section 4, RAN PMIP4 Tunnel Operation).

The AGW shall use the Session-Timeout attribute received in the RADIUS Access-Accept message from the AAA to manage the AT’s session lifetime. The Session-Timeout attribute contains the session lifetime in seconds after the RADIUS Access-Accept message has been received at the AGW. If the EAP session lifetime expires, the AGW shall discard all user packets associated with the AAA-Session-ID and delete resources associated with the AAA-Session-ID including the RAN PMIP4 binding (the binding entry).

If the AGW supports [35], the AGW shall include UserSessionTracking VSA in the RADIUS Access Request Message.

The AGW should use IPsec [11], [12] and IKEv2 [13] for hop-by-hop protection of RADIUS packets.

The Message-Authenticator field shall be present in the RADIUS Access-Accept message. The Message-Authenticator shall be computed using the HMAC-SHA-256 algorithm [23] over the entire RADIUS packet as specified in [6]. The message length is kept the same, and hence the first 16 octets of the output of the HMAC-SHA-256 function shall be used as the Message-Authenticator value.

The RADIUS Access-Accept message contains the attributes that the AGW stores as the AT's session information as specified in Table 2. If the mandatory attributes are not present, the AGW shall delete the AT's EAP session and shall revoke all PMIP bindings, if exists. The AGW shall silently discard the RADIUS Access-Accept message. The rest of the error conditions are as specified in [6], [5] and 0.

Table 1. Occurrence of RADIUS Attributes between SRNC and AGW for Access Authentication and Authorization

Attribute Name	Type	Access-Request	Access-Accept	Access-Challenge	Access-Reject
User-Name	1	1	0-1	0	0
NAS-IP-Address	4	0-1 Note 2	0	0	0
Class	25	0	0-1	0	0
Session-Timeout	27	0	1	0-1	0
NAS-Identifier	32	0-1	0	0	0
EAP-Message	79	1+	1+	1+	1+
Message-Authenticator	80	1	1	1	0
NAS-IPv6-Address	95	0-1 Note 2	0	0	0
MS-MPPE-Send-Key	26/16 (Vendor Type = 311)	0	1	0	0
MS-MPPE-Recv-Key	26/17 (Vendor Type = 311)	0	1	0	0
AAA-Session-ID	26/180	0-1 Note 1	1	1	0
PMN-AN-RK1	26/181	0	1	0	0
AGW-Redirect	26/182	0	0-1 Note 3	0	0
LinkID	26/183	0	1+	0	0
AGW-RAN-PMIP-Binding-Capability	26/202	0	0-1	0	0

0 This attribute shall not be present.
0+ Zero or more instances of this attribute may be present.
0-1 Zero or one instance of this attribute may be present.
1 Exactly one instance of this attribute shall be present.
1+ One or more of these attributes shall be present.

Note 1: AAA-Session-ID is omitted in the initial EAP Access Authentication from SRNC to AGW. AAA-Session-ID is mandatory if SRNC has AAA-Session-ID.
Note 2: At least one of NAS-IP-Address or NAS-IPv6-Address shall be included.
Note 3: If this attribute is included in the RADIUS Access-Accept message, none of the other attributes shall be included.

Table 2. Occurrence of RADIUS Attributes between AGW and AAA for Access Authentication and Authorization

Attribute Name	Type	Access-Request	Access-Accept	Access-Challenge	Access-Reject

Attribute Name	Type	Access-Request	Access-Accept	Access-Challenge	Access-Reject
User-Name	1	1	0-1	0	0
NAS-IP-Address	4	0-1 Note 2	0	0	0
Callback-ID	20	0	0-1	0	0
Class	25	0	0-1	0	0
Session-Timeout	27	0	1	1	0
NAS-Identifier	32	0-1	0	0	0
EAP-Message	79	1+	1+	1+	1+
Message-Authenticator	80	1	1	1	0
NAS-IPv6-Address	95	0-1 Note 2	0	0	0
AAA-Session-ID	26/180	0-1 Note 1	1	1	0
MS-MPPE-Send-Key	26/16 (Vendor Type = 311)	0	1	0	0
MS-MPPE-Recv-Key	26/17 (Vendor Type = 311)	0	1	0	0
Carrier-ID	26/142	1	0	0	0
User-Session-Tracking	26/184	0-1	0-1	0	0
IP-Services-Authorized	26/185	0	0-1	0	0

0 This attribute shall not be present.
0+ Zero or more instances of this attribute may be present.
0-1 Zero or one instance of this attribute may be present.
1 Exactly one instance of this attribute shall be present.
1+ One or more of these attributes shall be present.

Note 1: AAA-Session-ID is omitted in the initial EAP Access Authentication from AGW to AAA. AAA-Session-ID is mandatory if AGW has AAA-Session-ID.
Note 2: At least one of NAS-IP-Address or NAS-IPv6-Address shall be included.

3.5.2 Diameter

If the Diameter protocol is used, the AGW shall support the following RFCs:

- RFC 3588, Diameter Base Protocol,
- RFC 4005, Diameter Network Access Server Application,
- RFC 4072, Diameter Extensible Authentication Protocol (EAP) Application.

Diameter Application ID shall be set to 16777247 (3GPP2 CAN Access Authentication and Authorization).

The AGW shall act as a Diameter client in accordance with [9] and [10] and shall communicate EAP authentication information to the Visited Diameter server in a Diameter-EAP-Request (DER) command. Upon receipt of the DER command from the SRNC, the AGW shall create a DER command in accordance with Table 4. The AGW shall serve as the NAS from the HAAA perspective by replacing the NAS-Identifier with its own NAS-Identity and replacing NAS-IP-Address or NAS-IPv6-Address fields with its own IP address. If the AGW receives AAA-Session-ID, the MSK and additional information from the HAAA in the DEA command after successful authentication, it shall forward them to the SRNC as specified in Table 3. The AGW also shall derive a PMN-AN-RK1 from randomly generated PMN-AN-RK and send PMN-AN-RK1 to the SRNC for RAN PMIP4 signaling message protection (see section 4, PMIP Tunnel Operation).

The AGW shall use the Session-Timeout AVP received in the DEA command from the AAA to manage the AT's session lifetime. The Session-Timeout AVP contains the session lifetime in seconds and denotes the number of seconds after the DEA command is received at the AGW that the session is to expire.

The AGW shall use IPsec with IKEv2 for key management to protect the Diameter messages on a hop-by-hop basis.

The DEA command contains the attributes that the AGW stores as the AT's session information as specified in Table 4. If the mandatory AVPs are not present in the DEA command, the AGW shall delete the AT's EAP session and revoke all PMIP binding, if exists. The AGW shall silently discard the DEA packet. The rest of the error conditions are as specified in [8], [9] and [10].

Table 3. Occurrence of Diameter AVPs between SRNC and AGW for Access Authentication and Authorization

AVP Name	AVP Code	Diameter-EAP-Request	Diameter-EAP-Answer
User-Name	1	1	0-1
NAS-IP-Address	4	0-1 Note 1	0
Class	25	0	0-1
Session-Timeout	27	0	1
NAS-Identifier	32	0-1	0
NAS-IPv6-Address	95	0-1 Note 1	0
Session-Id	263	1	1
EAP-Master-Session-Key	464	0	0-1
EAP-Payload	462	1+	1+
AAA-Session-ID	5535/17	0-1 Note 2	1
PMN-AN-RK1	5535/18	0	1
LinkID	5535/19	0	1+
AGW-RAN-PMIP-Binding-Capability	5535/41	0	0-1

0 This AVP shall not be present.

0-1 Zero or one instance of this AVP may be present.
1 Exactly one instance of this AVP shall be present.
1+ One or more of these attributes shall be present.

Note 1: At least one of NAS-IP-Address or NAS-IPv6-Address shall be included.
Note 2: AAA-Session-ID is omitted in the initial Diameter-EAP-Request from SRNC to AGW. AAA-Session-ID is mandatory if SRNC has AAA-Session-ID.

Table 4. Occurrence of Diameter AVPs between AGW and AAA for Access Authentication and Authorization

AVP Name	AVP Code	Diameter-EAP-Request	Diameter-EAP-Answer
User-Name	1	1	0-1
NAS-IP-Address	4	0-1 Note 1	0
Callback-ID	20	0	0-1
Class	25	0	0-1
Session-Timeout	27	0	1
NAS-Identifier	32	0-1	0
NAS-IPv6-Address	95	0-1 Note 1	0
Session-Id	263	1	1
EAP-Payload	462	1+	1+
EAP-Master-Session-Key	464	0	0-1
AAA-Session-ID	5535/17 Note 2	0-1 Note 2	1
Carrier-ID	5535/20	1	0
IP-Services-Authorized	5535/21	0	0-1

0 This AVP shall not be present.
0-1 Zero or one instance of this AVP may be present.
1 Exactly one instance of this AVP shall be present.
1+ One or more of these attributes shall be present.

Note 1: At least one of NAS-IP-Address or NAS-IPv6-Address shall be included.
Note 2: AAA-Session-ID is omitted in the initial Diameter-EAP-Request from AGW to HAAA. AAA-Session-ID is mandatory if AGW has AAA-Session-ID.

3.6 HAAA Requirements

The HAAA shall support the following RFCs:

- RFC 3748, Extensible Authentication Protocol (EAP),

- RFC 4187, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA).

3.6.1 RADIUS

If the RADIUS protocol is used, the HAAA shall support the following RFCs:

- RFC 2865, Remote Authentication Dial in User Service (RADIUS),
- RFC 3579, RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP),
- RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS).

The Home RADIUS server and Visited RADIUS server shall support the attributes as specified in Table 2.

IPsec [11], [12] with IKEv2 for key management [13] should be used for hop-by-hop protection of RADIUS packets.

The Message-Authenticator field shall be present in the RADIUS Access-Request message. The Message-Authenticator shall be computed using the HMAC-SHA-256 algorithm [23] over the entire RADIUS packet as specified in [6]. The message length is kept the same, and hence the first 16 octets of the output of the HMAC-SHA-256 function shall be used as the Message-Authenticator value.

In addition to the specifications of [5], the HAAA shall ignore RADIUS attributes with an unknown Type value.

The HAAA shall send the attributes as specified in Table 2 in the RADIUS Access-Accept message, Access-Challenge message, or Access-Reject message.

The HAAA shall send the session lifetime in seconds via the Session-Timeout attribute in the RADIUS Access-Accept message.

If the HAAA has not received User-Session-Tracking attribute from the AGW in the RADIUS Access-Request message, the HAAA shall not include User-Session-Tracking attribute in the RADIUS Access-Accept message. If that HAAA has received User-Session-Tracking attribute from the AGW in the RADIUS Access-Request Message to indicate the AGW supports user session tracking (see [35]), the HAAA may send User-Session-Tracking attribute to the AGW in the RADIUS Access-Accept message to indicate that the user session tracking mechanism for AAA session start and termination is enabled.

The HAAA may send IP-Services-Authorized attribute to the AGW in the RADIUS Access-Accept message to indicate what IP services are authorized for this AT. If the HAAA authorizes MIPv6, the HAAA shall also authorize Simple IPv6. Lacking of this attribute indicates the AGW that all IP services are authorized to this AT.

The HAAA may send IMSI value to the AGW for the AT if it is a hybrid terminal in the Callback-ID attribute.

The error processing is as specified in [6], [5] and 0.

3.6.2 Diameter

If the Diameter protocol is used, the HAAA shall support the following RFCs:

- RFC 3588, Diameter Base Protocol,
- RFC 4072, Diameter Extensible Authentication Protocol (EAP) Application.

Diameter Application ID shall be set to 16777247 (3GPP2 CAN Access Authentication and Authorization).

The Home Diameter server and Visited Diameter server shall support the AVPs as specified in Table 4.

IPsec [11], [12] with IKEv2 for key management [13] shall be used for hop-by-hop protection of Diameter packets.

The HAAA shall send the AVPs as specified in Table 4 in the DEA command.

The HAAA shall send the session lifetime in seconds via the Session-Timeout AVP in the DEA command.

The HAAA may send IP-Services-Authorized AVP to the AGW in the DEA to indicate what IP services are authorized for this AT. If the HAAA authorizes MIPv6, the HAAA shall also authorize Simple IPv6 service. Lacking of this AVP indicates the AGW that all IP services are authorized to this AT.The HAAA may send IMSI value for the AT if it is a hybrid terminal in the Callback-ID AVP.

The error processing is as specified in [8], [9] and [10].

4 RAN Proxy Mobile IPv4 Tunnel Operation

The PMIP tunnel between eBS and AGW is established anytime after the EAP access authentication and authorization are performed successfully. The primary PMIP tunnel is established when the AGW successfully completes the primary PMIP registration with an eBS (i.e., sending a PMIP RRP in response to receiving a PMIP RRQ without a Binding Type Extension, or with a Binding Type Extension set to RL+ Primary). The primary PMIP binding is a bi-directional binding.

Based on the network's configuration in both eBS and AGW, the multiple PMIP registrations may be performed between the eBSs in the route set of the AT and the AGW to allow direct tunneling of reverse link packets from eBSs in the route set to the AGW without traversing the DAP.

Support of multiple binding in the eBS and AGW is optional based on operator's local policy. The AGW communicates its support for multiple bindings by sending 'AGW-RAN-PIMP-Binding-Capability' [42] information to the SRNC, and thereby to the eBS. If multiple binding in the AGW is supported and enabled by operator's policy, the AGW shall simultaneously support eBSs that require a single binding and eBSs that enable multiple bindings for the same AT.

Based on the network's configuration in both the SRNC and the AGW, signaling only PMIP registration may be performed between the SRNC and the AGW to allow signaling only binding for the AT.

Support of signaling only binding in the SRNC and AGW is optional based on operator's local policy. The AGW communicates its support for signaling only binding by sending 'AGW-RAN-PIMP-Binding-Capability' [42] information to the SRNC. If signaling binding in the AGW is supported and enabled by operator's policy, only one Signaling Only Binding or one Primary Binding (with or without multiple Reverse Link Bindings) may exist at a time for the AT.

Appropriate RFCs specify actions to be taken when a CVSE is not recognized. Actions specified in the remainder of this section assume that the receiver has recognized the received CVSE.

4.1 Protocol Stack

Figure 3 shows the protocol reference model for PMIP data flow and Figure 4 shows the protocol reference model for the PMIP signaling path.

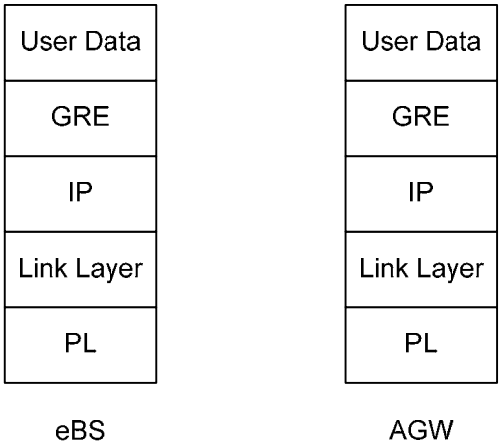


Figure 3. **Protocol Stack for PMIP Data Path**

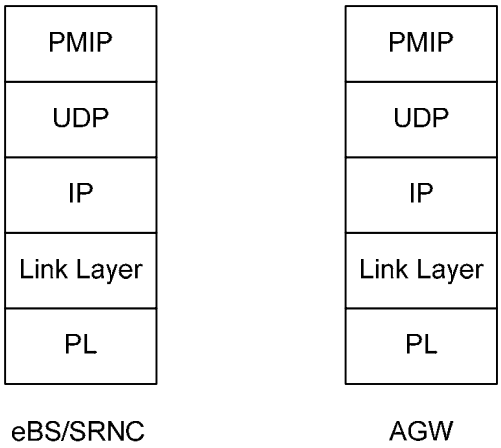


Figure 4. **Protocol Stack for PMIP Signaling Path**

4.2 PMIP Key Management

The eBS/SRNC and the AGW require a symmetric key for securing the PMIP signaling messages between these two entities. A per-AT key is used for this purpose. The AGW chooses a random key of 256-bit length for PMIP purposes, known as the PMN-AN-RK. At the time of access authentication, the AGW derives a PMN-AN-RK1 for the AT and sends it to the SRNC as a part of the authentication exchange. When an eBS is added to the route set, the SRNC derives a PMN-AN-HA1 key specific to that eBS and AT based on the latest PMN-AN-RK1 and provides it, along with the sequence number used to derive the key, to the eBS. The PMN-AN-RK1 and PMN-AN-HA1 keys are computed as follows:

PMN-AN-RK1 = HMAC-SHA-256(PMN-AN-RK, “PMN-AN-RK1”)

PMN-AN-HA1 = HMAC-SHA-256(PMN-AN-RK1, “Derived PMIP Key”, sequence, eBS/SRNC IP Address, AGW IP Address)

In order to compute the fresh PMN-AN-HA1 key for every PMIP binding, the SRNC maintains a sequence number. The SRNC chooses a sequence number that is unique for a

given AT during the eBS-AGW PMIP tunnel lifetime. This sequence number is coordinated between the SRNC and the eBS being added to the route set. The eBS/SRNC provides the sequence number to the AGW in the SPI field (see [4]) of the MN-HA authentication extension in the PMIP RRQ message. The eBS/SRNC prepends 4 MSBs to the 28 bits of sequence number to form the SPI field sent to the AGW. The 4 MSBs of the SPI field indicate the algorithm to compute the MN-HA Authentication extension. The 4 MSBs of the SPI field shall be set as the follows:

‘0000’: Reserved

‘0001’: HMAC-MD5 (See [46])

‘0010 – ‘1111’: Reserved.

Once the PMIP RRQ containing the MN-HA Authentication Extension, and thus the SPI with the sequence number in it, is received by the AGW, the AGW shall compute the same PMN-AN-HA1 key based on the latest PMN-AN-RK1, before verifying the authentication data in the MN-HA authentication extension.

4.3 eBS/SRNC Behavior

See [4] for the requirements.

4.3.1 Generic Notification

The SRNC shall formulate the Generic Notification Acknowledgement message to be transmitted to the AGW per [36], with the constraints specified below:

a. The Type field shall be set to [TBD][36].

b. The Subtype field shall be set to [TBD][36].

c. The MD (Message Direction) field shall be set to value 2 to indicate that the message is sent by the MN to the Home Agent.

d. The Reserved field shall be set to all zeros.

e. The Home Address shall be set to all zeros.

f. The Home Agent Address shall be set to the IP address of the AGW.

g. The Care-of-Address (Co-located CoA) field shall be set to the IP address of the SRNC or the eBS by which the message is generated.

h. The Identification field shall echo back the value contained in the Identification field of the corresponding PMIP Generic Notification message.

i. The GRE Key Extension as specified in [14] shall be included and set to the GRE key value corresponding to this PMIP session, as assigned by the AGW.

j. The Mobile Node NAI Extension per [41] shall be included.

The MN-HA Authentication extension based on the PMN-AN-HA1 key shared by the AGW and the SRNC/eBS by which the message was generated.

4.4 AGW Requirements

The AGW shall support the Home Agent (HA) behavior as specified in [15]. If the AGW receives an initial PMIP RRQ for a user session identified by the Mobile Node NAI Extension, the AGW shall check if the GRE Key extension with the value of all 0s is included in the message, as specified in [14]. If not, the AGW shall reject the PMIP RRQ by sending a PMIP RRP with the error code "134 poorly formed Request". If the GRE Key extension with all 0s is included in the message, the AGW shall assign a symmetric GRE key to be used as both forward direction and reverse direction GRE key for the user session identified by the Mobile Node NAI Extension.

The value of the assigned GRE key, say k, shall meet the following requirements:

1. The two MSBs of the GRE key shall be set to 0.
2. The value k assigned shall always be even, i.e. the LSB of the GRE key shall be set to zero. Then, the even GRE key k shall be associated with the Level 1 IP interface of the AT, while the value k+1 shall be associated with the Level 2 IP address of the AT. The AGW shall bind both GRE keys k and k+1 to the same AT, for different levels of IP interfaces. See Section 3.5. LinkID levels are described in Section 9.
3. The subsequent PMIP RRQ messages for the same AT shall be received with GRE key k, i.e., Level 1 GRE key. If PMIP RRQ packets are received with the Level 2 GRE key, the AGW shall reject the PMIP RRQ by responding with a PMIP RRP with the error code "134 poorly formed Request". The PMIP RRP rejecting the request shall use the same GRE key as the corresponding PMIP RRQ.

The AGW shall process packets differently depending on whether they are encapsulated in GRE key k or k+1. For packets encapsulated with key k+1, the AGW shall forward them to the LMA/HA via the PMIP tunnel (see [49]). Local breakout packets encapsulated with key k shall be routed to local destinations, without any encapsulation.

For the subsequent PMIP RRQ messages for a user session identified by the Mobile Node NAI Extension, the AGW shall check if the GRE Key extension with either the existing GRE key or all 0s is included in the message. If not, the AGW shall reject the PMIP RRQ by sending a PMIP RRP with the error code "134 poorly formed Request". Otherwise, the AGW shall perform the following:

- If the existing GRE key in GRE extension is included appropriately, the AGW shall process the PMIP RRQ in accordance with [15] and [14]. The AGW shall respond with a PMIP RRP including GRE Key Extension. GRE key extension shall be set to the value of the previously assigned symmetric GRE key for the user session identified by the Mobile Node NAI Extension.
- If all zero GRE key in GRE extension is included appropriately, the AGW shall process the PMIP RRQ in accordance with [15] and [14]. The AGW shall respond with a PMIP RRP including GRE Key Extension. GRE key extension shall be set to a newly assigned different symmetric GRE key for the user session identified by the Mobile Node NAI Extension. The AGW shall send MIP revocation to the previous primary/signaling PMIP binding end point if different.

The AGW shall not assign HoA to the AT in the PMIP RRP. The AGW may include the GRE Tunnel Endpoint Extension CVSE as defined in section 4.6 in the PMIP RRP. The AGW shall also maintain a binding between the GRE key, NAI and the eBS/SRNC IP address received in the PMIP Registration Request.

If the AGW using RADIUS protocol receives UserSessionTracking during EAP access authentication, immediately upon the primary PMIP tunnel establishment, the AGW shall send the Session Notification Message to the HAAA with session notification type set to "start" (see [35]) and with User Name and AAA-Session-ID included. When the primary PMIP tunnel is released and no Signaling Only Binding has been established or when the Signaling Only tunnel is released and no Primary Binding has been established, the AGW shall send Session Notification Message to the HAAA with session notification type set to "end" and with User Name and AAA-Session-ID attributes included.

Upon receiving PMIP RRQ from an eBS/SRNC, the AGW shall derive the PMN-AN-HA1 key associated with the eBS/SRNC for the AT, as specified in Section 4.2. The AGW shall verify the authentication extension upon receiving the PMIP RRQ in accordance with [15]. Upon successful validation of the MN-HA Authentication Extension, the AGW shall respond with a PMIP RRP including an MN-HA authentication extension computed using the PMN-AN-HA1 key that was provided or derived for that particular {eBS/SRNC, AT} pair. The AGW shall maintain the PMN-AN-HA1 key that was derived for that particular {eBS/SRNC, AT} pair, as well as the corresponding SPI, only for the duration of the PMIP tunnel for the AT from that eBS/SRNC. If the PMIP tunnel is released and later re-established, a new PMN-AN-HA1 key shall be derived for that {eBS/SRNC, AT} pair.

If the AGW receives a PMIP RRQ from the eBS/SRNC and the AGW does not have any user information associated with AT, the AGW shall send a PMIP RRP with the Code Field set to 128 (reason unspecified) to the eBS/SRNC. If the AGW receives PMIP RRQ and PMIP authentication fails, the AGW shall send a PMIP RRP with the Code Field set to 131 (mobile node failed authentication) to the eBS/SRNC.

The AGW shall not use the following error codes in PMIP RRP (see [16]):

- 132 foreign agent failed authentication,
- 135 too many simultaneous mobility bindings,
- 136 unknown home agent address.

The AGW shall send a Registration Revocation message to the primary PMIP binding end point or Signaling Only binding end point (whichever exists) upon receiving Disconnect-Request message (for RADIUS) or Abort-Session-Request command (for Diameter) (see Section 8). The AGW may send a Registration Revocation message to the primary PMIP binding end point or Signaling Only binding end point (whichever exists) (see [17]) for other reasons based on local policy.

The Primary PMIP binding end point is specified as the entity from which the AGW has received successful PMIP binding without Binding Type Extension, or the AGW has received successful PMIP binding with Binding Type Extension set to RL + Primary Binding. The Signaling Only binding end point is specified as the entity from which the AGW has received successful PMIP binding with Binding Type Extension set to Signaling-Only binding.

If the AGW sends a Registration Revocation message [17], the AGW shall perform the following:

- The AGW shall send Registration Revocation message with source IP address set to the AGW's IP address, with destination IP address set to the Primary PMIP binding end point's or Signaling Only binding end point's IP address, with 'A' bit set to 1 and 'I' bit set to '0', and with home address set to all zero IP address.
- The AGW shall include Mobile Node NAI Extension ([41]) and GRE extension with the existing GRE key in the Registration Revocation message.

- If the AGW does not receive a revocation acknowledgment message within a operator's configuration amount of time, it shall retransmit the registration Revocation message as specified in [17].

The AGW shall discontinue IP services and clean up the resources as specified in Section 8.

4.4.1 Single PMIP Binding

The AGW shall treat a PMIP RRQ without a Binding Type Extension as a primary PMIP binding. If the primary PMIP binding is successful, the AGW shall send the forward link packets only to this eBS. The AGW shall replace the previous primary PMIP binding or signaling PMIP binding with the new primary PMIP binding upon receiving and validating a new primary PMIP RRQ.

When the primary PMIP binding lifetime expires, or the AGW receives a primary PMIP Deregistration (a PMIP lifetime set to 0), the AGW shall delete the AT's state. However, the resource clean up at the AGW should not trigger release of the IP address if the IP address is still within the valid lease time.

4.4.2 Multiple PMIP Bindings

If the AGW is configured to use multiple bindings per AT, the AGW shall process the packets from the AT only if received from an eBS that has performed a successful reverse link PMIP registration (i.e., Binding Type extension set to "RL Only Binding") or primary PMIP registration for that AT. The AGW shall discard any data received from an eBS which has not performed a successful primary PMIP registration or reverse link PMIP registration. When the RL PMIP binding lifetime expires, or the AGW receives a PMIP RRQ Deregistration (a PMIP lifetime set to 0) with the Binding Type extension set to RL Binding only value, the AGW shall discard the data received from the eBS.

If the AGW receives a PMIP RRQ with a Binding Type extension for a RL only binding and the AGW is not configured to support RL only bindings the AGW shall return a PMIP RRP to the eBS with a Code 129.

If the AGW receives a PMIP RRQ with a Binding Type extension set to "RL Only Binding" for an AT for which it has no primary binding, the AGW shall reject the binding by returning a PMIP RRP with a Code 129.

4.4.3 Signaling-Only PMIP Binding

Only one Signaling Only Binding may exist at one time per AT. If a PMIP binding with Binding Type extension set to "Signaling Only" is successful, the AGW shall replace the previous primary PMIP binding or Signaling Only binding and shall not send data packets for the associated AT to this entity. The AGW shall send data notification signaling indication on this binding when data arrives from the network as specified in section 4.4.4.

4.4.4 Data Notification

If the AGW supports Signaling Only PMIP Binding, the AGW shall support data buffering based on operator's local policy and shall support [36]. If the AGW receives packet data from the network while the Signaling Only Binding is in effect, and if the AGW supports data buffering, the AGW shall buffer data and send Generic Notification Message as specified in [36], with the constrains specified below:

a. The Type field shall be set to [TBD][36].

b. The Subtype field shall be set to [TBD][36].

c. The MD (Message Direction) field shall be set to value 0 to indicate that the message is sent by the Home Agent to the MN.

d. The A bit shall be set to '1'.

e. The Reserved field shall be set to all zeros.

f. The Home Address shall be set to all zeros.

g. The Home Agent Address shall be set to the IP address of the AGW generating the message.

h. The Care-of-Address (Co-located CoA) field shall be set to the IP address of the SRNC for which the message is generated.

i. The Identification field shall be set according to the timestamp based replay protection method, per section 5.7 of [16].

j. The GRE Key Extension as specified in [14] shall be included and set to the GRE key value corresponding to this PMIP session at the AGW.

k. The Mobile Node NAI Extension per [41] shall be included.

l. The Data Notification Extension as specified in section 4.7 shall be included.

m. The MN-HA Authentication extension based on the PMN-AN-HA1 key shared by the AGW and the SRNC for which the message is generated.

The AGW shall support receipt of a Generic Notification Acknowledgement message from the SRNC in response to a transmitted Generic Notification message.

If the AGW has received Generic Notification Acknowledgment message with Data Notification Timer NVSE included for the GRE Key and NAI specified in the Generic Notification message within an operator configurable amount of time, the AGW should not resend the Generic Notification Message as specified above within the time specified by the SRNC in Generic Notification Acknowledgment message; otherwise, the AGW shall resend Generic Notification Message as specified above for an operator configurable number of times. If the AGW has not received Data Notification Timer NVSE in Generic Notification Acknowledgment message, the AGW should use an operator configurable time to decide when to resend Generic Notification Message. If the time specified by the SRNC or the operator configured time has lapsed and if the AGW has data for the AT, the AGW should send another Data Notification message to the SRNC.

If the AGW has received a PMIP RRQ (either without Binding Type Extension or with Binding Type Extension set to RL+Primary Binding), the AGW shall stop sending the Generic Notification Message.

The AGW should continue to buffer data for the session until receipt of a PMIP RRQ (either without Binding Type Extension or with Binding Type Extension set to RL+Primary Binding) for the GRE Key and NAI.

4.5 Binding Type Extension CVSE

To support multiple binding, the following PMIP CVSE is specified:

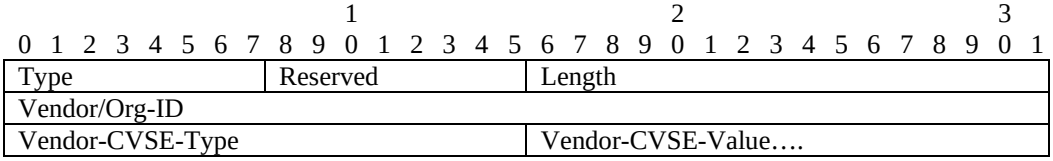


Figure 5. **Binding Type Extension CVSE**

Type:	CVSE-TYPE-NUMBER 38
Reserved:	Reserved for future use. To be set to '0'
Length:	Length in bytes of this extension, not including the Type and Length bytes.
Vendor/Org-ID:	5535
Vendor-CVSE-Type:	1281(05H 01H)
Vendor-CVSE-Value:	This 16-bit field is encoded as follows: 0: Signaling Only Binding (ie, no data) 1: RL Only Binding 2: Reserved for Future Use 3: RL + Primary Binding Other values: Reserved.

4.6 GRE Tunnel Endpoint Extension CVSE

To differentiate the PMIP Data Path from the PMIP Signaling Path, the following PMIP CVSE is specified:

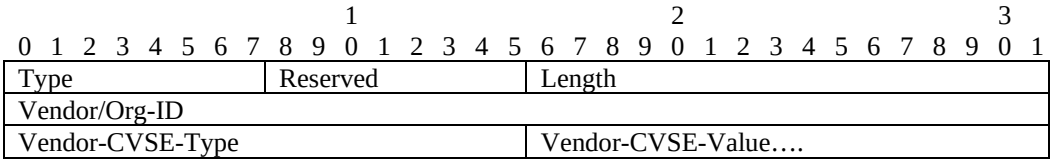
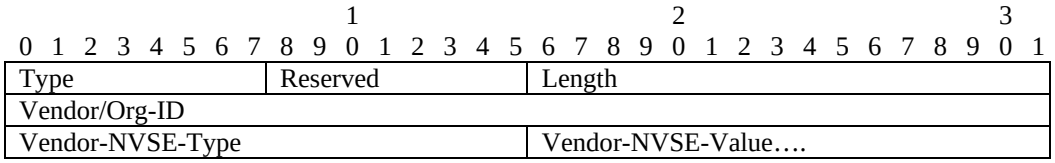


Figure 6. **GRE Tunnel Endpoint Extension CVSE**

Type:	CVSE-TYPE-NUMBER 38
Reserved:	Reserved for future use. To be set to '0'
Length:	Length in bytes of this extension, not including the Type and Length bytes.
Vendor/Org-ID:	5535
Vendor-CVSE-Type:	1537 (06H 01H)
Vendor-CVSE-Value:	This 32-bit field specifies the IP Address of the GRE tunnel associated with the PMIP Data Path. If this CVSE is omitted in the PMIP RRP then the IP Address is defaulted to the Destination Address of the PMIP RRQ.

4.7 Data Notification NVSE

To support data notification, the following Data Notification NVSE included in the Generic Notification Message is specified:



0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type	Reserved	Length
Vendor/Org-ID		
Vendor-NVSE-Type		Vendor-NVSE-Value….

Figure 7. **Data Notification Extension NVSE**

Type: NVSE-TYPE-NUMBER 16

Reserved: Reserved for future use. To be set to '0'

Length: Length in bytes of this extension, not including the Type and Length bytes.

Vendor/Org-ID: 5535

Vendor-NVSE-Type: 3073 (0CH 01H)

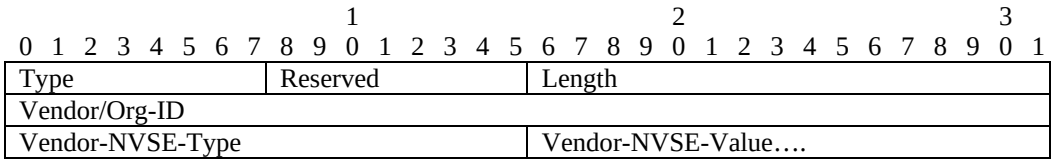
Vendor-CVSE-Value: This 16-bit field is encoded as follows:

0: Data Available.

Other values: Reserved.

4.8 Data Notification Timer NVSE

To support data notification, the following Data Notification Timer NVSE included in Generic Notification Acknowledgment message is specified:



0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type	Reserved	Length
Vendor/Org-ID		
Vendor-NVSE-Type		Vendor-NVSE-Value….

Figure 8. **Data Notification Extension NVSE**

Type: NVSE-TYPE-NUMBER 16

Reserved: Reserved for future use. To be set to '0'

Length: Length in bytes of this extension, not including the Type and Length bytes.

Vendor/Org-ID: 5535

Vendor-NVSE-Type: 3329 (0DH 01H)

Vendor-NVSE-Value: This field is set to the time, in units of the 100 milliseconds, within which the AGW should not resend Generic Notification Message. The value of zero means the AGW applies the local policy.

5 ERP Operation

There are two alternatives for the eBS to obtain the session key used for deriving the TSK (Temporary Session Key) for over-the-air (OTA) protection (see [3]). One alternative is that the eBS obtains a derivedMSK (derived from MSK) from the SRNC through session retrieval procedures as specified in [4] when it is added in the Route Set. The second alternative is that the eBS obtains the rMSK from the AGW through the EAP Re-authentication Protocol (ERP) operation.

After completion of initial authentication using EAP, an EMSK (Extended Master Session Key) for the AT is available at the AT and the HAAA server. If ERP is enabled, when the AT adds another eBS to its route set, it performs re-authentication using a key hierarchy based on the EMSK, to obtain a new MSK (called rMSK) at the eBS.

The re-authentication procedure is based on the EAP Re-authentication Protocol (ERP) [37].

ERP support is optional for an AT and the network. If the AGW supports ERP, it requests DSRK (derived from EMSK) from the HAAA through initial full EAP Access Authentication. The AGW also indicates its ERP support capability to the SRNC through initial full EAP Authentication. After successful full EAP authentication, the SRNC and AT negotiate whether or not to perform ERP via UMB session configuration procedures specified in OTA UMB session negotiation (see [3]). When a new eBS is added in the Route Set, if the UMB session indicates that ERP is supported, the AT starts the ERP procedures. In the case that the newly added eBS does not support ERP, the eBS uses the derivedMSK received from the SRNC through session retrieval procedures (see [4]) and indicates it to the AT using PMK ID as specified in [3]. In this case, AT and eBS uses DerivedMSKkey to derive TSK used for OTA protection. Also PMN-AN-HA1 is included in this case.

5.1 Protocol Stack

Figure 9 shows the protocol reference model for Re-authentication with RADIUS. Figure 10 shows the protocol reference model for Re-authentication with Diameter.

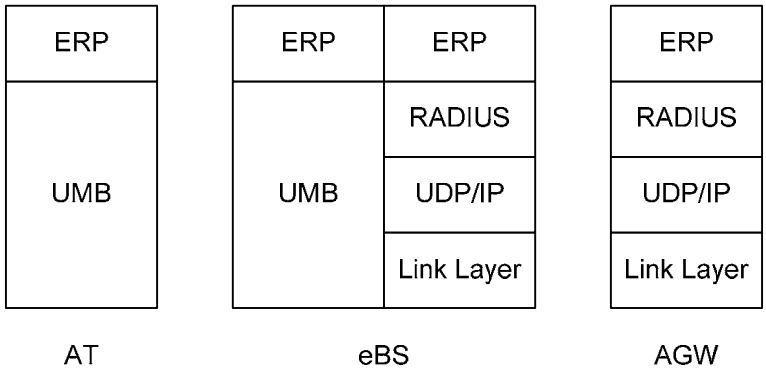


Figure 9. **Protocol Stack for ERP Operation with RADIUS**

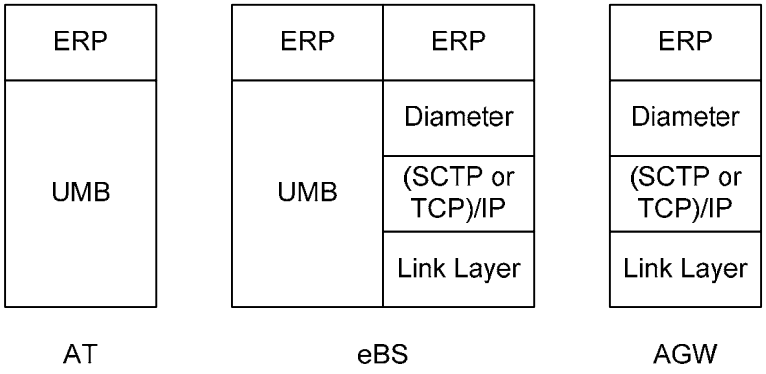


Figure 10. **Protocol Stack for ERP Operation with Diameter**

5.2 AT Requirements

When the AT supports ERP, it shall support the ER peer functionality described in [37]. Upon successful ERP operation, the AT shall use rMSK as its MSK to derive PMK as specified in section 3.2.

The AT shall trigger a full EAP exchange via the SRNC with an InitiateEAP message when the DSRK is close to expiry.

If the ERP exchange fails, the AT shall follow the behavior based on the error codes as defined in [37]. If the error code indicates lack of valid rIK in the network, the AT shall trigger a full EAP exchange via the SRNC with an InitiateEAP message.

The AT shall initiate ERP with the eBS when an eBS is added in the route set.

When ERP is used, upon change of AGW (indicated by a change in LinkID), the AT shall initiate an ERP bootstrapping exchange with the HAAA as specified in [37].

5.3 eBS Procedures

Support of ERP in the eBS is described in [37]. Upon receiving the rMSK from AGW, the eBS uses rMSK as is MSK to derive PMK as specified in section 3.2.

5.4 AGW Requirements

The AGW may support ERP as specified in [37].

In order to compute the PMN-AN-HA2 key for an AT for every PMIP binding, the AGW chooses a different sequence number from the previous sequence numbers given to the AT.

5.4.1 RADIUS

If RADIUS is used, the AGW shall follow the requirement as specified in this section.

If the AGW supports ERP, it shall act as the ER server described in [37]. The AGW shall support encapsulation of ERP messages in RADIUS. The AGW shall request a DSRK from the HAAA by using a RADIUS Key-Request attribute (see [38]) as part of the full EAP exchange or an ERP bootstrapping exchange. The Key-Request attribute shall be added in the

first EAP Response message of a full EAP exchange or in the EAP Initiate Re-auth message of the ERP Exchange. The Key-Request attribute shall contain the domain identification information. The AGW shall set domain identification information to the LinkID. If the HAAA supports ERP, and delivers a DSRK in a RADIUS Access-Accept message, the AGW shall derive the rRK and the rIK as specified in [37].

As part of the RADIUS Access-Accept message of the full EAP exchange, the AGW may send an attribute (ERP-Support) to the SRNC. The presence of this attribute indicates that the AGW is capable of acting as an ER server in the domain. When present, this attribute shall also contain the ERP domain name of the AGW. The SRNC can use this information to advertise the domain to the AT.

In addition to the parameters specified in EAP Access Authentication and authorization (see section 3.5.1), additional RADIUS Attributes between AGW and AAA for ERP are specified in Table 5 and additional RADIUS Attributes between AGW and SRNC for ERP are specified in Table 6.

Table 5. Additional RADIUS Attributes between AGW and AAA for Access Authentication and Authorization used for ERP

Attribute Name	Type	Access-Request	Access-Accept	Access-Challenge	Access-Reject
Key-Request	TBD[38]	0-1	0	0	0
Key-Response	TBD[38]	0	0-1	0	0

0 This attribute shall not be present.
0+ Zero or more instances of this attribute may be present.
0-1 Zero or one instance of this attribute may be present.
1 Exactly one instance of this attribute shall be present.
1+ One or more of these attributes shall be present.

Table 6. Additional RADIUS Attributes between AGW and SRNC for Access Authentication and Authorization used for ERP

Attribute Name	Type	Access-Request	Access-Accept	Access-Challenge	Access-Reject
ERP-Support	26/186	0	0-1	0	0

0 This attribute shall not be present.
0+ Zero or more instances of this attribute may be present.
0-1 Zero or one instance of this attribute may be present.
1 Exactly one instance of this attribute shall be present.
1+ One or more of these attributes shall be present.

The AGW shall also support transport of the rMSK to the eBS as specified in Table 7 for ERP.

The AGW shall support derivation of PMN-AN-RK2 from PMN-AN-RK for use when ERP is used. In this case, the AGW shall compute a PMN-AN-HA2 key and provide it, along with an SPI value through the PMN-AN-SPI attribute to the eBS as specified in Table 7. The 4 MSBs of the SPI field indicate the algorithm to compute the MN-HA Authentication extension. The AGW shall set 4 MSBs of the SPI field as specified in section 4.2. The AGW shall set the 28 LSBs of the SPI field to a unique value between 2^27 to 2^28-1 (i.e., the AGW shall set the 5th MSB of SPI field to '1'.) The eBS uses the PMN-AN-HA2 key to protect PMIP Signaling through the MN-HA authentication extension. The MN-HA authentication extension includes the SPI value provided by the AGW through ERP operation. The AGW shall compute the PMN-AN-RK2 and PMN-AN-HA2 key as follows:

PMN-AN-RK2 = HMAC-SHA-256 (PMN-AN-RK, “PM-AN-RK2”)

PMN-AN-HA2 Key = HMAC-SHA-256 (PMN-AN-RK2, “Derived PMIP Key”, sequence, eBS IP Address, AGW IP Address)

The RADIUS attributes that are sent between eBS and AGW for ERP are specified in Table 7.

Table 7. RADIUS Attributes between eBS and AGW for ERP

Attribute Name	Type	Access-Request	Access-Accept	Access-Challenge	Access-Reject
User-Name	1	1	0-1	0	0
NAS-IP-Address	4	0-1 Note 1	0	0	0
Class	25	0	0-1	0	0
NAS-Identifier	32	0-1	0	0	0
EAP-Message	79	1+	1+	1+	1+
Message-Authenticator	80	1	1	1	0
NAS-IPv6-Address	95	0-1 Note 1		0	0
MS-MPPE-Send-Key	26/16 (Vendor Type = 311)	0	1	0	0
MS-MPPE-Recv-Key	26/17 (Vendor Type = 311)	0	1	0	0
AAA-Session-ID	26/180	1	1	1	0
PMN-AN-SPI	26/187	0	0-1	0	0
PMN-AN-HA2	26/188	0	0-1	0	0

0 This attribute shall not be present.
0+ Zero or more instances of this attribute may be present.
0-1 Zero or one instance of this attribute may be present.
1 Exactly one instance of this attribute shall be present.
1+ One or more of these attributes shall be present.
Note 1: At least one of NAS-IP-Address or NAS-IPv6-Address shall be included.

5.4.2 Diameter

If Diameter is used, the AGW shall follow the requirements as specified in this section. Diameter Application ID shall be set to 16777247 (3GPP2 CAN Access Authentication and Authorization).

If the AGW supports ERP, the AGW shall support encapsulation of ERP messages in Diameter, using [10]. The AGW shall request a DSRK from the HAAA by using a Diameter Key-Request AVP (Type TBD)[47] as part of the full EAP exchange or an ERP bootstrapping exchange. The Key-Request AVP shall be added in the first EAP Response message of a full EAP exchange or in the EAP Initiate Re-auth message of the ERP Exchange. The Key-Request AVP shall contain the domain identification information that is identical to the

information the SRNC advertises to the AT. The AGW shall set domain identification information to the LinkID. If a DSRK is available, the AGW shall derive the rRK and the rIK as specified in [37].

As part of the Diameter EAP Answer (with EAP Success) message of the full EAP exchange, the AGW may send an AVP (ERP-Support) to the SRNC. The presence of this AVP indicates that the AGW is capable of acting as an ER server in the domain. When present, this AVP shall also contain the ERP domain name of the AGW. The SRNC can use this information to advertise the domain to the AT.

In addition to the parameters specified in the EAP Access Authentication and authorization (see section 3.5.2), additional Diameter AVP between the AGW and AAA for ERP are specified in Table 8 and additional Diameter AVP between the AGW and SRNC for ERP are specified in Table 9.

Table 8. Additional Diameter AVPs between AGW and AAA during Access Authentication and Authorization using ERP

AVP Name	AVP Code	Diameter EAP Request	Diameter EAP Answer
Key-Request	TBD[47]	0-1	0
Key-Response	TBD[47]	0	0-1

0 This AVP shall not be present.
0+ Zero or more instances of this AVP may be present.
0-1 Zero or one instance of this AVP may be present.
1 Exactly one instance of this AVP shall be present.
1+ One or more of these AVPs shall be present.

Table 9. Additional Diameter AVPs between AGW and SRNC during Access Authentication and Authorization using ERP

AVP Name	AVP Code	Diameter EAP Request	Diameter EAP Answer
ERP-Support	5535/22	0	0-1

0 This AVP shall not be present.
0+ Zero or more instances of this AVP may be present.
0-1 Zero or one instance of this AVP may be present.
1 Exactly one instance of this AVP shall be present.
1+ One or more of these AVP shall be present.

The AGW shall also support transport of the rMSK to the eBS as specified in Table 10 for ERP.

The AGW shall support derivation of PMN-AN-RK2 from PMN-AN-RK for use when ERP is used. In this case, the AGW shall compute a PMN-AN-HA2 key and provide it, along with an SPI value through PMN-AN-SPI AVP to the eBS as specified in Table 10. The 4 MSBs of the SPI field indicate the algorithm to compute the MN-HA Authentication extension. The AGW shall set 4 MSBs of the SPI field as specified in section 4.2. The AGW shall set the 28 LSBs of the SPI field to a unique value between 2^27 to 2^28-1 (i.e., the AGW shall set the 5th MSB of SPI field to '1'.) The eBS uses the PMN-AN-HA2 key to protect PMIP signaling through the MN-HA authentication extension. The MN-HA authentication extension includes the SPI value provided by the AGW. The AGW shall compute PMN-AN-RK2 and PMN-AN-HA2 key as follows:

PMN-AN-RK2 = HMAC-SHA-256 (PMN-AN-RK, “PMN-AN-RK2”)

PMN-AN-HA2 = HMAC-SHA-256 (PMN-AN-RK2, “Derived PMIP Key”, sequence, eBS IP Address, AGW IP Address)

The Diameter AVPs that are sent between eBS and AGW for ERP support are specified in Table 10.

Table 10. Diameter AVPs between eBS and AGW for ERP

AVP Name	AVP Code	Diameter EAP Request	Diameter EAP Answer
User-Name	1	1	0-1
NAS-IP-Address	4	0-1 Note 1	0
Class	25	0	0-1
Session-Timeout	27	0	1
NAS-Identifier	32	0-1	0
NAS-IPv6-Address	95	0-1 Note 1	
Session-ID	263	1	1
EAP-Payload	462	1+	1+
EAP-Master-Session-Key	464	0	1
AAA-Session-ID	5535/17	1	1
PMN-AN-SPI	5535/23	0	0-1
PMN-AN-HA2	5535/24	0	0-1

0 This AVP shall not be present.
0+ Zero or more instances of this AVP may be present.
0-1 Zero or one instance of this AVP may be present.
1 Exactly one instance of this AVP shall be present.
1+ One or more of these AVPs shall be present.
Note 1: At least one of NAS-IP-Address or NAS-IPv6-Address shall be included.

5.5 HAAA Requirements

The HAAA may support ERP as specified in [37]. If the HAAA supports ERP, it shall support the requirements as specified in this section.

The HAAA shall support the EMSK-based key hierarchy as specified in [39].

5.5.1 RADIUS

If RADIUS is used, the HAAA shall support the DSRK RADIUS Key-Request attribute. The HAAA shall derive the DSRK and send it in the RADIUS Access-Accept message along with the MSK to the AGW. The DSRK and the DSRK lifetime are transported using the RADIUS Key-Response attribute. The lifetime of the DSRK shall not be more than that of the EMSK.

In addition to the parameters specified in EAP Access Authentication and authorization (see section 3.6.1), the HAAA shall support parameters as specified in Table 5.

5.5.2 Diameter

If Diameter is used, the HAAA shall support the Diameter Key-Request AVP. Diameter Application ID shall be set to 16777247 (3GPP2 CAN Access Authentication and Authorization). The HAAA shall derive the DSRK and send it in the Diameter EAP Answer command along with the MSK to the SRNC. The DSRK and the DSRK lifetime are transported using the Diameter Key-Response AVP. The lifetime of the DSRK shall not be more than that of the EMSK.

In addition to the parameters specified in EAP Access Authentication and authorization (see section 3.6.2), the HAAA shall support parameters as specified in Table 8.

5.6 RAN PMIP4 Tunnel Operation

If the ERP is used, the procedures specified in section 4 shall apply except for using the PMN-AN-RK2 and PMN-AN-HA2 key instead of PMN-AN-RK1 and PMN-AN-HA1 key for the RAN PMIP4 tunnel security association.

6 Simple IPv4 Operation

This section specifies the requirements for Simple IPv4 Operation.

6.1 Protocol Stack

Figure 11 shows the protocol reference model for Simple IPv4 service.

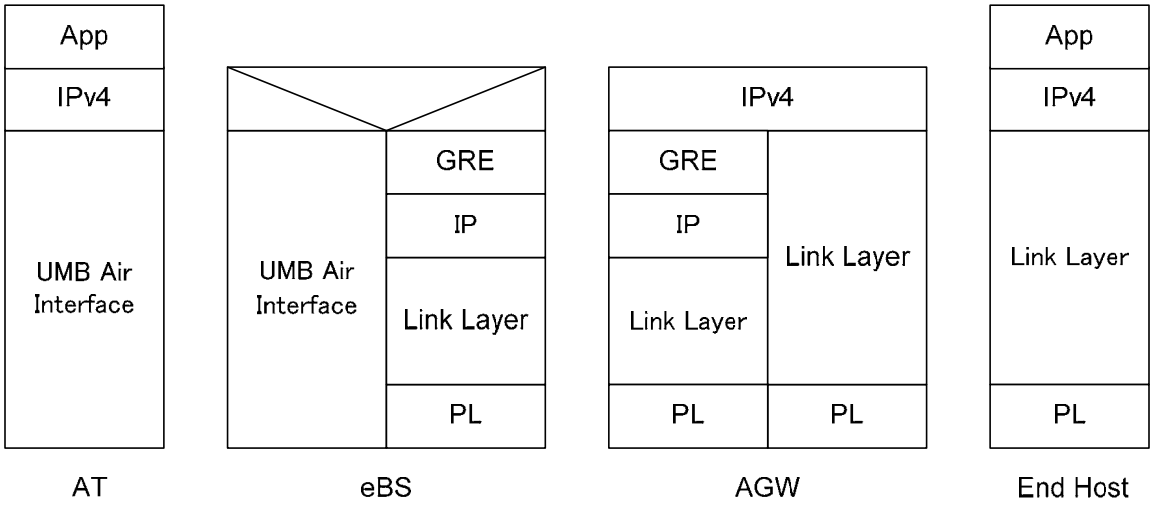


Figure 11. **Control and User Plane Protocol Stack for Simple IPv4 Operation**

6.2 AGW Requirements

The AGW shall support Simple IPv4 operation for Level 1 IP interface.

6.2.1 IP Address Assignment

The AGW shall support procedures for IP address assignment as defined in [18] and [19]. The procedures for the AGW as the DHCP server are described in this section.

If the Simple IPv4 service is not authorized (see section 3), the AGW shall silently discard the DHCP packets received from the AT on Level 1 IP interface; otherwise, the AGW shall perform the following:

If the AGW receives a DHCPDISCOVER with Rapid Commit option encapsulated with the GRE key for Level 1, the AGW shall send a DHCPACK to the AT if it successfully configures AT's requested configuration options. If not, the AGW shall send a DHCPNAK message to the AT.

If the AGW receives a DHCPDISCOVER without the Rapid Commit option encapsulated with the GRE key for Level 1, the AGW shall send a DHCPOFFER with offered configuration parameters.

If the AGW receives a DHCPREQUEST message from the AT 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 GRE Key through which the AGW received the DHCPREQUEST message. If the IP addresses are matched, the AGW shall send the DHCPACK to the AT using the same GRE key. If the IP addresses do not match, the AGW shall silently discard the DHCPREQUEST message.

All DHCP responses to the AT shall be encapsulated using the same GRE key (i.e. key associated with Level 1) as the corresponding DHCP messages.

All other DHCP or DHCP with Rapid Commit Option operations shall comply with [18] and [19].

6.2.2 IP Address Release

The AGW shall support procedures for IP address deallocation as defined in [18] and [19]. The procedures for the AGW as the DHCP server are described in this section.

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 GRE Key through which the AGW received a DHCPRELEASE message. If the IP addresses are matched, the AGW shall mark the assigned IP address as not allocated. If the IP addresses do not match, the AGW shall silently discard the DHCPRELEASE message.

When the IP address lease time expires, the AGW shall mark the assigned IP address as not allocated. The AGW shall discard packets to/from that IP address for the session.

If the AGW wants to release an assigned IP address before the IP address lease time expires, the AGW shall send a unicast DHCPFORCERENEW message to the AT as specified in [48]. Upon receiving DHCPREQUEST message from the AT, the AGW shall send DHCPACK message to the AT with ‘yiaddr’ set to all zero and IP address lease time to zero second.

6.2.3 DHCPv4 Support

The AGW shall act either as a DHCPv4 Relay Agent or a DHCPv4 server.

If the AGW acts as a DHCP Relay Agent, the AGW shall relay the DHCP messages between the DHCPv4 server and AT according to [20] [21]. The AGW shall include a DHCP Relay Agent Information option[21] when relaying DHCP messages to the server and shall set the giaddr field to the relay agent IP address. The AGW may support [22] to indicate the link on which the DHCP client (i.e., AT) resides if different from the link from which the agent is communicating with the server.

If the AGW acts as a DHCP Relay Agent and the same IP address has been assigned, e.g., by the CMIP4, to the AT for a different IP session, the AGW shall reject the IP address assignment by sending DHCPNACK. The previous assigned IP address is not affected.

If the AGW acts as a DHCP server, the AGW shall not assign the same IP address, e.g., by the CMIP4, that has been assigned to the AT for a different IP session.

If the AGW acts as a DHCP server, the AGW shall support both [18] and [19].

6.2.4 Ingress Address Filtering

The AGW shall check the source IP address of every packet received on the per AT tunnel between the eBS and AGW. Upon receiving packets from the AT with an invalid source IP address except for DHCP packets with IP address set to 0, the AGW shall discard the packets.

6.3 AT Requirements

The AT may support Simple IPv4 operation. If the AT supports Simple IPv4 operation, it shall follow the requirements described in this section. The AT shall perform its simple IPv4 operations on the proper IP interface associated with its Link Level's IP address. For simple IPv4 associated with Level 1 IP interface, the AT shall perform all its simple IPv4 operations on that IP interface.

6.3.1 IP Address Assignment

IP Address Assignment shall be performed with either DHCP [18] or DHCP with the Rapid Commit option [19].

6.3.1.1 DHCP with Rapid Commit Option

Upon a successful EAP Access authentication and per AT tunnel establishment between the eBS and AGW, the AT indicates to the upper layer that the link is up. If an application requests IPv4 Simple IP services, the AT shall send the DHCPDISCOVER message with Rapid Commit option to the AGW if the AT supports [19]. When the AT receives the DHCPACK with Rapid Commit, the AT shall configure its IP address with the IP address in the 'yiaddr' field.

If a lower layer handoff is performed and a different IP Interface is presented to the upper layer and an application still requires Simple IPv4 service, the AT shall send a DHCPDISCOVER message with Rapid Commit option to the AGW to reconfigure its IP address.

All other DHCP/DHCP with Rapid Commit Option operations shall comply with [18] and [19].

6.3.1.2 DHCP without Rapid Commit Option

Upon a successful EAP Access authentication and per AT tunnel establishment between the eBS and AGW, the AT presents an IP Interface to the upper layer. If an application requests IPv4 Simple IP services, the AT shall broadcast the DHCPDISCOVER message to the AGW if the AT does not support [19]. After the AT receives the DHCPOFFER message from the AGW, the AT shall send the DHCPREQUEST message with the 'server identifier' option. The 'requested IP address' option shall be set to the value of 'yiaddr' contained in the DHCPOFFER message from the AGW. The AT may include other options specifying desired configuration values. When the AT receives the DHCPACK message from the AGW, the AT shall configure its IP address with the IP address in the 'yiaddr' field.

If a lower layer handoff is performed and a different IP Interface is presented to the upper layer and an application still requires Simple IPv4 service, the AT shall follow the procedures specified in [18].

All other DHCP operations shall comply with [18].

6.3.2 IP Address Release

If the AT wants to release an assigned IP address before the IP address lease time expires, the AT shall send the DHCPRELEASE message to the AGW.

If the IP address lease time expires and the AT no longer requires Simple IPv4 services, the AT shall silently release the assigned IP address.

Upon receiving DHCPFORCERENEW message from the AGW (see [48]), the AT shall send DHCPREQUEST message to the AGW to renew the IP address. Upon receiving DHCPACK message with 'yiaddr' set to all zero and/or IP address lease time set to zero second, the AT shall treat the previous assigned IP address as invalid IP address.

6.3.3 DHCPv4 Support

The AT shall support [18] and may support [19].

7 Simple IPv6 Operation

This section specifies the requirements for Simple IPv6 Operation.

7.1 Protocol Stack

Figure 12 shows the protocol reference model for Simple IPv6 service.

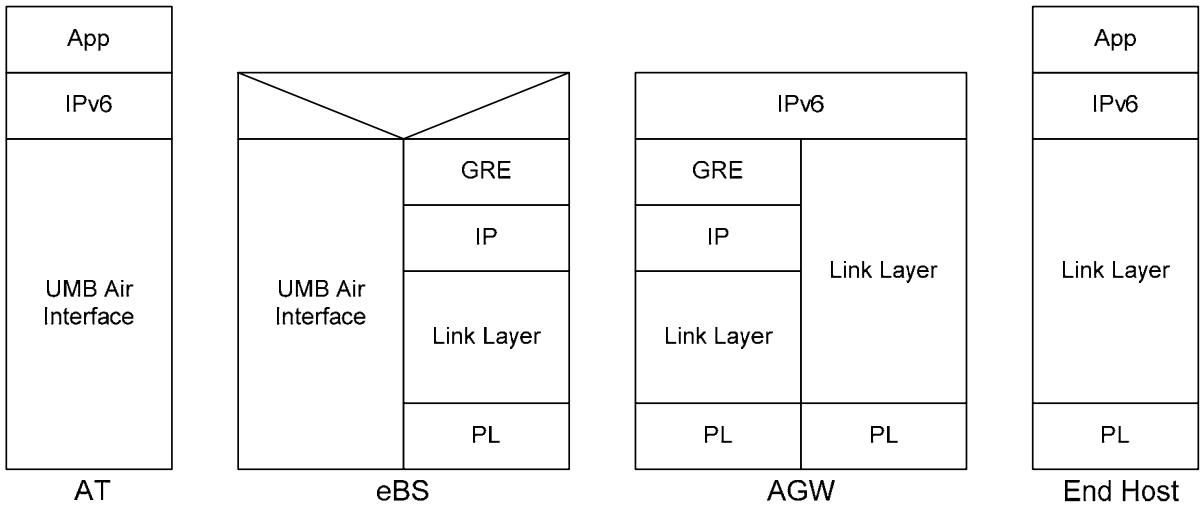


Figure 12. **Control and User Plane Protocol Stack for Simple IPv6 Operation**

7.2 Common Service Specification

The common requirements for the AGW and AT are described here.

The AGW and AT shall use IPv6 Stateless Address Auto-configuration [23] for IP address assignment and release for Simple IPv6 operation.

For Simple IPv6 operation, the following RFCs shall be supported:

- IPv6 Aggregatable Global Unicast Address Format [24],
- Internet Protocol, Version 6 (IPv6) [25],
- Neighbor Discovery for IP Version 6 [26],
- IPv6 Stateless Address Auto-configuration [27],
- Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification [28],
- IP Version 6 Addressing Architecture [29].

7.3 AGW Requirements

The AGW shall support Simple IPv6 operation for Level 1 interface.

7.3.1 IP Address Assignment

The AGW shall act as an IPv6 default router. The AGW shall select an interface ID which is within the range between 0000:0000:0000:0002 and 0000:0000:0000:FFFF and construct its link-local IPv6 address by pre-pending the link-local prefix FE80:: /64 [29] to this interface identifier. How the AGW selects the interface ID form the range is beyond the scope of this document.

If the AGW receives the Router Solicitation message from the AT encapsulated with the GRE key for the Level 1 IP interface, the AGW shall send the IPv6 Router Advertisement message [26] to the AT with the source IP address set to the AGW's link local IPv6 address and destination address set as specified in [26]. If Simple IPv6 is authorized, the AGW shall assign a unique prefix to the link for the AT. Based on policy, the AGW may send a Route Advertisement to the AT without the AT's solicitation.

Upon receiving the Router Solicitation message from the AT, if Simple IPv6 is not authorized, the AGW shall send Router Advertisement message by setting prefix to all 0s.

The AGW may receive the Router Solicitation message before the Prefix Valid Life time expires; if so, the AGW shall send a Router Advertisement message to the AT. If the AGW assigns a different unique Prefix from the previous prefix assigned, the AGW shall maintain both Prefixes until the Prefix Valid Life time for the previous prefix expires.

All Router Advertisements to the AT will be encapsulated using the same GRE key (i.e. key associated with Level 1) as the corresponding Router Solicitation messages.

7.3.2 IP Address Release

If the Prefix Valid Life time expires, the AGW shall release the assigned Prefix for the AT. The AGW shall discard packets to/from those IP addresses with the assigned Prefix for the session.

If the AGW wants to release an assigned prefix before the Prefix Valid Life time expires, the AGW shall send Router Advertisement message to the AT by setting the prefix to the currently assigned prefix with Prefix Valid Life time set to zero.

7.3.3 Stateless DHCPv6 Support

The AGW shall act either as a DHCPv6 Relay Agent or a Stateless DHCPv6 server.

If the AGW acts as a DHCPv6 Relay Agent, the AGW shall relay the DHCPv6 messages between the DHCPv6 server and AT as specified in [30].

If the AGW acts as a Stateless DHCPv6 server, the AGW shall support [31].

7.3.4 Ingress Address Filtering

The AGW shall check the prefix of the source IP address of every packet received on the per AT tunnel between the eBS and AGW. If the prefix of the source IP address is not assigned to the AT, the address is considered invalid. Upon receiving packets from an AT with an invalid prefix of the source IP address, the AGW shall discard the packets. If the source address is the IPv6 unspecified address and the message type is Neighbor Solicitation for Duplicate Address Detection (DAD), then the AGW shall silently discard the packet received from the AT. If the source address is the IPv6 unspecified address for purposes other than DAD or the source address is the AT's IPv6 link-local address, the AGW shall respond according to [26].

7.4 AT Requirements

The AT may support Simple IPv6 operation. If the AT supports Simple IPv6 operation, it shall follow the requirements described in this section. The AT shall perform its simple IPv6 operations on the proper IP interface associated with its Link Level's IP address. For simple IPv6 associated with Level 1 IP interface, the AT shall perform all its simple IPv6 operations on that IP interface.

7.4.1 IP Address Assignment

IP Address Assignment shall be performed with IPv6 Stateless Address Auto-configuration [27].

The AT shall select an interface ID which is not within the range between 0000:0000:0000:0000 and 0000:0000:0000:FFFF and construct its link-local IPv6 address by pre-pending the link-local prefix FE80:: /64 [29] to this interface identifier. The AT may support the Privacy Extensions for Stateless Address Autoconfiguration in IPv6 [32]. How the AT selects the interface ID from the range above is beyond the scope of this document.

Upon a successful initial EAP authentication and per AT tunnel establishment between the eBS and AGW, the AT presents an IP Interface to the upper layer (see [3]). If an application requests IPv6 Simple IP services, the AT shall send a Router Solicitation message as specified in [26].

After the AT receives a Router Advertisement message from the AGW, the AT shall construct a global IPv6 address by pre-pending the prefix in the Router Advertisement to the interface identifier generated by the AT. The AT shall send the Neighbor Advertisement message to the AGW containing its global IPv6 address in the Target address field of the Neighbor Advertisement message. Since the prefix assigned to the AT is globally unique and exclusive to the link, the AT should not perform the Duplicate Address Detection.

If a lower layer handoff is performed and a different IP Interface is presented to the upper layer and an application still requires Simple IPv6 service, the AT shall send a Router Solicitation message as specified in [26].

Upon receiving the Router Advertisement message by setting prefix to all 0s, the AT shall consider that Simple IPv6 service is not authorized.

7.4.2 IP Address Release

If the Prefix Valid Life time expires and the AT no longer requires Simple IPv6 services, the AT shall release the assigned Prefix.

If the AT decides to release the assigned Prefix before the Prefix Valid Life time expires, the AT shall silently release the assigned Prefix.

Upon receiving the Router Advertisement message with prefix set to currently assigned prefix but the Prefix Valid Life time set to zero, the AT shall treat the previous assigned IPv6 prefix as invalid IPv6 prefix.

7.4.3 Stateless DHCPv6 Support

The AT shall support Stateless DHCPv6 [31]. The AT may use the Stateless DHCPv6 mechanism to obtain configuration information.

8 Session Management

8.1 HAAA Requirements

8.1.1 RADIUS

If RADIUS is used, the HAAA may send a RADIUS Disconnect-Request message (see [34]) to the AGW for administrative reason or some other reasons to clean up the AGW resource.

If the HAAA sends Disconnect-Request Message, the HAAA shall include the attributes as specified in Table 11 in the Disconnection-Request Message.

Table 11. RADIUS Messages used for Session Management between HAAA and AGW

Attributes	Type	Disconnect-Request	Disconnect-Response	Description
User-Name	1	1	0	Contains the user's NAI to be disconnected
Framed-IP-Address	8	0-1	0	Contained AT's IP address to be disconnected
NAS-Identifier	32	1	0	Contains the NAS-Identifier of the AGW as was sent in a RADIUS Access-Request message
Framed-Interface-Id	96	0-1	0	Contained AT's IPv6 Interface ID to be disconnected
Framed-IPv6-Prefix	97	0-1	0	Contained AT's IPv6 prefix to be disconnected
AAA-Session-ID	26/180	1	0	Uniquely identifies the session to be disconnected.

0+ Zero or more instances of this attribute may be present.
0-1 Zero or one instance of this attribute may be present.
1 Exactly one instance of this attribute shall be present.
1+ One or more of these attributes shall be present.

8.1.2 Diameter

If Diameter is used, the HAAA may send an Abort-Session-Request command (see [8]) to the AGW for administrative reason or some other reasons to clean up the AGW resource. Diameter Application ID shall be set to 16777247 (3GPP2 CAN Access Authentication and Authorization).

If the HAAA sends an Abort-Session-Request command, the HAAA shall include the AVPs as specified in Table 12 in the Abort-Session-Request Message in addition to the mandatory AVP specified in the [8].

Table 12. Diameter Command used for Session Management between HAAA and AGW

AVP	Type	Abort-Session-Request	Abort-Session-Answer	Description
User-Name	1	1	0	Contains the user's NAI to be disconnected
Framed-IP-Address	8	0-1	0	Contained AT's IP address to be disconnected
NAS-Identifier	32	1	0	Contains the NAS-Identifier of the AGW as was sent in a Diameter EAP Request
Framed-Interface-ID	96	0-1	0	Contained AT's IPv6 Interface ID to be disconnected
Framed-IPv6-Prefix	97	0-1	0	Contained AT's IPv6 prefix to be disconnected
AAA-Session-ID	5535/17	1	0	Uniquely identifies the session to be disconnected.

0+ Zero or more instances of this AVP may be present.
0-1 Zero or one instance of this AVP may be present.
1 Exactly one instance of this AVP shall be present.
1+ One or more of these AVPs shall be present.

8.2 AGW Requirements

8.2.1 RADIUS

Upon receiving a RADIUS Disconnect-Request message, the AGW shall follow the procedures specified in [34]. The AGW shall release all IP Sessions associated with user identified by the identification attributes included in RADIUS Disconnect-Request message and described in Table 11. The AGW shall send MIP Registration Revocation message to the Primary PMIP tunnel binding or Signaling Only PMIP binding end point following the procedures in section 4. Upon receiving MIP Registration Revocation Acknowledgment message from the Primary or Signaling Only PMIP tunnel binding end point, the AGW shall send a RADIUS Disconnect-Ack message to the HAAA.

8.2.2 Diameter

Diameter Application ID shall be set to 16777247 (3GPP2 CAN Access Authentication and Authorization).

Upon receiving a Diameter Abort-Session-Request Command, the AGW shall follow the procedures specified in [8]. The AGW shall release all IP Sessions associated with the user identified by the identification AVPs included in Diameter Abort-Session-Request Command and described in Table 12. The AGW shall send MIP Registration Revocation Message to the Primary PMIP tunnel binding or Signaling Only PMIP binding end point following the

procedures specified in Section 4. Upon receiving MIP Registration Revocation Acknowledgment message from the Primary or Signaling Only PMIP tunnel binding end point, the AGW shall send Diameter Abort-Session-Answer Command to the HAAA.

9 LinkID Format

Globally Unique LinkID shall be set as specified in Figure 13.

Version (4 bits)	MCC (12 bits)	MNC (12 bits)	level (3 bits)	ID (33 bits)

Where:

Version: the version number of LinkID format. Version shall be set to ‘0000’ in this release.

MCC: Mobile Country Code. It shall be coded as specified in [3].

MNC: Mobile Network Code: It shall be coded as specified in [3].

Level: The Link Level associated with this LinkID. It shall be set to a value of 1 or 2.

ID: The identity of FHR unique within MCC and MNC domain.

Figure 13. **LinkID Format**

The LinkID Level supports two values – Level 1 and Level 2. The Level 1 LinkID corresponds to the AGW that serves as the first hop router to the AT, while the Level 2 LinkID corresponds to the LMA/HA that also serves as the first hop router, for a different interface of the AT.

Figure 14 describes the levels of LinkID associated with an AT. AT1 has two LinkIDs associated with it. The Level 1 LinkID corresponds to AGW-b while the Level 2 LinkID corresponds to LMA/HA-a. AT2 also has two LinkIDs. The Level 1 LinkID corresponds to AGW-c while the Level 2 LinkID corresponds to LMA/HA-a.

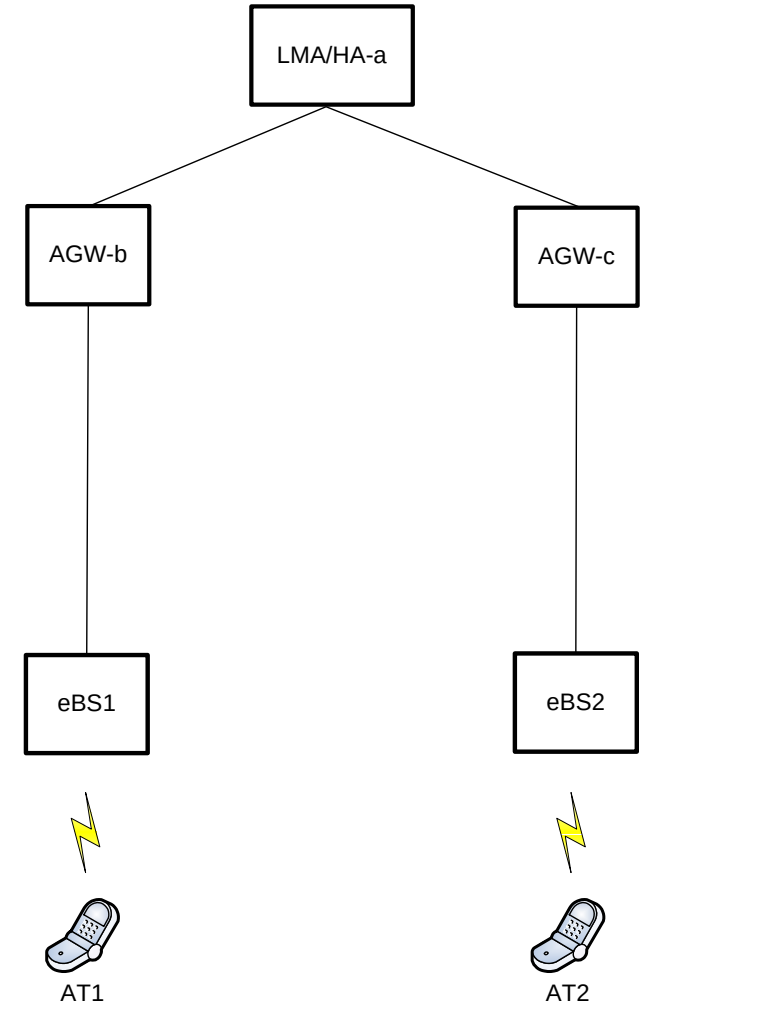


Figure 14. **Levels of LinkID**

10 Call Flows

10.1 Access Authentication and Authorization

Figure 15 illustrates an example call flow for access authentication and authorization.

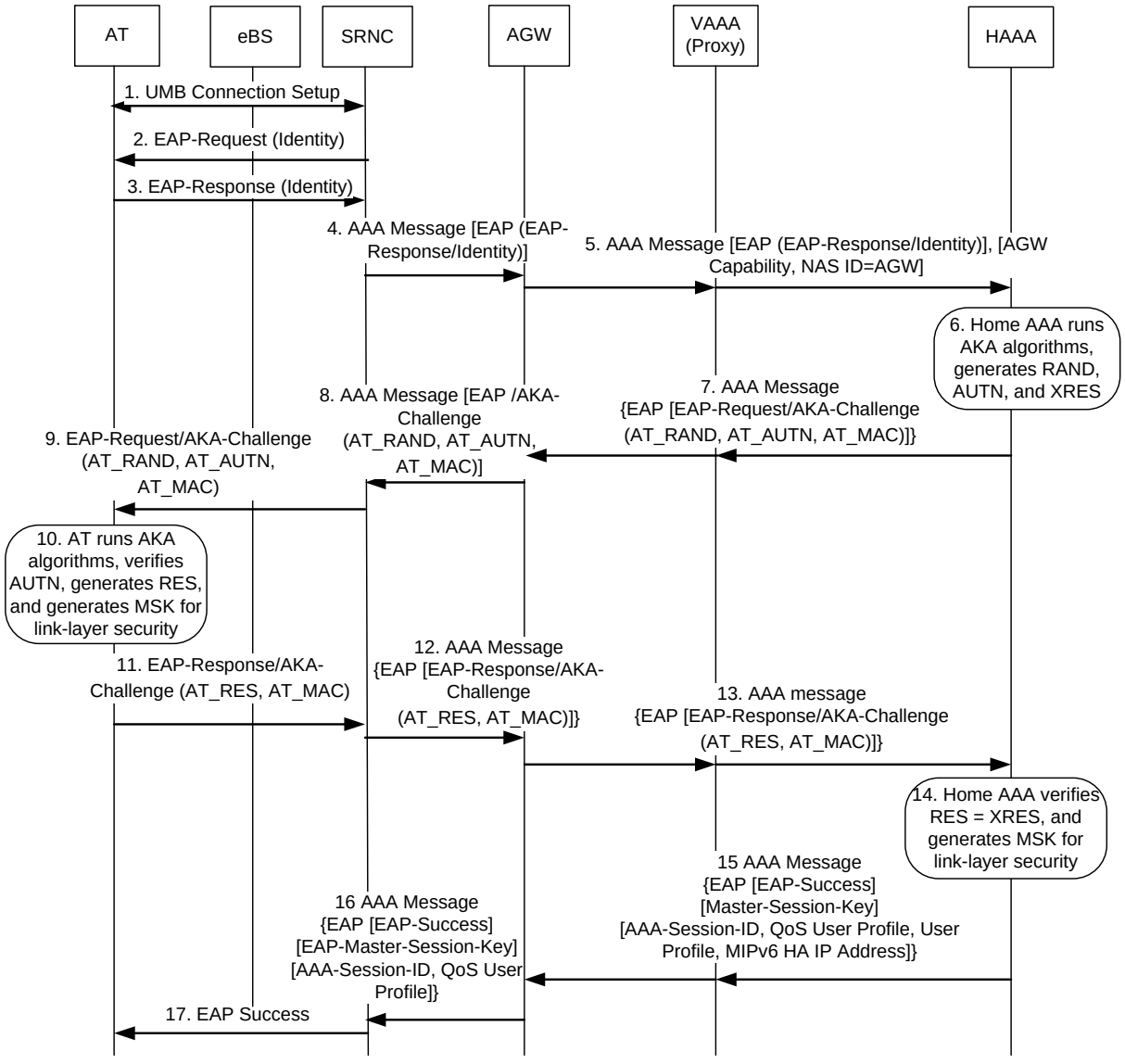


Figure 15. **Initial Access Authentication and Authorization**

The steps in Figure 15 are described below.

1. The AT sets up a UMB connection with an SRNC tunneled through the eBS. See the details in [3] and [4].
2. Upon successful connection and session establishment, the SRNC sends an EAP-Request/Identity message to the AT to query the identity of the user.

3. The AT sends an EAP-Response/Identity message to the SRNC containing the identity (NAI, see [33]) of the user.

4. The SRNC selects an AGW and forwards the AT's EAP-Response/Identity message to the AGW by encapsulating the EAP-Response/Identity message within the EAP Message attribute or EAP-Payload AVP, as a AAA Message (RADIUS Access-Request or Diameter-EAP-Request) to the AGW (see [10]). In the AAA Message (RADIUS Access-Request or Diameter-EAP-Request message), the SRNC sets NAS ID to SRNC ID.

5. The AGW adds its (AGW's) capabilities, replace the NAS-Identifier with the AGW's identifier, and sends a AAA Message (RADIUS Access-Request or Diameter-EAP-Request) to the HAAA.

6. Based upon a pre-shared key (agreed to beforehand by the user's identity module and the Home AAA) and a sequence number, the Home AAA runs the AKA algorithms and generates an authentication vector comprising a random part RAND, an authenticator part AUTN used for authenticating the network to the user identity module, an expected result part XRES, a 128-bit session key for the integrity check IK, and a 128-bit session key for encryption CK. See [2] for details.

7. The Home AAA sends a AAA Message (RADIUS Access-Challenge or Diameter-EAP-Answer) to the AGW containing EAP message attribute or EAP-Payload which encapsulates the EAP-Request/AKA-Challenge message. The AKA-Challenge subtype contains the AT_RAND and AT_AUTN attributes which in turn contain the RAND and AUTN, respectively, generated by the Home AAA in Step 6. The AKA-Challenge subtype also contains the AT_MAC attribute which provides message integrity protection.

8. The AGW forwards an AAA Message (RADIUS Access-Challenge or Diameter-EAP-Answer) to the SRNC.

9. The SRNC sends the Home AAA's EAP-Request/AKA-Challenge message to the AT.

10. Based upon a pre-shared key (agreed to before hand by the user's identity module and the Home AAA) and a sequence number, the AT runs the AKA algorithms and verifies the AUTN contained in the EAP-Request/AKA-Challenge message that it received from the SRNC in Step 9. The AT also generates result RES, a 128-bit session key for the integrity check IK, and a 128-bit session key for encryption CK. See [RFC4187] for details. Finally, the AT generates the Master Session Key (MSK) using IK and CK. Additional keys such as a MIPv4 MN-AAA key is generated for protecting subsequent MIPv4 signaling messages (see <1>).

11. The AT sends an EAP-Response/AKA-Challenge message to the Home AAA via the SRNC. The AKA-Challenge subtype contains the AT_RES attribute which in turn contains the RES generated by the AT in Step 10. The AKA-Challenge subtype also contains the AT_MAC attribute which provides message integrity protection.

12. The SRNC forwards the AT's EAP-Response/AKA-Challenge message to the AGW by encapsulating the EAP-Response/AKA-Challenge message in EAP Message attribute or EAP-Payload AVP of a AAA Message (RADIUS Access-Request or Diameter-EAP-Request message (see [10])).

13. The AGW forwards the AT's EAP-Response/AKA-Challenge message to the HAAA by encapsulating the EAP-Response/AKA-Challenge message in EAP Message attribute or EAP-Payload AVP of a AAA Message (RADIUS Access-Request or Diameter-EAP-Request message (see [10])).

14. The Home AAA verifies that RES = XRES (where XRES was generated by the Home AAA in Step 6). The Home AAA also generates the MSK using IK and CK (where IK and CK were generated by the Home AAA in Step 6). Additional keys such as a MIPv4 MN-AAA key may be generated for protecting subsequent MIPv4 signaling messages (see <1>).

15. The Home AAA sends a AAA Message (RADIUS Access -ccept or Diameter-EAP-Answer message) to the AGW containing an EAP-Success encapsulated in an EAP Message attribute or EAP-Payload AVP, the MSK, AAA-Session-ID, QoS User Profile, HA IP address etc. The MSK generated by the Home AAA in Step 14 and is specifically intended to deliver the MSK to the SRNC. The AAA-Session-ID is used by SRNC and AGW for the AAA session identification since a pseudonym-NAI may be used in AKA exchanges. The AAA-Session-ID is also used by SRNC for forming NAI contained in PMIP signaling between the eBS and AGW.

16. The AGW copies the informaiton it needs such as AAA-Session-ID and sends a AAA Message (RADIUS Access -Accept or Diameter-EAP-Answer message) to the SRNC containing an EAP-Success encapsulated in an EAP Message attribute or EAP-Payload AVP, the MSK, AAA-Session-ID, and a QoS User Profile etc. The AGW adds AGW-RAN-PMIP-Binding-Capability VSA/AVP to the AAA (RADIUS Access Accept or Diameter-EAP-Answer) message indicating the types of RAN PMIP bindings supported by the AGW.

17. The SRNC copies the VSAs/AVPs it needs, including the AGW-RAN-PMIP-Binding-Capability VSA/AVP received from the AGW, The SRNC sends EAP-Success to the AT.

10.1.1 Access Authentication and Authorization with R-UIM/CSIM

The Figure 16 illustrates an example call flow when the AKA algorithms are implemented on the R-UIM/CSIM part of the AT. The EAP terminates at the ME.

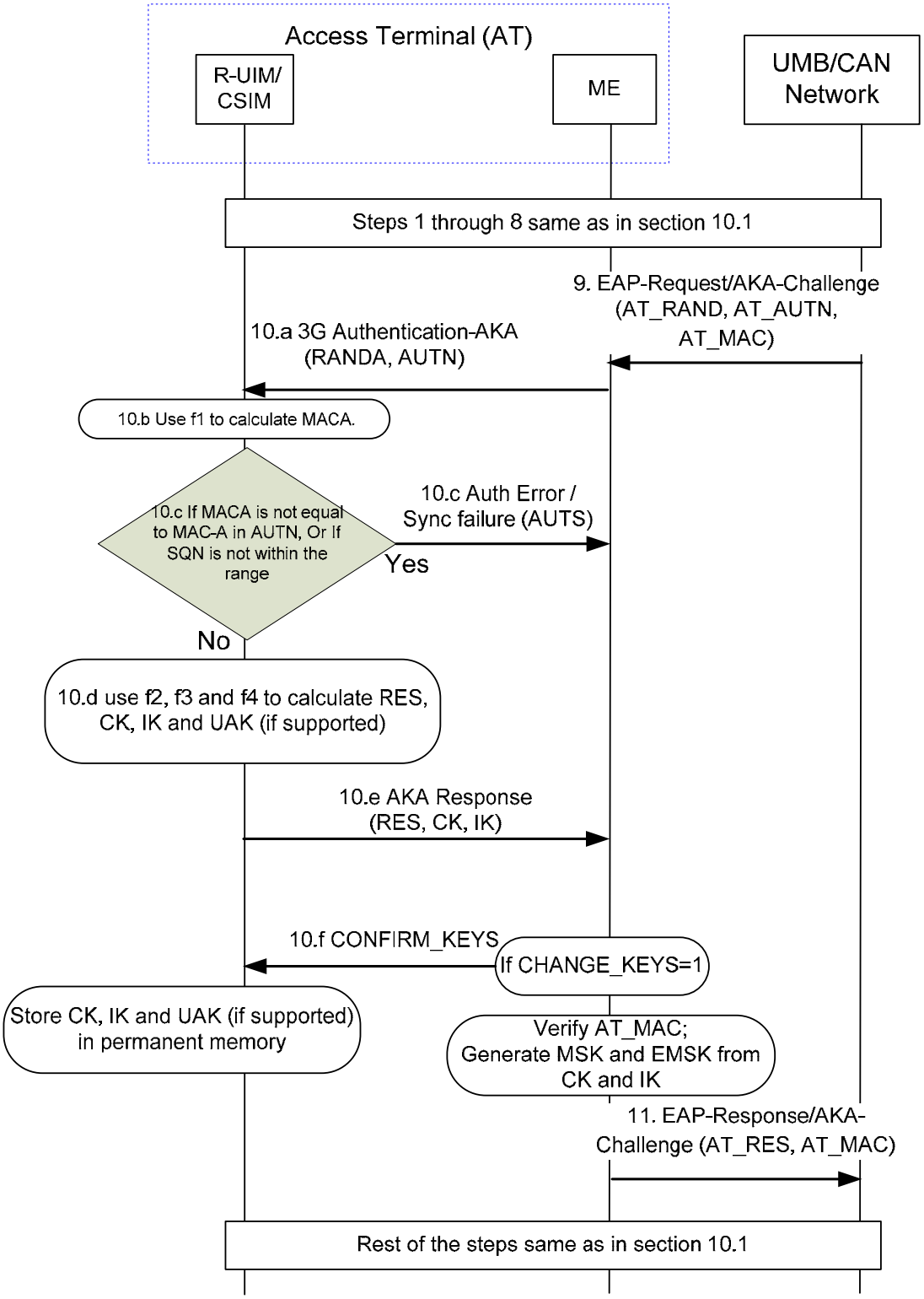


Figure 16. **Initial Access Authentication and Authorization with R-UIM/CSIM**

The steps in Figure 16 are described below.

1-8 The steps 1 through 8 are same as in section 10.1.

9. When the ME part of the AT receives the EAP-AKA Challenge from the UMB network (specifically from the SRNC), the ME extracts RANDA and the AUTN (RAND, AUTN may be optionally protected with the AKA Anonymity Key or AK) from the EAP message.

10. The step 10 in section 10.1 is further divided to illustrate the exchange between the ME and the R-UIM/CSIM.

    a. Then the ME issues 3G Authentication-AKA command to the R-UIM/CSIM over the R-UIM-ME/UICC-ME interface with RANDA and AUTN parameters.

    b. Using the pre-configured AKA root key (K) and AK (if available), the R-UIM/CSIM runs f1 to calculate MACA.

    c. If MACA is not equal to MAC-A present in the AUTN field, the R-UIM/CSIM sends network authentication error indication to the ME. Or if SQN in the AUTN field is not within the acceptable range of the SQN stored at the R-UIM/CSIM, the R-UIM/CSIM calculates resynchronization authentication token AUTS and sends synchronization failure message with AUTS to the ME. The AT follows the rest of procedures as specified in [2] for the failure the case (not shown in this figure.)

    d. If MACA is same as MAC-A present in the AUTN field, then the network authentication is successful. The R-UIM/CSIM proceeds to check whether the received SQN in the AUTN field is within the acceptable range of the SQN stored at the R-UIM/CSIM, the R-UIM/CSIM uses AKA functions to calculate RES (using f2), CK (using f3) and IK (using f4). Optionally, if supported, the R-UIM/CSIM may calculate the UAK (UIM Authentication Key).

    e. The R-UIM/CSIM sends AKA response with RES, CK and IK to the ME.

    f. The ME confirms the receipt of the keys to R-UIM/CSIM by issuing CONFIRM_KEYS command. Upon receiving this command, the R-UIM/CSIM stores the keys in it's permanent memory. The ME then proceeds to verify the AT-MAC parameter to ensure that the EAP message has not been tampered with in transit. If successful, the ME calculates the Master Session Key (MSK) and the Extended Master Session Key (EMSK) as specified in [2] and may store them securely in its non-volatile memory.

11. The ME sends an EAP-Response/AKA-Challenge message to the UMB network (specifically to SRNC). The AKA-Challenge subtype contains the AT_RES attribute which in turn contains the RES generated by the R-UIM/CSIM in Step 10.b. The AKA-Challenge subtype also contains the AT_MAC attribute which provides message integrity protection for the EAP message.

12. The rest of the message flows are same as in section 10.1.

10.2 PMIP Tunnel Operation

Figure 17 illustrates an example call flow for PMIP tunneling operation without multiple bindings and ERP is not used.

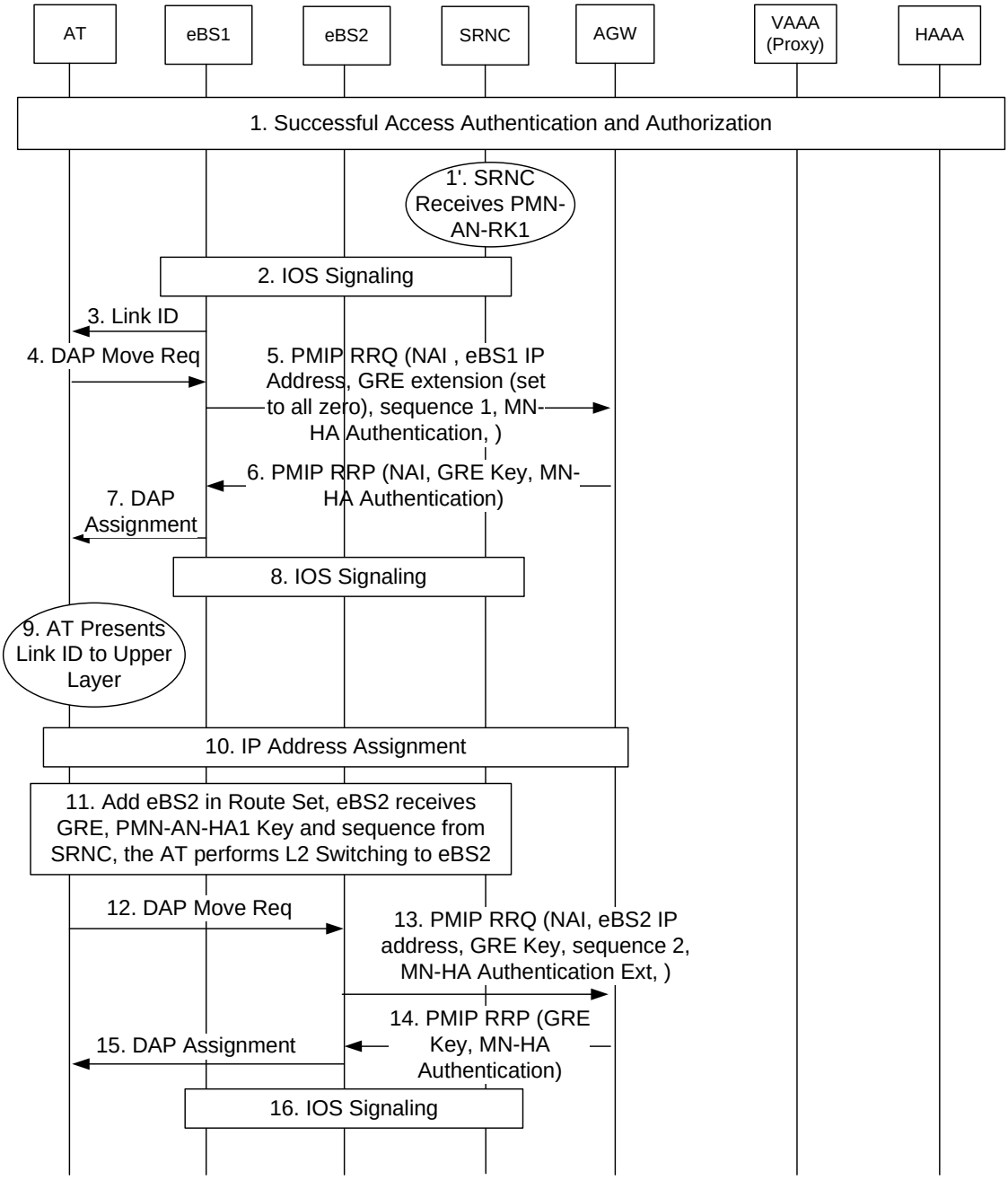


Figure 17. **PMIP Tunnel Operation (without multiple bindings)**

The steps in Figure 17 are described below.

1. The AT performs successful access authentication and authorization. The AGW receives AAA-Session-ID and other parameters from the HAAA. The AGW selects a unique random key called PMN-AN-RK for the AT and derives PMN-AN-RK1

from PMN-AN-RK. The AGW sends PMN-AN-RK1, AAA-Session-ID, and other parameters to the SRNC through EAP Access authentication and authorization procedures. The AGW adds AGW-RAN-PMIP-Binding Capability VSA/AVP to the AAA (RADIUS Access Accept or Diameter-EAP-Answer) message indicating the types of RAN PMIP bindings supported by the AGW (See access authentication and authorization call flow for details).

2. The eBS and SRNC performs IOS signaling exchanges in which the SRNC sends AGW IP Address, LinkID, User Name, AAA-Session-ID, and PMN-AN-HA1 key derived from PMN-AN-RK1 to the eBS1. The SRNC sends AGW-RAN-PMIP-Binding-Capability information also to the eBS1. The sequence value is also sent from the SRNC to the eBS1 (used for calculating PMN-AN-HA1 key in AGW.) (See [4] for the details.)

3. eBS1 presents the LinkID to the AT. The LinkID represents the IP interface that the AT creates to talk to the IP layer.

4. The AT sends DAP Move Request to the eBS1.

5. Since eBS1 does not have GRE key, eBS1 sends a PMIP RRQ (see [15]) to the AGW which includes GRE extension (set to all zero), NAI (formatted as AAA-Session-ID@Realm, where AAA-Session-ID is received from SRNC at step 2, and Realm is the Realm portion of User Name received from SRNC at step 2) and eBS1 IP address, and an MN-HA authentication extension calculated by using PMN-MN-HA1 key received from step 2. In the MN-HA Authentication extension, the SPI field contains sequence number as specified in [4]. The eBS1 does not request multiple bindings with the AGW because (a) eBS1 is not configured to support multiple bindings, and/or (b) the AGW-RAN-PMIP-Binding-Capability information indicates that the AGW does not support multiple bindings.

6. The AGW verifies MN-HA Auth extension by using the PMN-AN-HA1 key (PMN-AN-HA1 Key = HMAC-SHA-256 (PMN-AN-RK1, “Derived PMIP Key”, Sequence, eBS1 IP Address, AGW IP Address). If authentication passes, the AGW selects a GRE key associated with this NAI and includes it through a GRE extension (see [14]) in the PMIP RRP sent to eBS1.

7. eBS1 sends DAP Assignment to the AT.

8. The eBS1 sends DAP notification to SRNC and other eBSes in the route set through IOS signaling (see [4] for the details.)

9. The AT indicates to the IP layer that the link is up. The upper IP layer compares the IP Interface with its current IP Interface. If it is different, it triggers IP Address assignment.

10. The AGW and AT perform IP address assignment if AT requests an IP address. (See IP address assignment call flow.)

11. The AT adds eBS2 in the Route Set and performs L2 fast switching to eBS2. During this procedure, eBS2 receives AGW IP Address, GRE key, and PMN-AN-HA1 key and sequence from SRNC. The eBS2 receives AGW-RAN-PMIP-Binding-Capability information also for the SRNC. The PMN-AN-HA1 key received by eBS2 is different from the PMN-AN-HA1 key received by the eBS1 at step 2.

12. The AT sends DAP Move Request to eBS2 requesting DAP handoff.

13. eBS2 sends PMIP RRQ to the AGW including eBS2 IP address, and GRE Key received from step 11, and MN-HA authentication extension calculated by using PMN-AN-HA1 key received from step 11. In the MN-HA Authentication extension,

the SPI field contains sequence number as specified in [4]. The eBS2 does not request multiple bindings with the AGW because (a) eBS2 is not configured to support multiple bindings, and/or (b) the AGW-RAN-PMIP-Binding-Capability information indicates that the AGW does not support multiple bindings

14. The AGW verifies MN-HA Auth extension by using PMN-AN-HA1 key (PMN-AN-HA1 Key = HMAC-SHA-256 (PMN-AN-RK1, “Derived PMIP Key”, Sequence, eBS2 IP Address, AGW IP Address). If authentication passes, the AGW sends PMIP RRP to eBS2.
15. eBS2 sends DAP Assignment to the AT.
16. eBS2 sends DAP notification to SRNC and other eBSes in the Route Set through IOS signaling (see [4] for the details.)

10.3 PMIP Tunnel Operation with Multiple Binding

Figure 18 through Figure 24 illustrates example calls flow for PMIP tunneling operation with multiple binding.

10.3.1 PMIP Tunnel Operation for Initial Power Up

Figure 18 shows PMIP multiple binding updates for initial power up.

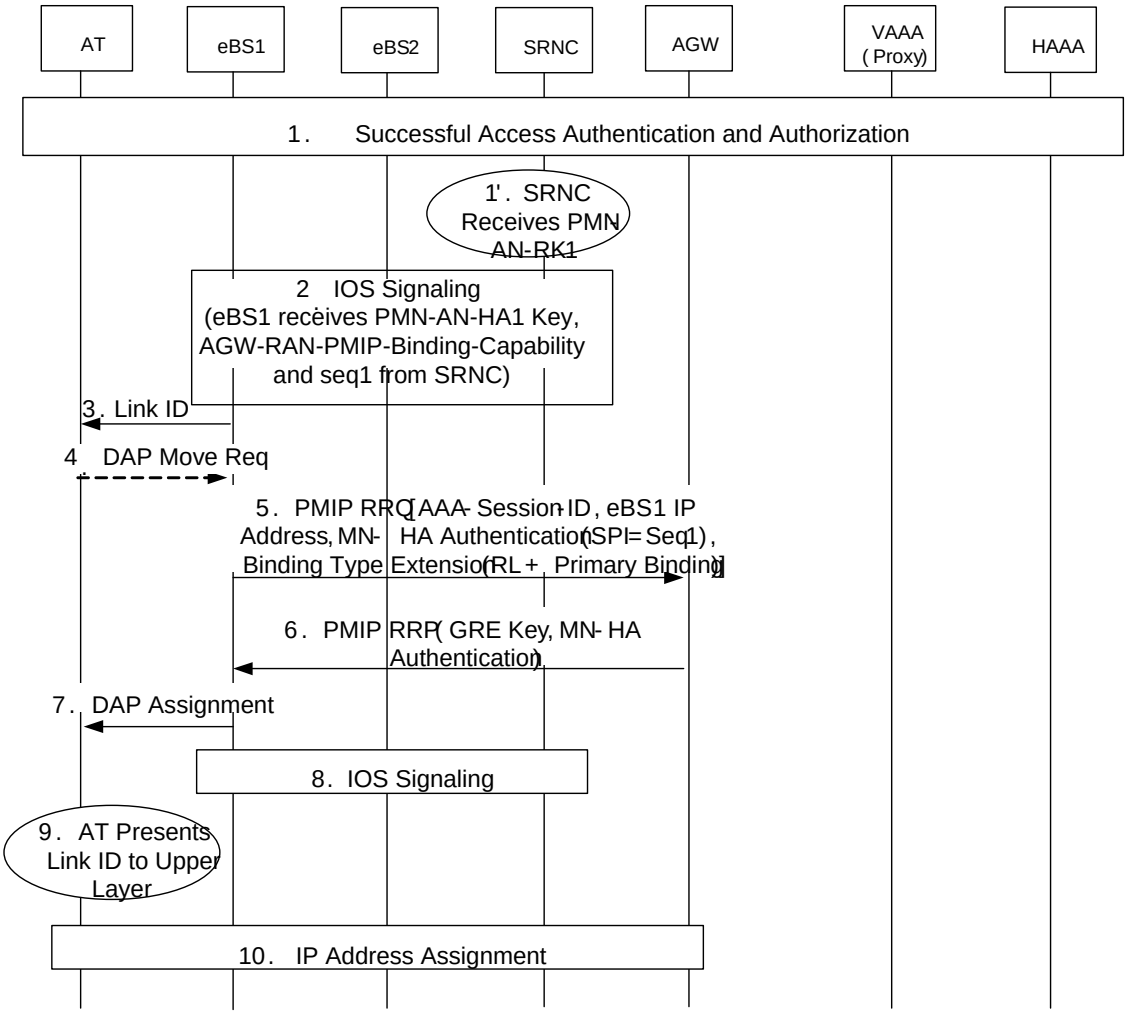


Figure 18. **PMIP Tunnel Operation with multiple bindings (Initial Power Up)**

The steps in Figure 18 are described below.

1. The AT , SRNC, AGW, and AAA perform successful access authentication and authorization as same as step 1 specified in section 10.2. The AGW is configured to support multiple RAN PMIP bindings and (possibly) RAN PMIP signaling only binding also. The AGW sends AGW-RAN-PMIP-Binding-Capability AVP with the appropriate setting of the vendor-value field to the SRNC.

2. The eBS and SRNC perform IOS signaling exchanges in which the SRNC sends AGW IP Address, AAA-Session-ID, User name and PMN-AN-HA1 key derived from PMN-AN-RK1 to eBS1. The SRNC sends AGW-RAN-PMIP-Binding-Capability information also to the AGW. The sequence number (Seq1) is also sent from the SRNC to eBS1 (used for calculating PMN-AN-HA1 key in AGW.) (See [4] for the details.)

3. eBS1 presents the LinkID to the AT. The LinkID represents the IP interface that the AT creates to talk to the IP layer.

4. This step is optional. For AT assisted DAP move, the AT sends DAP Move Request to the eBS1.

5. Since eBS1 does not have GRE key, eBS1 sends a PMIP RRQ (see [15]) to the AGW which includes GRE extension (set to all zero), eBS1 IP address, NAI (formatted as AAA-Session-ID@Realm, where AAA-Session-ID is received from SRNC at step 2, and Realm is the Realm portion of User Name received from SRNC at step 2)) and eBS1 IP address, and an MN-HA authentication extension calculated by using the PMN-AN-HA key received from step 2. In the MN-HA Authentication extension, the SPI field contains the sequence number as specified in [4]. eBS1 supports multiple RAN PMIP bindings, and the AGW-RAN-PMIP-Binding-Capability information indicates support of multiple RAN PMIP bindings at the AGW as well. The eBS1 requests establishment of Primary + RL PMIP bindings by including Binding Type Extension in the PMIP RRQ that indicates this PMIP Binding is for RL + Primary binding.

6. The AGW verifies MN-HA Auth extension by using the PMN-AN-HA1 key (PMN-AN-HA Key = HMAC-SHA-256 (PMN-AN-RK1, “Derived PMIP Key”, Seq1, eBS1 IP Address, AGW IP Address). If authentication passes, the AGW selects a GRE key as specified in section 4 associated with this AT and includes it in the GRE extension (see [14]) in the PMIP RRP sent to the eBS1. Since the PMIP RRQ includes a Binding Type Extension with RL and Primary indication, the AGW can send and receive packets to and from eBS1.

7. It occurs if step 4 is performed. eBS1 sends DAP Assignment to the AT.

8. eBS1 sends DAP notification to SRNC and other eBSs in the route set through IOS signaling (see [4] for the details.)

9. The AT indicates to the upper IP layer that the link is up. The upper IP layer compares the IP Interface with its current IP Interface. If it is different, it triggers an IP Address assignment.

10. The AGW and AT performs IP address assignment if the AT request for it. (See IP address assignment call flow.)

10.3.2 PMIP Tunnel Operation for Subsequent Route Adding or Connection Setup (Scenario 1)

Figure 19 shows PMIP multiple binding updates for subsequent route adding and DAP move. The same call flow also applies when the AT transitions to active from the idle state and establishes a connection with eBS2. The assumption is that the AGW and the eBS2 are configured to support multiple RAN PMIP bindings. This call flow shows RL binding and Primary binding in different steps.

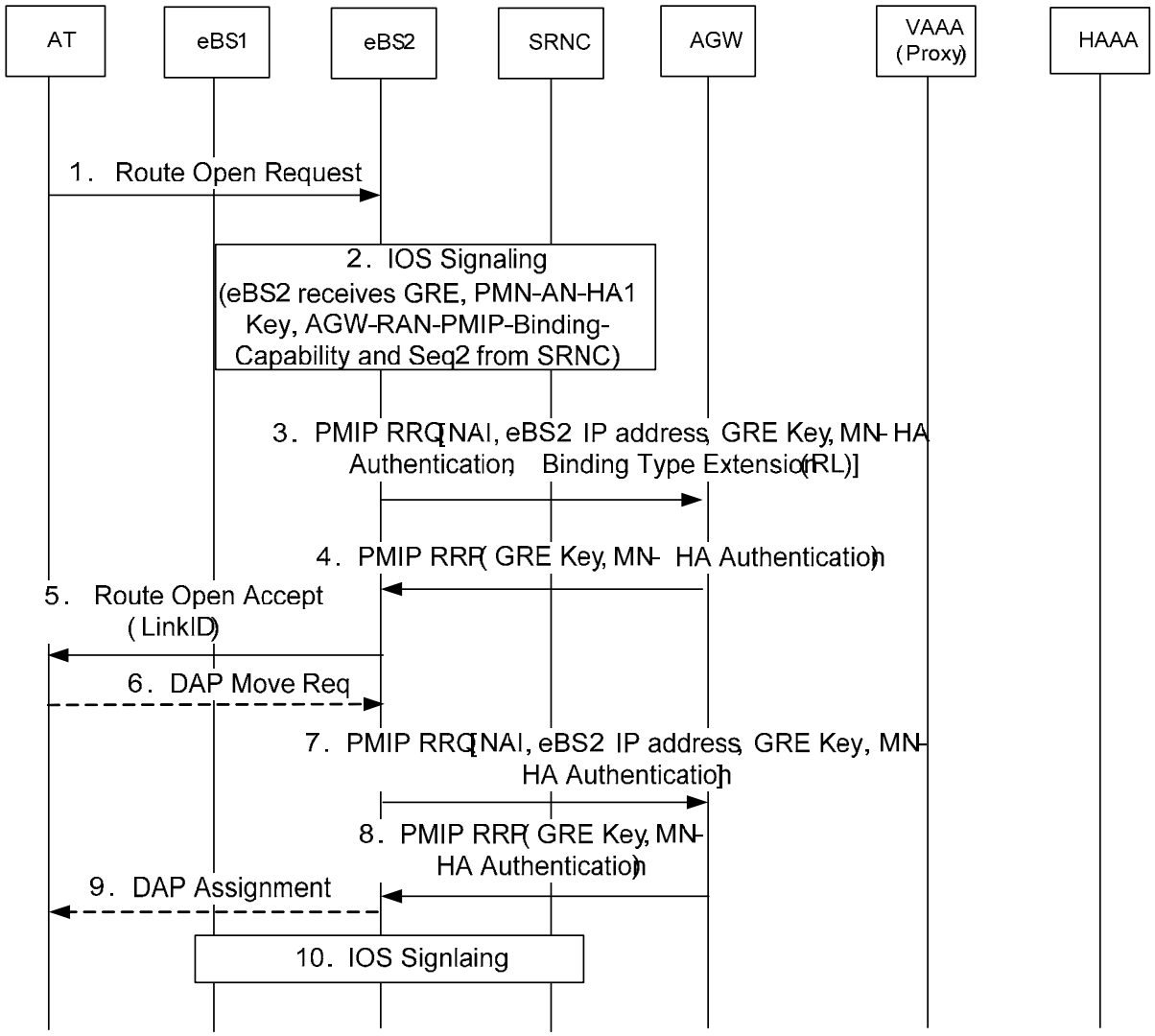


Figure 19. **PMIP Tunnel Operation with Connection Setup or Route Adding (Scenario 1)**

The steps in Figure 19 are described below.

1. The AT sends Route Open Request to eBS2.
2. During the IOS procedure, eBS2 receives AGW IP Address, User Name, AAA-Session-ID, GRE key, and PMN-AN-HA1 key sequence (Seq2) and AGW-RAN-PMIP-Binding-Capability information from the SRNC. (See [4] for the details.)
3. eBS2 sends a PMIP RRQ to the AGW including Binding Type Extension indicating RL only in addition to eBS2 IP address, NAI (formatted as AAA-Session-ID@Realm, where AAA-Session-ID is received from SRNC at step 2, and Realm is the Realm portion of User Name received from SRNC at step 2), GRE extension, and MN-HA authentication extension. In the MN-HA Authentication extension, the SPI field contains the sequence number as specified in [4].
4. The AGW verifies MN-HA Auth extension by using PMN-AN-HA1 key (PMN-AN-HA1 Key = HMAC-SHA-256 (PMN-AN-RK1, “Derived PMIP Key”, Seq2, eBS2 IP Address, AGW IP Address). If authentication passes, the AGW sends the PMIP

RRP to eBS2. Since PMIP RRQ includes the RL Only Extension, the AGW can only receive packets from eBS2.

5. eBS2 sends Route Open Accept to the AT. The LinkID represents the IP interface that the AT creates to talk to the IP layer. It is assumed LinkID is unchanged in this call flow.

6. Sometimes later, the AT sends a DAP Move Request to eBS2 requesting DAP handoff. This step is optional and is performed only for an AT assisted DAP move.

7. eBS2 sends a PMIP RRQ to the AGW including NAI, GRE Key and eBS2 IP address, and an MN-HA authentication extension. In the MN-HA Authentication extension, SPI field contains the sequence number as specified in [4].

8. The AGW verifies MN-HA Auth extension by using the PMN-AN-HA1 key (PMN-AN-HA1 Key = HMAC-SHA-256 (PMN-AN-RK1, “Derived PMIP Key”, Seq2, eBS2 IP Address, AGW IP Address). If authentication passes, the AGW sends a PMIP RRP to eBS2. Since the PMIP RRQ in previous step does not include a Binding Type Extension, the AGW treats it as a primary PMIP binding and it can receive and send packets from and to eBS2. Please note if the other eBSs in the Route Set has performed RL binding or RL+ Primary binding, the AGW treats other eBSs to be RL binding only at this time.

9. The eBS2 sends DAP Assignment to the AT. This step is optional and only is performed for AT assisted DAP move.

10. The eBS2 sends DAP notification to SRNC and other eBSes in the Route Set through IOS signaling (see [4] for the details.)

10.3.3 PMIP Tunnel Operation for Subsequent Route Adding or Connection Setup (Scenario 2)

Figure 20 shows PMIP multiple binding updates for subsequent route adding and DAP move. The same call flow also applies when the AT transitions to active from the idle state and establishes a connection with eBS2. The call flow assumes that the AGW and the eBS2 are configured to support multiple RAN PMIP bindings. This call flow shows a RL binding and Primary binding in the same step for the network initiated DAP move.

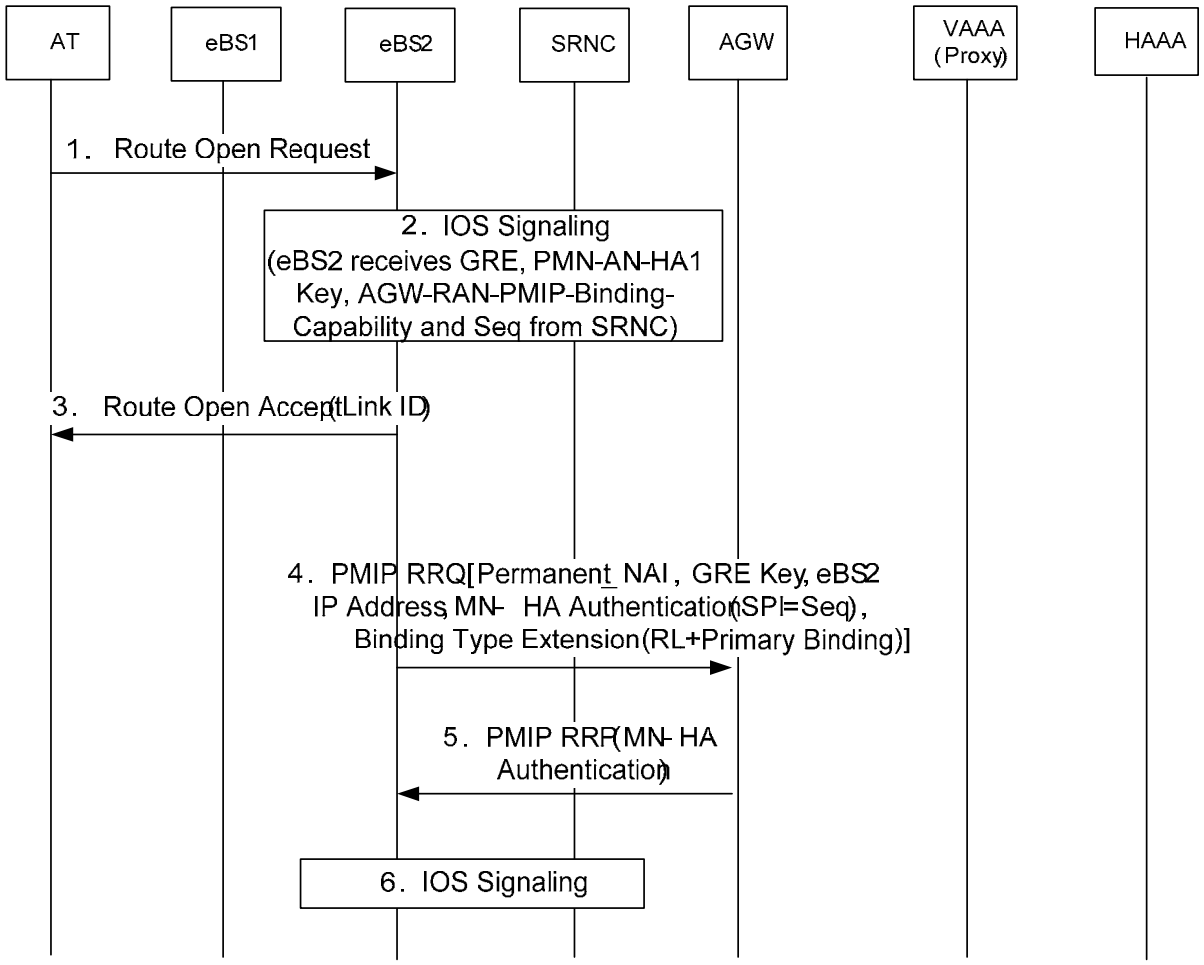


Figure 20. **PMIP Tunnel Operation with Connection Setup or Route Adding (Scenario 2)**

The steps in Figure 20 are described below.

1. The AT sends a Route Open message to eBS2.
2. eBS2 and the SRNC performs IOS signaling exchanges in which the SRNC sends session info including the AGW IP address, LinkID, User Name, AAA-Session-ID, GRE Key, and the PMN-AN-HA1 key derived from PMN-AN-RK1 and AGW-RAN-PMIP-Binding-Capability information to eBS2. The sequence number is also sent from the SRNC to eBS2 (used for calculating PMN-AN-HA1 key in AGW.) (See [4] for the details.)
3. eBS2 sends a Route Open Accept including LinkID to the AT. The LinkID represents the IP interface that the AT creates to talk to the IP layer. It is assumed LinkID is unchanged in this call flow.
4. eBS2 sends PMIP RRQ (see [15]) to the AGW which includes eBS2 IP address, NAI (formatted as AAA-Session-ID@Realm, where AAA-Session-ID is received from SRNC at step 2, and Realm is the Realm portion of User Name received from SRNC at step 2), GRE extension received from step 2, and the MN-HA authentication extension calculated by using PMN-AN-HA1 key received from step 2. In the MN-HA Authentication extension, the SPI field contains the sequence number as

specified in [4]. In the PMIP RRQ, the Binding Type Extension is also included to indicate that this PMIP Binding is for both a RL and Primary PMIP binding.

5. The AGW verifies the MN-HA Auth extension by using the PMN-AN-HA1 key (PMN-AN-HA1 Key = HMAC-SHA-256 (PMN-AN-RK1, "Derived PMIP Key", Seq2, eBS2 IP Address, AGW IP Address). If authentication passes, the AGW sends the PMIP RRP to eBS2. Since the PMIP RRQ includes Binding Type Extension with RL and primary binding, the AGW can send and receive packets to and from the eBS2.

6. eBS2 sends DAP notification to the SRNC and other eBSs in the route set through IOS signaling (see [4] for the details.)

10.3.4 PMIP Tunnel RL Deregistration

Figure 21 shows RL PMIP binding deregistration.

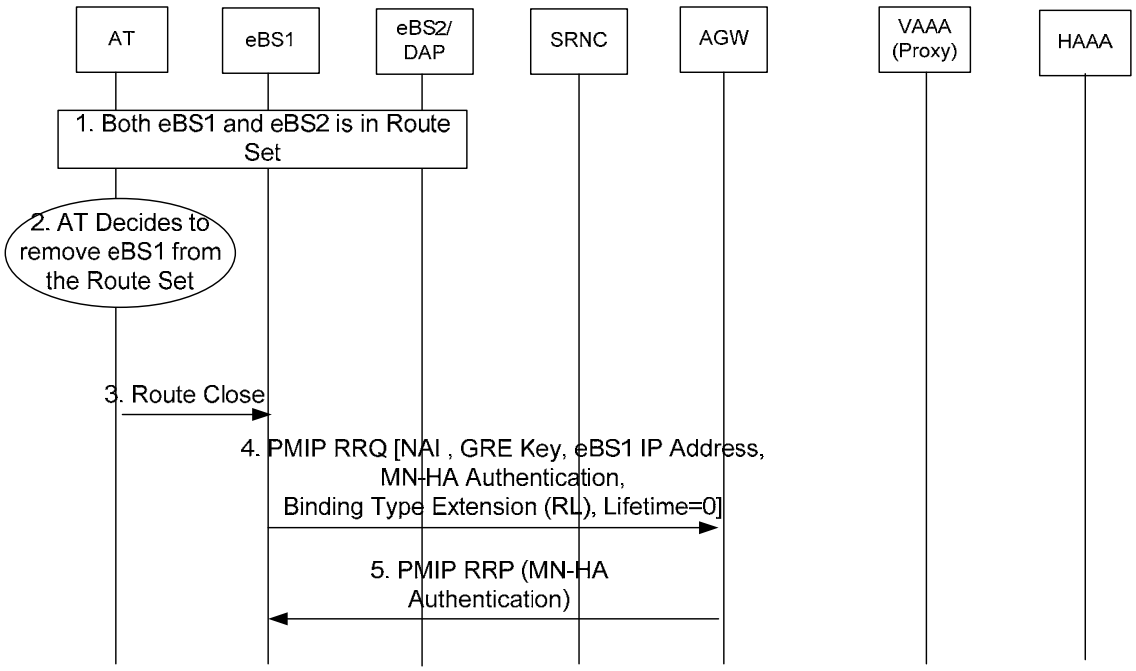


Figure 21. **RL PMIP Deregistration**

The steps in Figure 21 are described below.

1. eBS1 and eBS2 are in the AT's Route Set.

2. The AT decides to remove eBS1 from the Route Set.

3. The AT sends the Route Close to the eBS1.

4. eBS1 sends a PMIP RRQ (see [15]) with PMIP lifetime set to 0 and a Binding Type extension to the AGW to indicate this PMIP Binding is for RL binding deregistration.

5. The AGW verifies MN-HA Auth extension. If authentication passes, the AGW sends a PMIP RRP to eBS1. Since PMIP RRQ includes RL Extension lifetime equal to 0, the AGW stop accepting the packets from the eBS1.

10.3.5 Signaling Only PMIP-Registration for Multiple PMIP Binding Case

Figure 22 illustrates a successful Signaling Only PMIP binding registration sequence. The Signaling Only PMIP binding registration happens when both the SRNC and the AGW are configured to support Signaling Only binding, and the AT moves from the Active state to Idle state. Idle state is triggered when all routes between the AT and eBS's are closed.

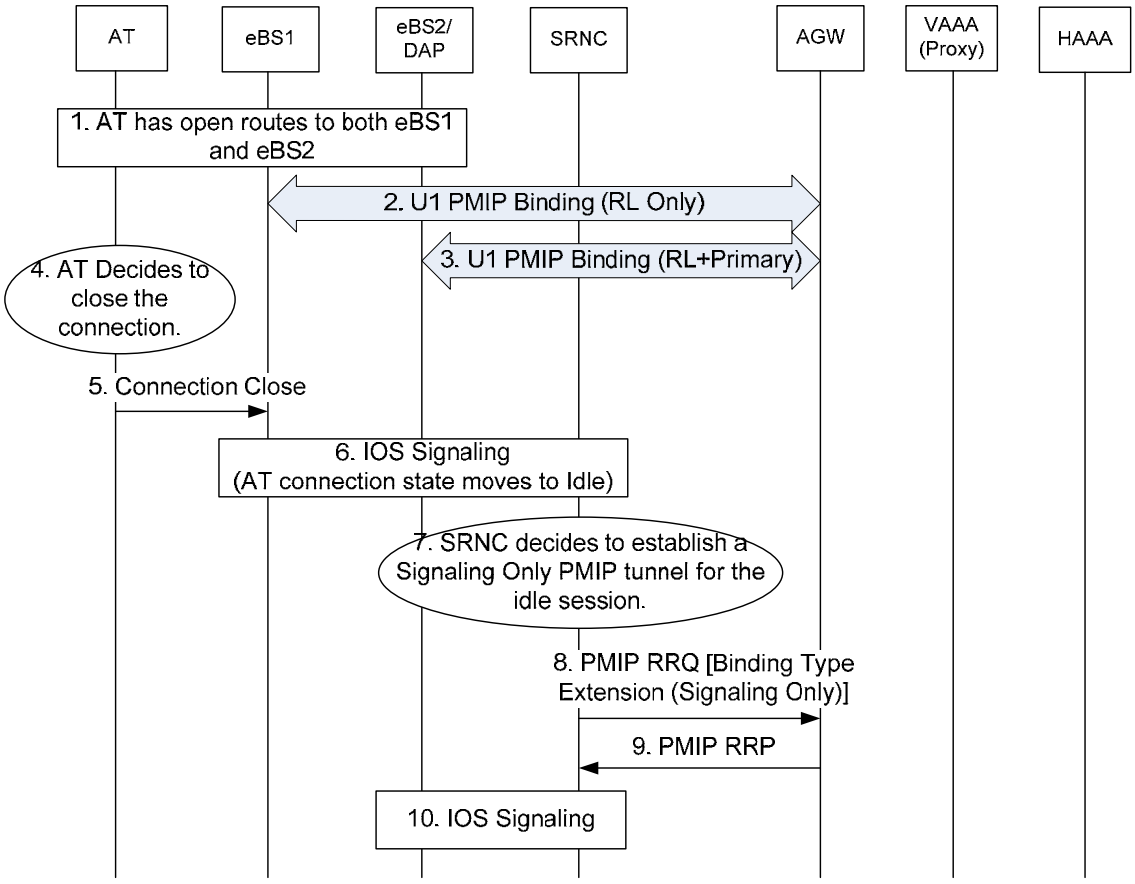


Figure 22. **Signaling Only PMIP Registration**

The steps in Figure 22 are described below.

1. The AT has open routes to both eBS1 and eBS2.
2. A PMIP binding exists between eBS1 and the AGW. This binding is RL Only, thus eBS1 may send reverse link packets directly to the AGW (i.e., does not need to route through eBS2/DAP).
3. A PMIP binding exists between eBS2 and the AGW. This binding is RL + Primary, thus eBS2 receives forward link packets from the AGW, and sends reverse link packets to the AGW.

4. The AT decides to close the connection. The SRNC route remains open.
5. The AT sends the ConnectionClose to eBS1.
6. IOS signaling occurs between eBS1, eBS2, and the SRNC. This signaling moves the AT's connection state to Idle.
7. Both, the SRNC and the AGW support Signaling Only RAN PMIP binding. The SRNC decides to establish a Signaling Only PMIP tunnel for the idle session. Details can be found in [4].
8. The SRNC sends PMIP RRQ to AGW with Binding Type extension to Signaling Only.
9. The AGW sends the PMIP RRP to the SRNC. Since the AGW accepted the Signaling Only binding type, the AGW will revoke PMIP tunnels which existed with eBS1 and eBS2 (as shown in steps 2 and 3 respectively).
10. IOS signaling occurs between SRNC and the eBS2/DAP to allow eBS2 to clean up the resource associated with the AT.

10.3.6 Signaling Only PMIP-Registration for Single PMIP binding case

The figure below illustrates an example of Signaling Only PMIP binding registration sequence when only a bi-directional PMIP tunnel exists between the DAP and the AGW for a data session. In this scenario, both the eBS1 and eBS2 are in the Route Set for the AT: the eBS1 is the RLSE for the AT and the eBS2 is the FLSE and the DAP for the AT.

The Signaling Only PMIP registration binding happens when both the SRNC and the AGW are configured to support Signaling Only binding, and the AT moves from Active state to Idle state. Idle state is triggered when all routes between the AT and eBS's are closed.

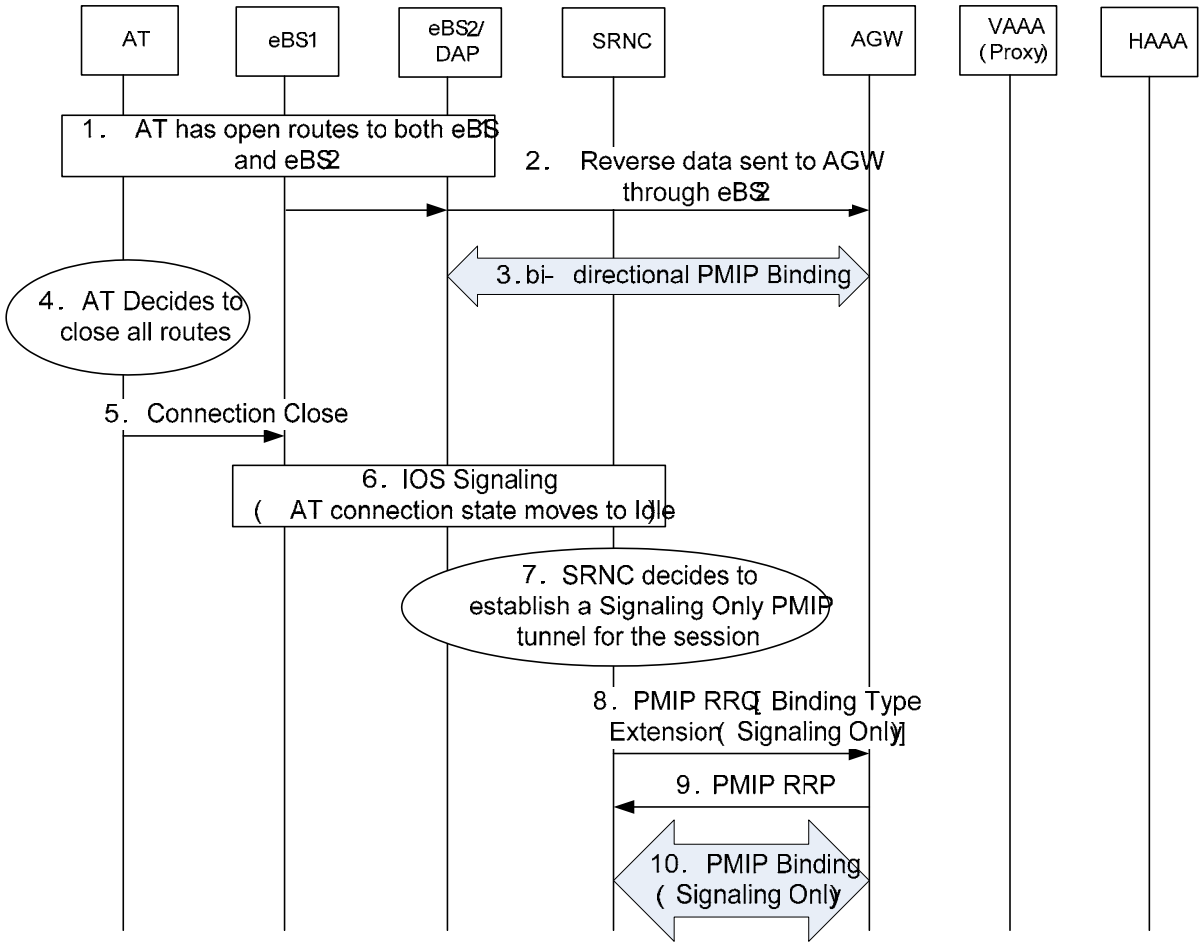


Figure 23. **Signaling Only PMIP Registration for Single PMIP binding case**

The steps in Figure 23 are described below.

1. The AT has open routes to both eBS1 and eBS2. eBS1 is the RLSE for the AT and the eBS2 is the FLSE and the DAP.
2. There is no RL Only U1 PMIP binding between eBS1 and the AGW. Thus, eBS1 sends reverse link packets to the AGW through eBS2/DAP.
3. A bi-directional PMIP binding exists between eBS2 and the AGW, established via a PMIP Registration Request without the Binding Type Extension included in the message. Thus, eBS2 receives forward link packets from the AGW, and sends reverse link packets to the AGW.
4. The AT decides to close all routes.
5. The AT sends Connection Close to the eBS1.
6. IOS signaling occurs between eBS1, eBS2, and the SRNC. This signaling moves the AT connection state to Idle.
7. DAP or SRNC decides to establish a Signaling Only PMIP tunnel for the idle session. (Later steps, only SRNC is shown.)
8. The SRNC sends PMIP RRQ to AGW with Binding Type extension set to Signaling Only.

9. The AGW sends the PMIP RRP to the SRNC. Since the AGW accepted the Signaling Only binding type, the AGW will revoke PMIP tunnels which existed with eBS2.

10. A PMIP binding exists between the SRNC and AGW.

10.3.7 Signaling Only PMIP Deregistration

Figure 24 shows Signaling Only PMIP binding deregistration. Signaling Only PMIP binding deregistration is triggered when a PMIP signaling only binding exists at the AGW for an AT, and a new primary PMIP registration for that AT is performed successfully. The AGW replaces the existing Signaling Only PMIP binding with the new primary PMIP binding.

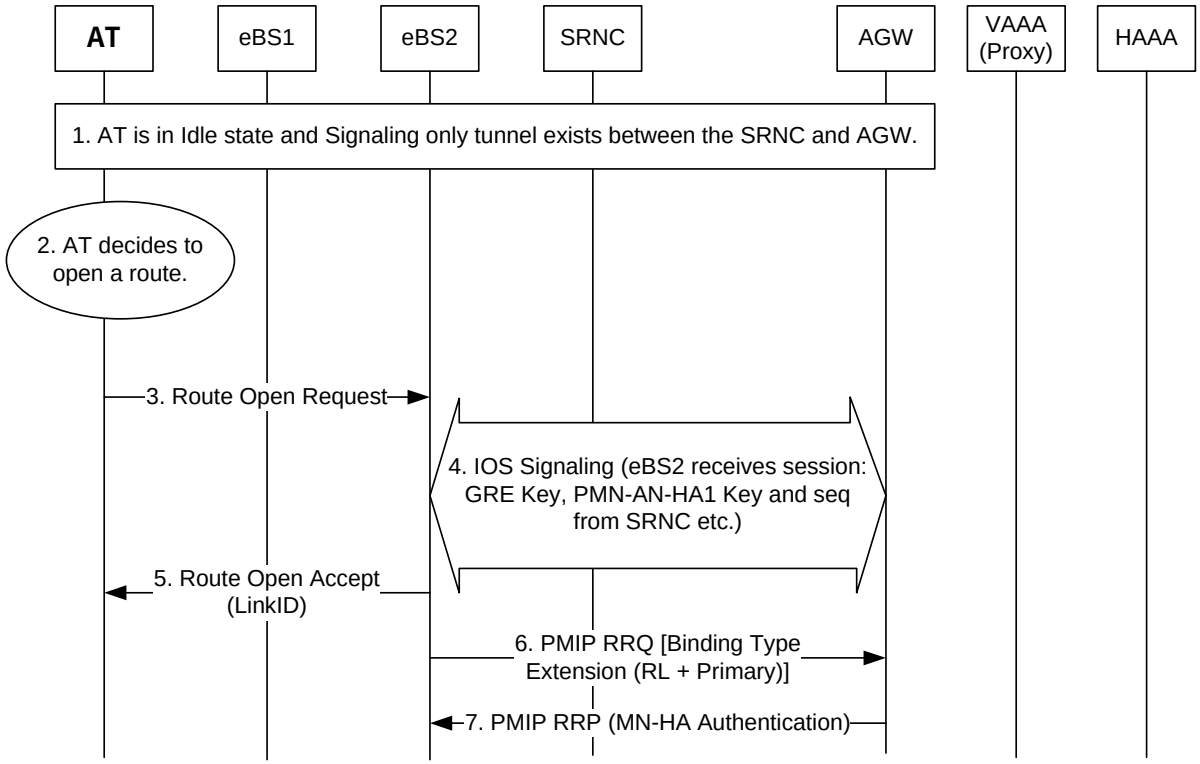


Figure 24. **PMIP Deregistration**

The steps in Figure 24 are described below.

1. AT is in the Idle state and Signaling only tunnel exists between the SRNC and AGW or between the DAP and AGW.

2. The AT decides to open a route to eBS2.

3. The AT sends a Route Open Request to eBS2.

4. eBS2 and SRNC exchange IOS signaling to establish a session for the AT.

5. eBS2 accepts the route open request and sends LinkID to AT.

6. eBS2 sends PMIP RRQ with RL + Primary Binding Type extension to the AGW. (To include this extension is optional.)

7. The AGW verifies the MN-HA Auth extension. If authentication passes, the AGW sends a PMIP RRP indicating success to eBS2. Since the PMIP RRP was successful, the AGW autonomously revokes the PMIP binding which existed in step 1. A PMIP binding now exists between the AGW and eBS2.

10.4 MSK Derivations

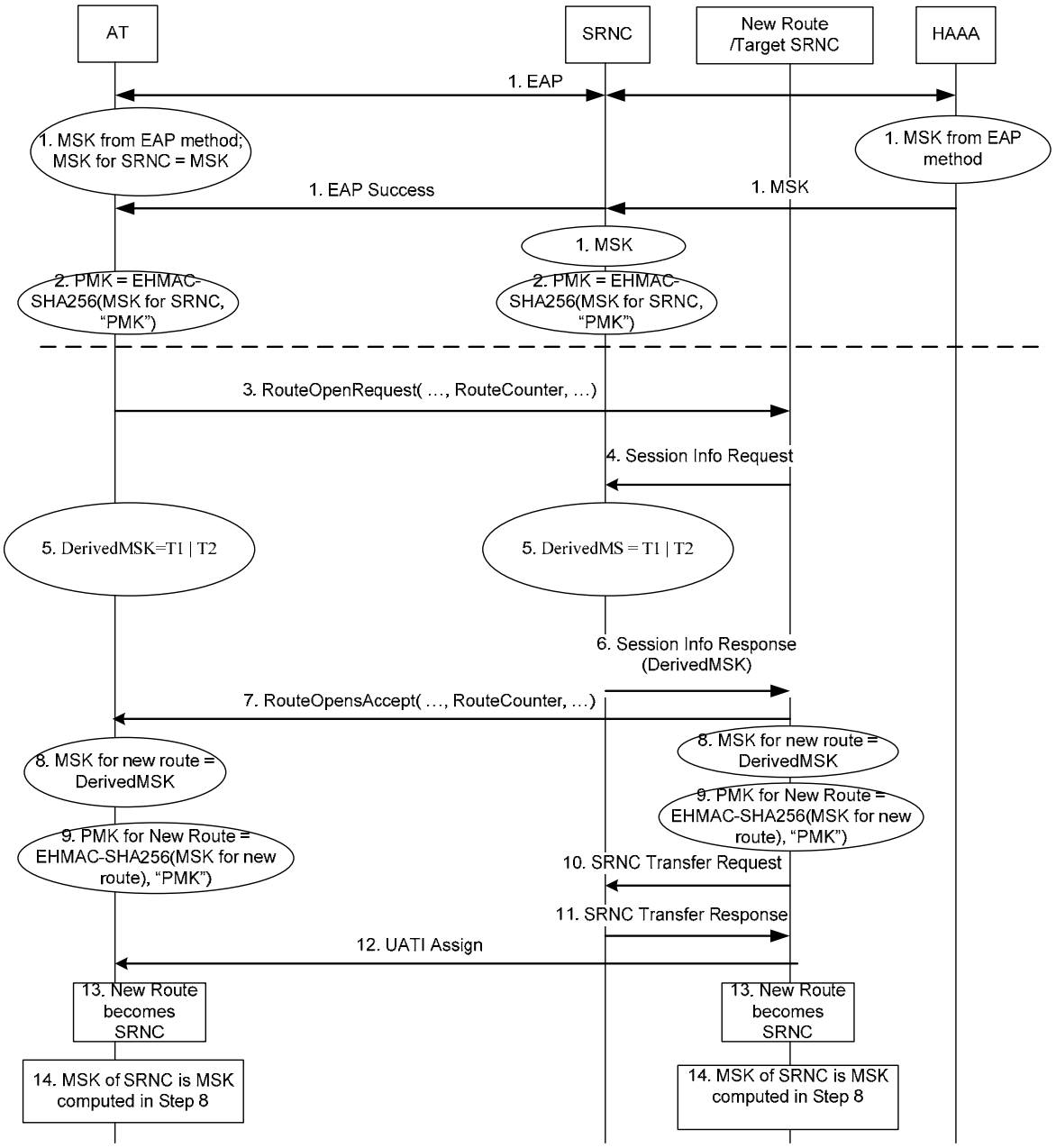


Figure 25. **MSK Derivations**

1. The AT runs EAP with the H-AAA; SRNC is the EAP authenticator and receives the MSK.

2. The AT and the SRNC derive the PMK for SRNC as follows: PMK = EHMAC-SHA256 (MSK for SRNC, “PMK”).

3. The AT opens a new route (which can be an eBS or the Target SRNC). The RouteCounter is part of the Route Open Request message.

4. The New Route requests session information from the SRNC.

5. The SRNC and the AT compute a DerivedMSK= T1 | T2, where T1= EHMAC-SHA256(MSK for SRNC, “DerivedMSK”,0x01, RouteCounter) and T2 = T2 = EHMAC-SHA-256(MSK, T1, “DerivedMSK”, 0x02, RouteCounter).

6. The SRNC sends Session Info Response to the New Route including the DerivedMSK.

7. The New Route sends Route Open Accept to the AT.

8. The New Route receives and stores the MSK. The AT sets the MSK of the New Route to the DerivedMSK.

9. The AT and the New Route derive PMK for the New Route.

10. The New Route decides to become the SRNC. The New Route sends SRNC Session Transfer.

11. The Source SRNC sends SRNC Session Response.

12. The Target SRNC sends UATI assign to the AT.

13. The New Route becomes the SRNC.

14. The AT and the Target-SRNC start using the MSK of the New Route computed at the step 8 for future DerivedMSK derivations.

10.5 Re-authentication Protocol (ERP)

10.5.1 ERP Procedure

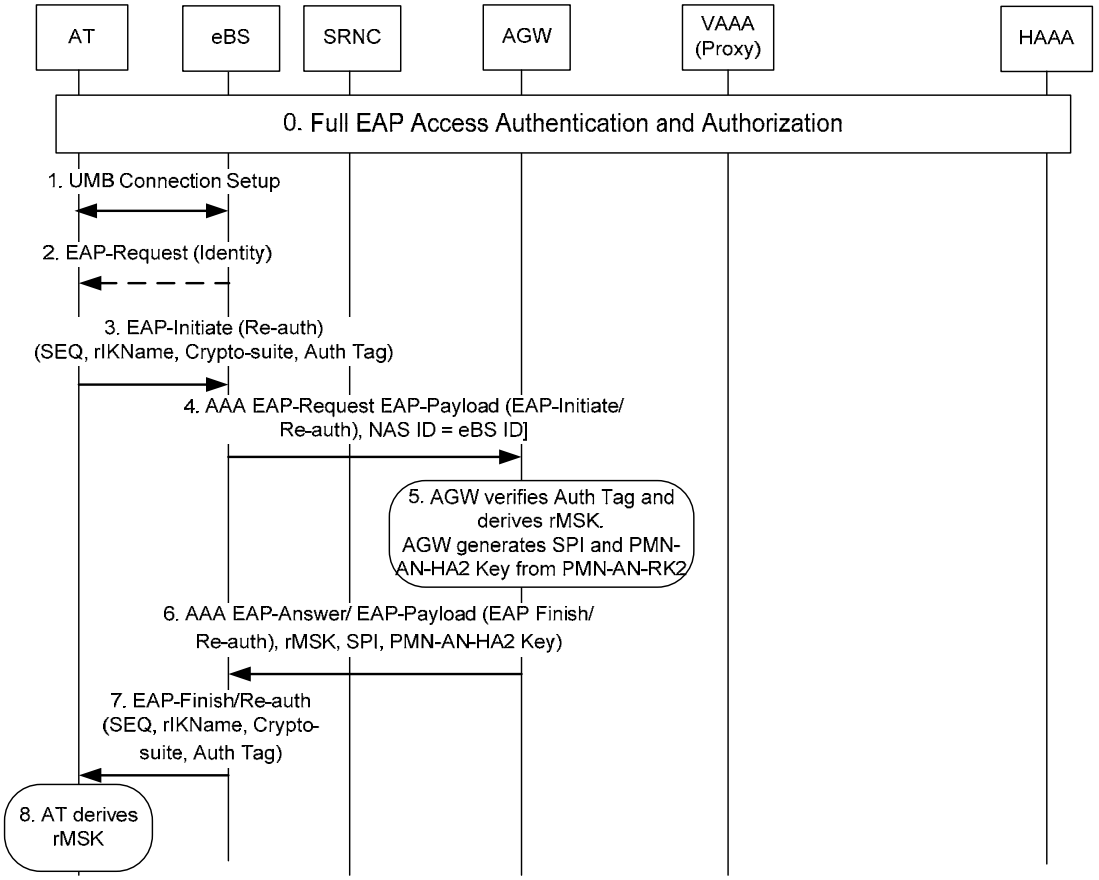


Figure 26. **ERP Procedure**

0. The AT performs a full EAP authentication exchange when it first attaches to the network. If the AGW supports ERP, it requests DSRK (derived from EMSK) from the HAAA through this step. The AGW also indicates its ERP support capability to the SRNC. If ERP is supported by the AT and network, this step establishes an EMSK at the AT and HAAA and a DSRK and a rRK at the AT and AGW (see EAP access authentication and authorization call flow for the full EAP exchange).

1. The AT establishes a UMB connection with the eBS it wants to add to the route set.

2. eBS may send an EAP Request Identity, if the policy is set to the network initiated authentication.

3. The AT sends an EAP Initiate Re-auth message, in accordance with the EAP Re-authentication Protocol (ERP). The message includes a sequence number, the key name used to index the key (rIKName), the crypto-suite used to indicate algorithms and an authentication tag computed over the entire message.

4. The eBS carries the EAP Initiate Re-auth message in a AAA EAP Request EAP Payload. The NAS ID is set to the eBS ID.

5. The AGW verifies the authentication tag and if the verification is successful, derives an rMSK to be sent to the eBS. The AGW also derives a PMN-AN-RK2 from PMN-AN-RK which is generated during EAP Access Authentication and Authorization.

Then the AGW generates a SPI value and derives PMN-AN-HA2 key from the PMN-AN-RK2 associated with the SPI.

6. The AGW responds with an EAP Finish Re-auth message encapsulated in a AAA EAP-Answer EAP-Payload. The AGW also sends the rMSK, SPI, and associated PMN-AN-HA2 key to the eBS in an encrypted manner.

7. The eBS forwards the EAP Finish Re-auth message to the AT. The message contains a sequence number (the same as in EAP Initiate Re-auth sent by the AT), the rIKName that identifies the key, the crypto-suite used and an authentication tag computed over the entire message.

8. The AT derives an rMSK using the sequence number and the rRK once it receives a successful EAP Finish Re-auth message.

10.5.2 Key Hierarchy for Access Authentication

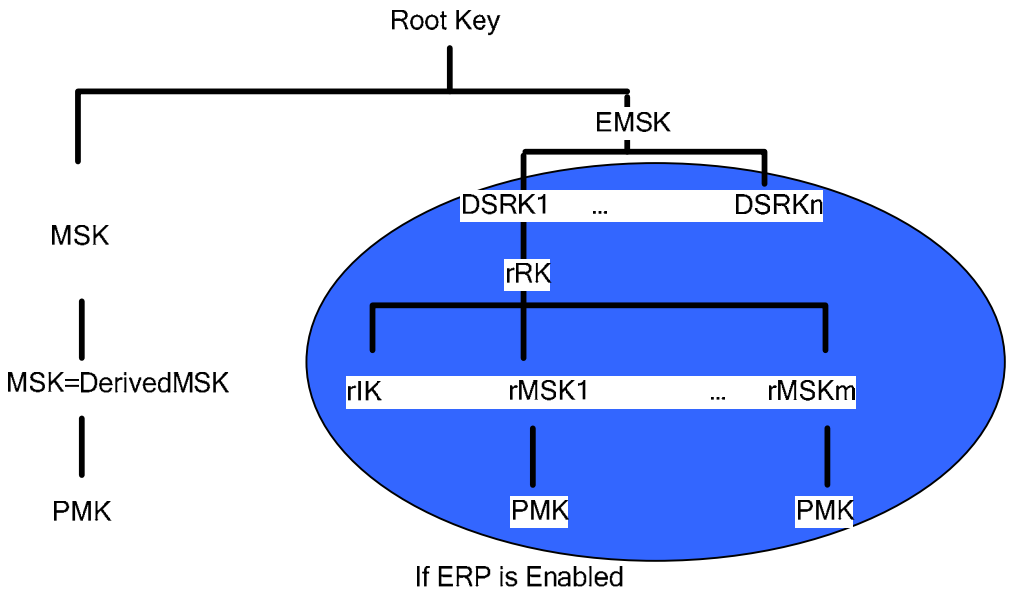


Figure 27. **Key Hierarchy for Access Authentication**

EMSK is specified in [1]. MSK is specified in [2]. The DerivedMSK and PMK are specified in section 3.2. For ERP operation, DSRKn, rRK, rIK, and rMSKm are specified in [39].

10.5.3 PMIP Key Hierarchy for PMIP between SRNC/eBS and AGW

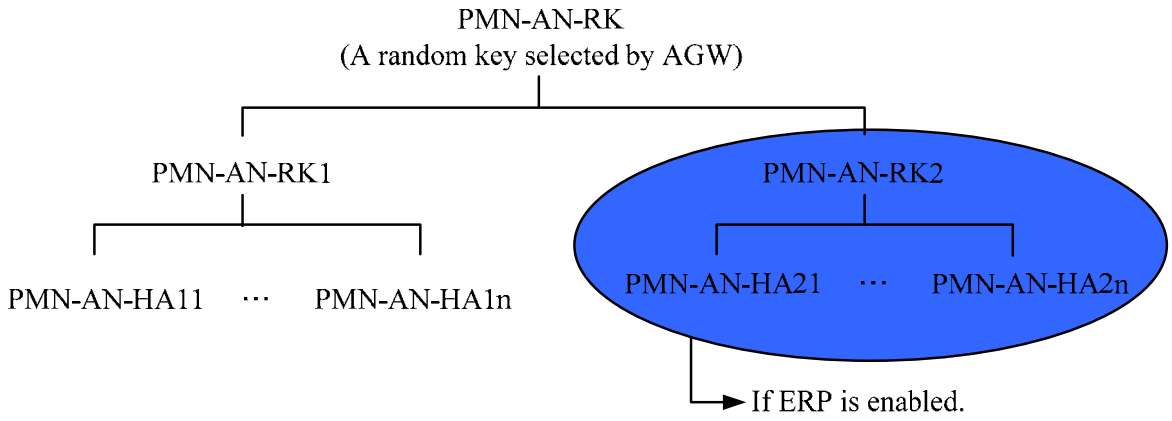


Figure 28. **PMIP Key Hierarchy for the PMIP between AN and AGW**

The PMN-AN-RK is a random key selected by the AGW for the AT. The PMN-AN-RK1 is used for derivation of PMN-AN-HA1 key for AN-AGW PMIP signaling protection when ERP is disabled. See the section 4.2 for the key derivation. The PMN-AN-RK2 is used for derivation of PMN-AN-HA2 key for AN-AGW PMIP signaling protection when ERP is enabled. See section 5.4 for the key derivation.

10.6 Simple IPv4 Address Assignment

10.6.1 Simple IPv4 Addressing with DHCP Rapid Commit Option

Figure 29 illustrates an example call flow for Simple IPv4 address assignment by using DHCPv4 Rapid Commit option (see [19]).

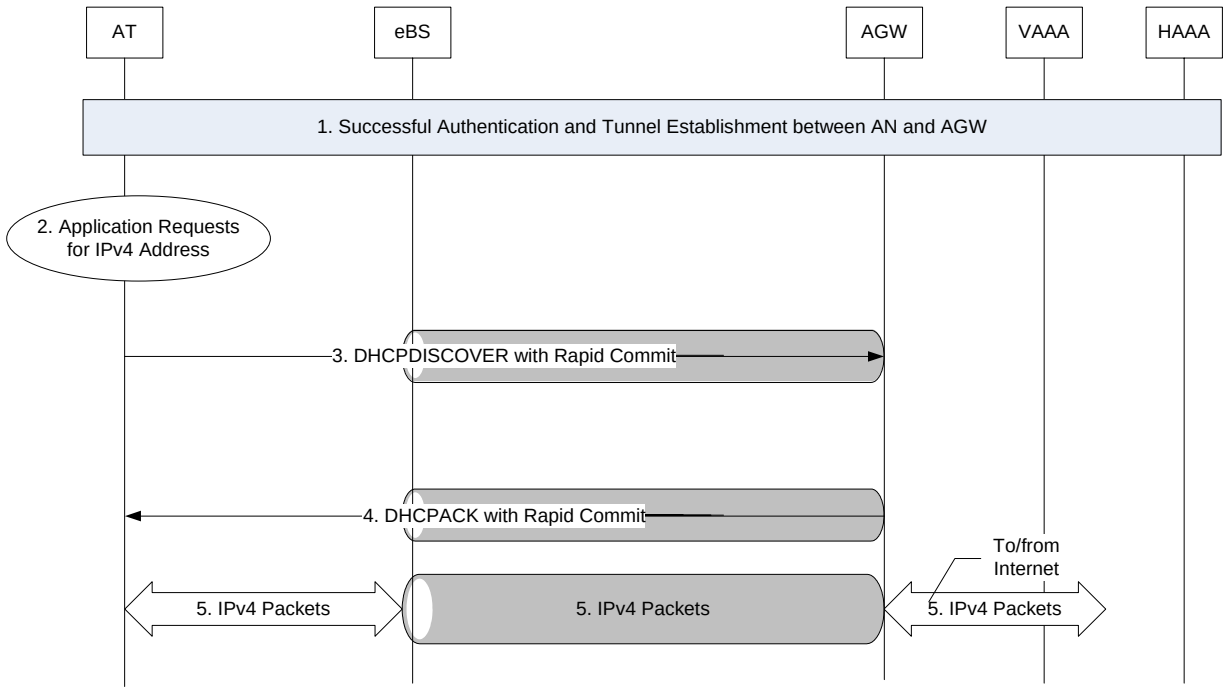


Figure 29. **Simple IPv4 Addressing using DHCP Rapid Commit Option**

The steps in Figure 29 are described below.

1. The AT performs a successful authentication and per AT tunnel is established between the eBS and AGW.
2. AT's application requests a simple IPv4 address. Step 2 may occur during step 1.
3. The AT broadcasts a DHCPDISCOVER message with the Rapid Commit option to the AGW through the tunnel between the eBS and AGW. The AT uses the DHCPv4 Rapid Commit option [19] in order to obtain an IPv4 address and configuration information using a 2-message exchange rather than the usual 4-message exchange.
4. The AGW is acting either as a DHCPv4 Relay Agent or as a DHCPv4 server. If AGW is acting as a DHCP Relay Agent, the AGW forwards the AT's DHCPDISCOVER message to the DHCPv4 server (not shown in this figure.). The AGW sends a DHCPACK message with the Rapid Commit option to the AT through the tunnel between the eBS and AGW.
5. The AT sends/receives IPv4 packets to/from the Internet through the tunnel between the eBS and AGW.

10.6.2 Simple IPv4 Addressing using DHCP

Figure 30 illustrates an example call flow for Simple IPv4 address assignment by using DHCP (see [18]).

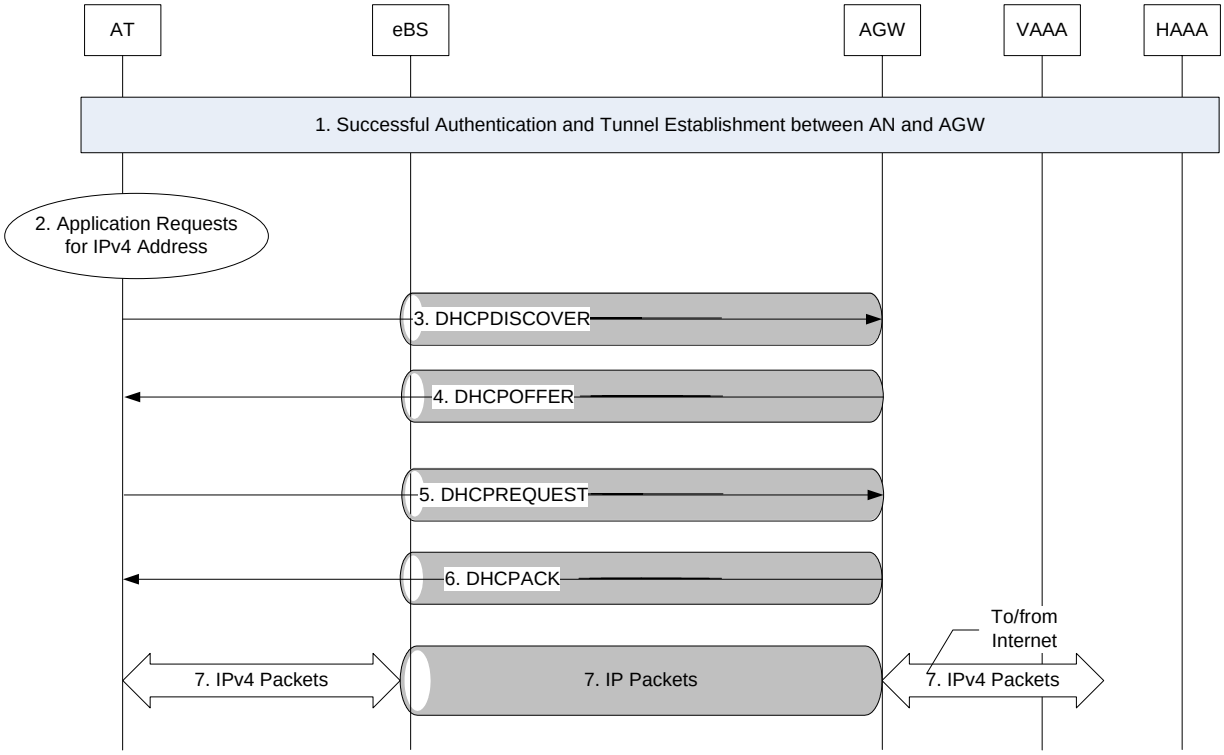


Figure 30. **Simple IPv4 Addressing using DHCP**

The steps in Figure 30 are described below.

1. The AT performs a successful authentication and the per AT tunnel is established between the eBS and AGW.
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 AGW through the tunnel between the eBS and AGW.
4. The AGW is acting either as a DHCPv4 Relay Agent or as a DHCPv4 server. If the AGW is acting as a DHCP Relay Agent, the AGW forwards the AT's DHCPDISCOVER message to the DHCPv4 server (not shown in this figure.). The AGW sends a DHCPOFFER message that includes an available network address in the 'yiaddr' field through the tunnel between the eBS and AGW.
5. The AT broadcasts a DHCPREQUEST message through the tunnel between the eBS and AGW. The DHCPREQUEST message includes the 'server identifier' option and may include other options specifying desired configuration values. The 'requested IP address' option is set to the value of 'yiaddr' in the DHCPOFFER message from the AGW.
6. The AGW sends a DHCPACK message to the AT through the tunnel between the eBS and AGW.
7. The AT sends/receives IPv4 packets to/from the Internet through the tunnel between the eBS and AGW.

10.7 Simple IPv6

Figure 31 illustrates an example call flow for Simple IPv6 address assignment.

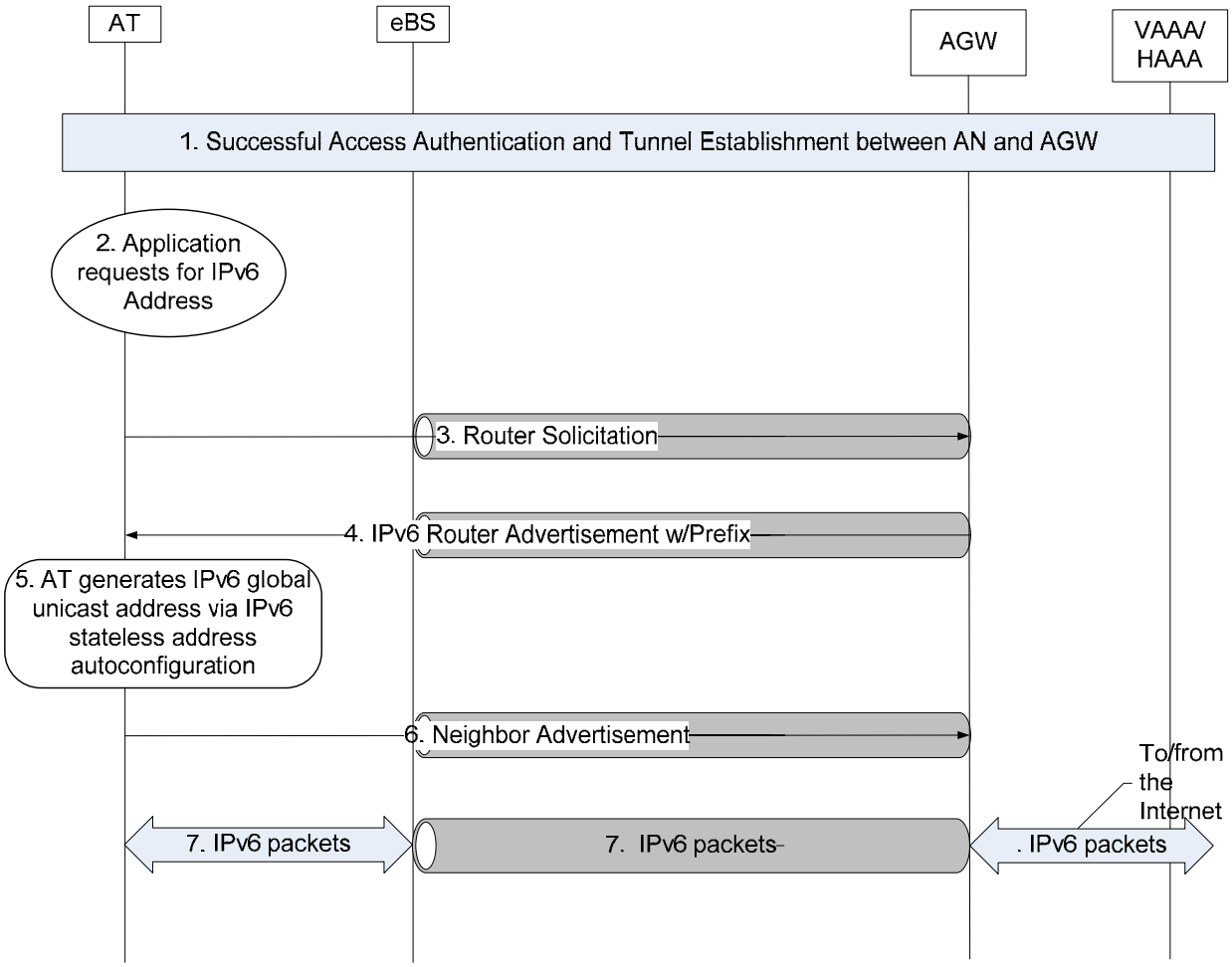


Figure 31. **Simple IPv6 Address Assignment**

The steps in Figure 31 are described below.

1. The AT performs a successful authentication and per AT tunnel is established between eBS and AGW.

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

3. The AT chooses an interface ID which is not within the range between 0000:0000:0000:0000 and 0000:0000:0000:FFFF and constructs its link-local IPv6 address by pre-pending the link-local prefix FE80:: /64 [29] to this interface identifier. The AT sends Router Solicitation message with the source IP address set to its link local IP address and destination address set to all-routers multicast address

[26]. The Router Solicitation message is sent to the AGW through the tunnel between the eBS and the AGW.

4. Upon receiving the Route Solicitation message from the AT over the AT's GRE tunnel, the AGW chooses an interface ID which is within the range between 0000:0000:0000:0002 and 0000:0000:0000:FFFF and construct its link-local IPv6 address by pre-pending the link-local prefix FE80:: /64 [29] to this interface identifier. The AGW, acting as a default router, sends an IPv6 Router Advertisement message [26] to the AT with the source IP address set to its link local IP address and destination address set to all-nodes multicast address or the AT's link local IP address [26]. The Router Advertisement message, tunneled through the eBS, contains an AT's unique prefix. The prefix length can be configured in the AGW based on operator's policy.
5. The AT generates an IPv6 global unicast address via IPv6 stateless address autoconfiguration [27].
6. The AT sends the Neighbor Advertisement message with setting its global IPv6 address in the Target address filed in order to tell the AGW full AT's IPv6 address.
7. The AT sends/receives IPv6 packets to/from the Internet through the tunnel between the eBS and AGW.

10.8 Simple IP Address Release Procedure

The call flows in this section assume that the AGW is the DHCP Server.

10.8.1 Simple IPv4 Address Release Procedure

10.8.1.1 IP Address Release Upon Timer Expiration

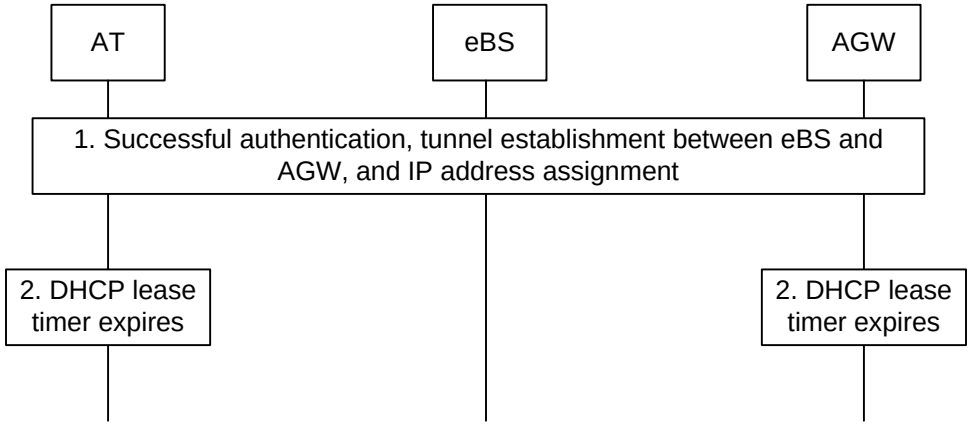


Figure 32. **IP Address Release upon Timer Expiration**

1. After successful authentication, tunnel establishment between eBS and AGW, and IP address assignment via DHCP are performed. The AT sends/receives IPv4 packets to/from the Internet through the tunnel between the eBS and AGW.
2. When the DHCP lease timer expires, both AT and AGW release assigned IP address.

10.8.1.2 IP Address Release before Timer Expiration

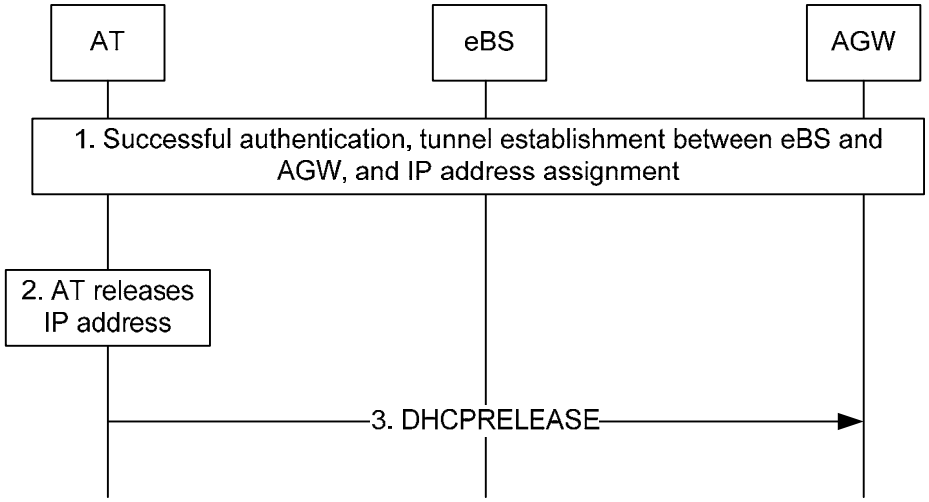


Figure 33. **IP Address Release before Timer Expiration**

1. After successful authentication, tunnel establishment between eBS and AGW, and IP address assignment via DHCP are performed. The AT sends/receives IPv4 packets to/from the Internet through the tunnel between the eBS and AGW.
2. The AT releases the IP address before DHCP lease timer expires.
3. AT sends the DHCPRELEASE to the AGW. The AGW checks if the DHCPRELEASE comes from a valid AT. The AGW marks the IP address as not allocated.

10.8.2 Simple IPv6 Address Release Procedure

10.8.2.1 IPv6 Address Release upon Timer Expiration

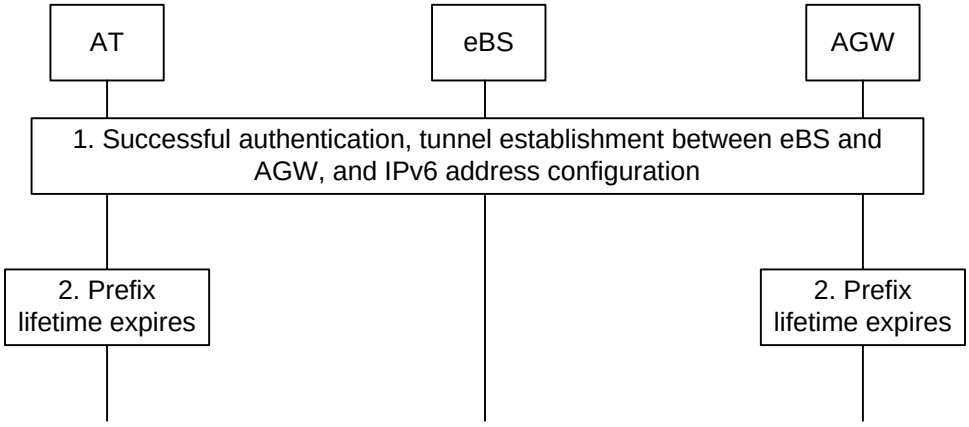


Figure 34. **IPv6 Address Release upon Timer Expiration**

1. After successful authentication, tunnel establishment between eBS and AGW, and IPv6 address auto-configuration are performed. The AT sends/receives IPv6 packets to/from the Internet through the tunnel between the eBS and AGW.
2. When the Prefix lifetime expires, both AT and AGW release the assigned Prefix.

10.8.2.2 IPv6 Address Release before Timer Expiration

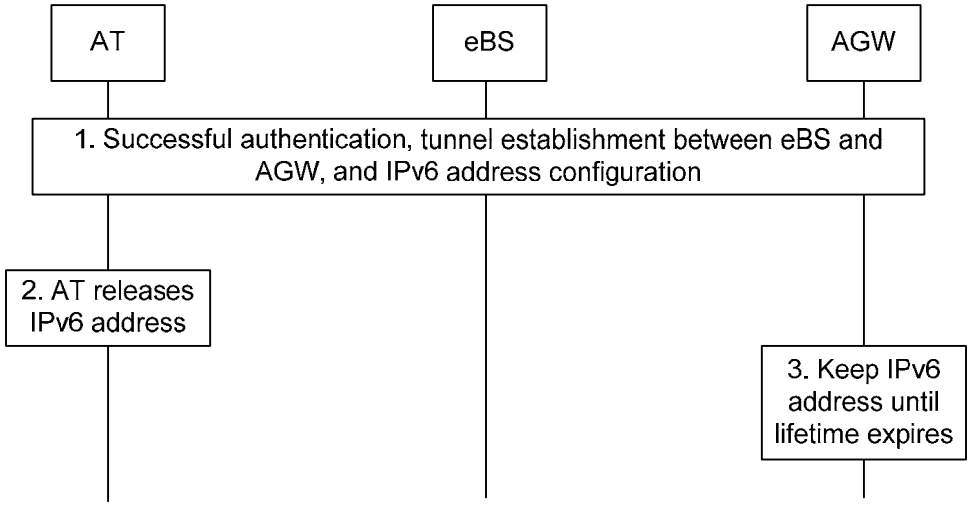


Figure 35. **IPv6 Address Release before Timer Expiration**

1. After successful authentication, tunnel establishment between eBS and AGW, and IPv6 address auto-configuration are performed. The AT sends/receives IPv6 packets to/from the Internet through the tunnel between the eBS and AGW.
2. When the AT releases IPv6 address, it does not send any message to eBS or AGW.
3. The AGW maintains the assigned Prefix until lifetime expires.