

3GPP2 X.S0054-110-0

Version 2.0

Date: August 29, 2008



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

MIPv4 Specification in Converged Access Network Specification

COPYRIGHT

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

This page is left blank intentionally.

MIPv4 Specification in Converged Access Network

CONTENTS

1	1	Introduction	1
2	1.1	SCOPE	1
3	2	References	2
4	2.1	Normative References	2
5	2.2	Informative References	2
6	3	Client Mobile IPv4 Operation	4
7	3.1	Protocol Stack	4
8	3.2	CMIP4 Key Management	4
9	3.3	AT Requirements	5
10	3.3.1	Agent Discovery	5
11	3.3.2	CMIP4 Registration	5
12	3.3.3	Reverse Tunneling	6
13	3.3.4	Termination	6
14	3.4	AGW Requirements	6
15	3.4.1	Agent Advertisement	6
16	3.4.2	CMIP4 Registration	7
17	3.4.3	FA-HA Security	8
18	3.4.4	Reverse Tunneling	9
19	3.4.5	Ingress Address Filtering	10
20	3.4.6	Overlapping Private Address Support	10
21	3.4.7	Registration Revocation	10
22	3.5	HA Requirements	11
23	3.5.1	CMIP4 Registration	11
24	3.5.2	FA-HA Security	12
25	3.5.3	DHCPv4 Support	13
26	3.5.4	Registration Revocation	13
27	3.6	AAA Requirements	13
28	3.6.1	CMIP4 Registration	13
29	3.6.2	FA-HA Security	14
30	3.6.3	Reverse Tunneling	15
31	4	Call Flows	16
32	4.1	Mobile IPv4 Addressing with RADIUS	16

LIST OF FIGURES

<i>Figure 1</i>	Protocol Reference Model for CMIP4 Control	4
<i>Figure 2</i>	Protocol Reference Model for CMIP4 User Data	4
<i>Figure 3</i>	Mobile IPv4 Addressing with RADIUS.....	16

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

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

LIST OF TABLES

<i>Table 1.</i>	Additional RADIUS Attributes between AGW and AAA during Access Authentication and Authorization for Supporting CMIP4 Registration.....	8
<i>Table 2.</i>	RADIUS Attributes between AGW and AAA for Supporting FA-HA MSA Distribution	9
<i>Table 3.</i>	RADIUS Attributes between HA and AAA for Supporting CMIP4 Registration	12
<i>Table 4.</i>	RADIUS Attributes between HA and AAA for Supporting FA-HA MSA distribution	12

REVISION HISTORY

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

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

FOREWORD

(This foreword is not part of this Standard.)

This document was prepared by 3GPP2 TSG-X.

This document is a new specification.

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

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

X.S0054-110-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 client based Mobile IPv4 access to the Converged Access Network supporting Ultra Mobile Broadband^{TM1} radio access.

1.1 SCOPE

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

The scope of this document covers client based Mobile IPv4 aspects in support of the UMB wireless access.

¹ Ultra Mobile BroadbandTM and (UMBTM) 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: RFC3344, Parkins, “IP Mobility Support for IPv4”, August 2002.
- [2] IETF: RFC2794, Calhoun, et.al., “Mobile IP Network Access Identifier Extension for IPv4”, March 2000.
- [3] IETF: RFC3012, Parkins, et.al., “Mobile IPv4 Challenge/Response Extensions”, November 2000.
- [4] IETF: RFC3543, Glass, et.al., “Registration Revocation in Mobile IPv4”, August 2003.
- [5] IETF: RFC3024, Montenegro, “Reverse Tunneling for Mobile IP, revised”, January 2001.
- [6] 3GPP2: X.S0054-100-0 v2.0, “Basic IP Service for Converged Access Network Specification”, August 2008.
- [7] 3GPP2: X.S0011-002-D, “cdma2000 Wireless IP Network Standard: Simple IP and Mobile IP Access Service”, March 2006.
- [8] IETF: RFC1918, Rekhter, et.al., “Address Allocation for Private Internets”, February 1996.
- [9] IETF: RFC2131, Dorms, “Dynamic Host Configuration Protocol”, March 1997.
- [10] IETF: RFC3046, Patrik, “DHCP Relay Agent Information Option”, January 2001.
- [11] 3GPP2: S.S0078-B, “Common Security Algorithms”, February 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.S0054-000-0 v2.0, “CAN Wireless IP Network Overview and List of Parts”, August 2008.
- <2> 3GPP2: X.S0054-102-0 v2.0, “Multiple-Authentication and Legacy Authentication Support for Converged Access Network”, August 2008.
- <3> 3GPP2: X.S0054-210-0 v1.0, “CMIP based Inter-AGW Handoff”, December 2007.
- <4> 3GPP2: X.S0054-220-0 v2.0, “Network PMIP Support”, August 2008.
- <5> 3GPP2: X.S0054-300-0 v1.0, “QoS Support for Converged Access Network Specification”, December 2007.

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

- <6> 3GPP2: X.S0054-400-0 v1.0, "Converged Access Network Accounting Specification", December 2007.
- <7> 3GPP2: X.S0054-910-0 v2.0, "CAN Data Dictionary", August 2008.

3 Client Mobile IPv4 Operation

This section describes the requirements and procedures for CMIP4.

3.1 Protocol Stack

Figure 1 shows the protocol reference model for CMIP4 control data between the AT and the HA. Figure 2 shows the protocol reference model for CMIP4 user data between the AT and CN.

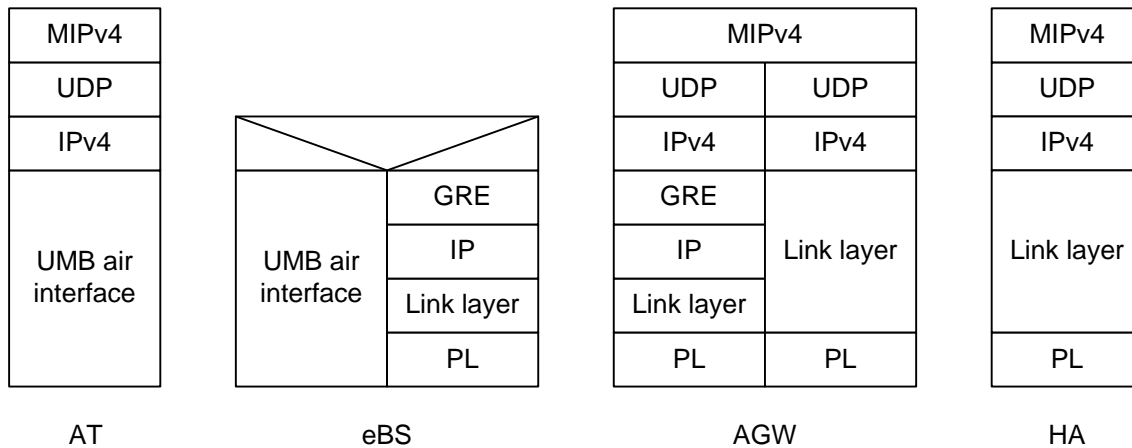


Figure 1 Protocol Reference Model for CMIP4 Control

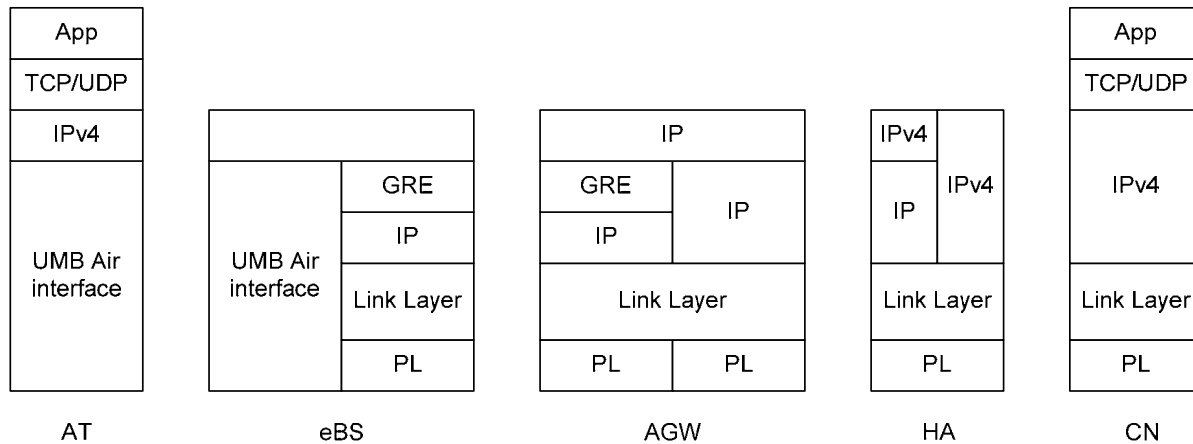


Figure 2 Protocol Reference Model for CMIP4 User Data

3.2 CMIP4 Key Management

The AT may use static MN-HA key and static MN-AAA key. If the static MH-HA key and MN-AAA key are used, the procedures in [7] shall be used. If the AT uses dynamic MN-HA key and dynamic MN-AAA key, the requirements described below in this section are applicable.

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

Upon successful EAP access authentication, the EMSK is available at AT and the HAAA. From the EMSK, the CMIP4-MN-RK shall be computed as follows:

CMIP4-MN-RK key = HMAC-SHA-256[11] (EMSK, "CMIP4-MN-RK@3gpp2")

From the CMIP4-MN-RK, the MN-AAA key and its associated MN-AAA-SPI shall be derived as follows:

MN-AAA key = HMAC-SHA-256 (CMIP4-MN-RK, "MN-AAA@3gpp2")

MN-AAA-SPI = HMAC-SHA-256 (MN-AAA key, "3GPP2-MN-AAA-SPI@3gpp2")

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

From the CMIP4-MN-RK, the MN-HA key and its associated MN-HA-SPI shall be derived as follows:

MN-HA Key = HMAC-SHA-256 (CMIP4-MN-RK, "MN-HA@3gpp2", HA IP Address)

MN-HA-SPI = HMAC-SHA-256 (MN-HA key, "3GPP2-MN-HA-SPI@3gpp2")

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

Using the same rules for SPI calculation at the AT and the HAAA results in same unique SPI value at both ends.

3.3 AT Requirements

3.3.1 Agent Discovery

After successful access authentication, if the AT wants to use CMIP4, the AT shall send an Agent Solicitation [1] on Level 1 IP interface. If the AT does not have a home address, the AT shall set the source IP address to 0.0.0.0. The AT shall set the destination IP address to 255.255.255.255 (the IPv4 limited broadcast address).

When the FA advertisement lifetime expires, the AT may send Agent Solicitations.

3.3.2 CMIP4 Registration

Upon receiving an Agent Advertisement from the AGW, the AT may send an RRQ [1] on Level 1 IP interface.

During initial CMIP4 registration, if the AT wants to request an HA in the AT's home network, the AT shall set the HA Address field to 255.255.255.255 in the RRQ; otherwise, the AT shall set the HA Address field to 0.0.0.0 in the RRQ. The AT shall set the Home Address field to 0.0.0.0 in the RRQ. The AT shall include the MN-NAI extension [2], MN-FA Challenge extension, and MN-AAA Authentication extension [3] in the RRQ. The AT shall use the MN-AAA key to generate MN-AAA-SPI and include it in the MN-AAA Authentication extension. Upon receiving RRP, if the AT does not have a static MN-HA key, the AT shall generate a dynamic MN-HA key along with its associated SPI called MN-HA-SPI as specified in Section 3.2.

The AT shall use the MN-HA key to verify the MN-HA Authentication extension in the RRP.

During CMIP4 re-registration (to refresh lifetime) or inter-AGW handoff (change of FA CoA), the AT shall use the same HA address and home address field in the RRQ. The AT shall include the MN-HA Authentication extension 0, MN-NAI extension [2], and MN-FA Challenge extension in the RRQ. For the SPI field of the MN-HA Authentication extension in the RRQ, the AT shall use the same value in the SPI field of the MN-HA Authentication extension of the RRP that was received during the initial CMIP4 registration.

If the MN-HA-SPI generated by AT is different from the value received in the SPI field of the MN-HA Authentication extension of the RRP, the AT shall overwrite its computed value with that received.

3.3.3 Reverse Tunneling

If the AT's home network policy requires reverse tunneling, the AT shall set the 'T' bit in the RRQ [5]. The AT may negotiate encapsulated delivery style with the AGW [5].

If the AT wants to request DHCP option through the HA, the AT shall negotiate Encapsulating Deliver Style with the AGW (see [5]). The AT shall send DHCPINFORM message by using Encapsulating Deliver Style.

3.3.4 Termination

When the AT wishes to terminate a CMIP4 session, the AT may send an RRQ with registration lifetime field set to zero 0.

3.4 AGW Requirements

The AGW shall support the FA operations specified in [1], [2], and [3] on Level 1 IP interface.

3.4.1 Agent Advertisement

Upon receiving an Agent Solicitation encapsulated with the GRE key for Level 1 from an AT, the AGW shall send the Agent Advertisement to the AT on Level 1 IP interface. Based on AGW local policy, the AGW may send the Agent Advertisements to the AT on Level 1 IP interface without the AT's solicitation upon establishment of the primary PMIP4 tunnel with the eBS.

The AGW shall include the MN-FA Challenge Extension [3] in the Agent Advertisement. Because Advertisements are rarely sent (to save air resources), the AGW shall include in the RRP a new challenge that the AT should use in its next re-registration with this AGW.

In order to minimize Agent Advertisements sent over the air, the AGW shall not send unsolicited Agent Advertisements to an AT to periodically refresh the FA advertisement

lifetime. The Advertisement Lifetime shall be set to 9000 seconds (the maximum ICMP router advertisement lifetime).

3.4.2 CMIP4 Registration

If the AT is not authorized with CMIP4 service (see [6] section 3), upon receiving RRQ from the AT from Level 1 IP interface, the AGW shall send RRP with the reason code set to 65 (Administratively Prohibited) to indicate that the AT is not authorized with CMIP4 service.

If the AT is authorized with CMIP4 service, the AGW shall perform the following:

For dynamic Home Address assignment, the AGW shall accept RRQ with the source IP address set to 0.0.0.0, from an AT. The AGW shall use the AT's NAI (in the MN-NAI extension) and the Identification field [2] for the pending registration.

Upon receiving an RRQ with the HA Address field set to a value other than 0.0.0.0 or 255.255.255.255, if the FA-HA MSA already exists between the AGW and the HA identified in the HA Address field of the RRQ, or if the FA-HA MSA between the AGW and the HA is not required based on policy, the AGW shall forward the RRQ to the HA. Upon receiving a RRP from the HA, the AGW shall process the RRP, acquire the AT's home address from the RRP, and forward it to the AT according to 0.

If the AGW wants to indicate its support for registration revocation to the HA, the AGW shall include Mobile IP Revocation Support extension in the RRQ sent to the HA. If the AGW receive an RRP that does not include Mobile IP Revocation Support extension, the AGW shall assume that HA does not support registration revocation.

If the AGW receives an RRP from a HA and the same IP address has been assigned to the AT for a different IP session, the AGW shall reject the IP address assignment. The AGW shall set the Code field to 65 (administratively prohibited) before forwarding the RRP to the AT and send Registration Revocation message to the HA. The previous assigned IP address is not affected.

3.4.2.1 Diameter

Diameter is not supported in this release.

3.4.2.2 RADIUS

During the EAP access authentication of a roaming AT, if the visited network's policy allows local HA assignment in its network, the AGW may allocate an HA from the visited network and include the VAAA-Assigned-MIP4-HA VSA in the RADIUS Access-Request for the EAP access authentication.

Upon receiving an RRQ with the HA Address field set to 255.255.255.255, if during the access authentication the AGW received the RADIUS Access-Accept message with the Home Agent VSA (containing an HA address assigned by the HAAA), the AGW shall forward the RRQ to that HA.

Upon receiving an RRQ with the HA Address field set to 255.255.255.255, if during the access authentication the AGW did not receive the Home Agent VSA, or the AGW received the Home Agent VSA in the RADIUS Access-Accept message, but by policy the AGW considers it not valid, the AGW shall send a RADIUS Access-Request message to the HAAA, via VAAA if roaming, for requesting dynamic HA assignment from the HAAA. Upon receiving a RADIUS Access-Accept message that contains an HA address in the Home Agent VSA, the AGW shall forward the RRQ to that HA.

Upon receiving an RRQ with the HA Address field set to 0.0.0.0, if during the access authentication the AGW received a RADIUS Access-Accept message with the VAAA-Assigned-MIP4-HA VSA (containing a HA address assigned by the VAAA) and Home Agent VSA (containing an HA address assigned by the HAAA), the AGW shall forward the RRQ to one of the HAs based on local policy.

Upon receiving an RRQ with the HA Address field set to 0.0.0.0, if during the access authentication the AGW received a RADIUS Access-Accept message with either VAAA-Assigned-MIP4-HA VSA (containing a HA address assigned by the VAAA) or Home Agent VSA (containing an HA address assigned by the HAAA), the AGW shall forward the RRQ to the received HA IP address.

Upon receiving an RRQ with the HA Address field set to 0.0.0.0, if during the access authentication the AGW received the RADIUS Access-Accept message with neither the VAAA-Assigned-MIP4-HA VSA nor the Home Agent VSA included, or if the AGW has received the Home Agent or VAAA-Assigned-MIP4-HA VSA but by policy the AGW considers it not valid, the AGW shall send the RADIUS Access-Request message to the HAAA, via VAAA if roaming, for requesting a dynamic HA assignment from the HAAA. Upon receiving a RADIUS Access-Accept message that contains an HA address in the Home Agent VSA or/and VAAA-Assigned-MIP4-HA VSA, the AGW shall forward the RRQ to the HA according to the procedures specified above in this section.

Table 1. Additional RADIUS Attributes between AGW and AAA during Access Authentication and Authorization for Supporting CMIP4 Registration

Attribute Name	Type	Access-Request	Access-Accept	Interface(s)
Home Agent	26/7	0	0-1	AGW <- HAAA
VAAA-Assigned-MIP4-HA	26/189	0	0-1	AGW <- VAAA

0 This attribute shall not be present.

0-1 Zero or one instance of this attribute may be present.

1 Exactly one instance of this attribute shall be present.

3.4.3 FA-HA Security

Based on policy, an FA-HA Mobility Security Association (MSA) or an IPsec Security Association (SA) may be used to protect the CMIP4 registration messages exchanged between the AGW and HA. The use of an IPsec SA is outside the scope of this document. The usage of an FA-HA MSA is specified in the following sections.

3.4.3.1 Diameter

Diameter is not supported in this release.

3.4.3.2 RADIUS

During the initial CMIP4 registration, if an FA-HA MSA is required, the AGW shall perform the following:

- If the AGW has not received an assigned HA during the AT's access authentication and the AGW needs to request the HAAA to assign an HA for the AT, the AGW shall include the FA-HA-MSA-Request VSA in a RADIUS Access-Request message to the HAAA, via VAAA if roaming, to request a dynamic HA assignment from the HAAA according to [7].

- If during access authentication the AGW has received a HA address from the HAAA, and the HA address is to be assigned to the AT, the AGW shall check whether it has an FA-HA MSA with the HA in the AT’s home network. If the AGW does not have an FA-HA MSA with the HA, the AGW shall send a RADIUS Access-Request message to the HAAA, via VAAA if roaming, which includes the User-Name attribute and FA-HA-MSA-Request VSA. The AGW shall set the User-Name attribute to “AGW|HA@realm”. The AGW shall form the “AGW|HA” by concatenating the AGW’s and HA’s IP addresses encoded using eight hexadecimal ASCII characters. The AGW shall set the “realm” equal to the realm portion of the AT’s NAI.
- If the assigned HA is in the visited network, the AGW shall check whether it has an FA-HA MSA with the HA. If the AGW does not have FA-HA MSA with the HA, the AGW shall send a RADIUS Access-Request message, including the User-Name attribute and FA-HA-MSA-Request VSA, to the VAAA. The AGW shall set the User-Name attribute to “AGW|HA@realm”. The AGW shall set the “realm” equal to the realm of the visited network where the HA is assigned.

During inter-AGW handoff, upon receiving an RRQ with a HA address that is not 0.0.0.0 or 255.255.255.255, if an FA-HA MSA is required, the AGW shall check whether it has FA-HA MSA with the HA. If the AGW does not have an FA-HA MSA with the HA, the AGW shall send a RADIUS Access-Request that includes the User-Name attribute and FA-HA-MSA-Request VSA. The AGW shall set the User-Name attribute to “AGW|HA@realm”. The AGW shall set the “realm” equal to the HA’s realm in the received HA-Realm VSA of the RADIUS Access-Accept during EAP access authentication.

Upon receiving a RADIUS Access-Accept message that includes the FA-HA-MSA VSA, the AGW shall use the FA-HA MSA to compute the FA-HA Authentication extension in the RRQ to be forwarded to the HA. The AGW shall use the FA-HA MSA to verify the FA-HA Authentication extension in the RRP received from the HA 0.

Table 2. RADIUS Attributes between AGW and AAA for Supporting FA-HA MSA Distribution

Attribute Name	Type	Access-Request	Access-Accept	Interface(s)
User-Name	1	1	0	AGW -> HAAA
NAS-IP-Address	4	1	0	AGW -> HAAA
HA-Realm	26/176	0	0-1	AGW <- HAAA
FA-HA-MSA-Request	26/177	1	0	AGW -> HAAA
FA-HA-MSA	26/178	0	1	AGW <- HAAA

- 0 This attribute shall not be present.
- 0-1 Zero or one instance of this attribute may be present.
- 1 Exactly one instance of this attribute shall be present.

Note 1: The HA-Realm VSA may be included in the RADIUS Access-Accept during access authentication.

3.4.4 Reverse Tunneling

The AGW shall support both direct delivery and encapsulated delivery styles as specified in [5].

If reverse tunneling with encapsulating delivery style is negotiated with the AT, the AGW shall send all the packets as specified in [5].

Upon receiving the DHCPINFORM from the AT using encapsulating delivery style, the AGW shall support DHCP forwarding function (not including giaddr) to forward DHCPINFORM to HA through CMIP4 reverse tunnel. If DHCPACK or DHCPNAK with destination IP address set to broadcast IP address is received from the HA, the AGW shall forward DHCPACK or DHCPNAK to the AT's GRE tunnel to the eBS based on CHADDR field.

If during AT's access authentication the AGW receives the Reverse-Tunnel-Specification VSA in the RADIUS Access-Accept message, the AGW shall reject the CMIP4 registration, from an AT that does not set the T bit in the RRQ, with an error code of 75.

3.4.5 Ingress Address Filtering

Upon receiving a packet from the AT while CMIP4 registration is pending, the AGW shall discard the packet if the source IP address of the packet is invalid, and the packet is not a CMIP4 control packet (RRQ or Agent Solicitation).

3.4.6 Overlapping Private Address Support

It is possible that two different ATs served by the same AGW have the same overlapping private address assigned by two different HAs. To support this scenario, the AGW associates the RAN PMIP4 GRE key, the AT's home address, and the HA address. When the AGW receives a CMIP4-tunneled packet from an HA, which is destined for an AT's private home address, the AGW shall transmit the packet in the appropriate PMIP4 tunnel identified by the AT's PMIP4 GRE key. When the AGW receives a packet from the PMIP4 tunnel identified by the AT's PMIP4 GRE key, and the packet is originated with the AT's private home address, the AGW shall forward the packet to the appropriate HA.

For additional CMIP4 registrations from the same AT, if the AGW receives an RRP from a second HA that includes a private address as the AT's home address, and if the private address has already been assigned to that AT by another HA, the AGW shall set the Code field to 65 (administratively prohibited) before forwarding the RRP to the AT and send Registration Revocation message to the HA. The first address assigned to the AT is not affected.

3.4.7 Registration Revocation

Upon receiving Disconnect-Request message (for RADIUS) the AGW shall follow the procedures defined in [6]. In addition, if the AGW supports registration revocation and if it negotiated it with the HA during CMIP4 registration the AGW shall send Registration Revocation message to the HA as specified in the [4].

If the AGW receives the Registration Revocation message from the HA, the AGW shall validate the message. Upon successful validation, the AGW shall clean up the resources associated with the AT's IP address that is being revoked and send a Registration Revocation Acknowledgment message to the HA.

3.5 HA Requirements

3.5.1 CMIP4 Registration

The HA shall save the MN-HA key and the MN-HA-SPI received from the HAAA for the duration of the CMIP4 session with the AT. The MN-HA key shall be indexed by the MN-HA-SPI associated with this Security Association.

Upon receiving an RRQ that includes Mobile IP Revocation Support extension, the HA supporting registration revocation shall include Mobile IP Revocation Support extension in the RRP sent to the AGW. Upon receiving an RRQ that does not include Mobile IP Revocation Support extension, the HA shall assume that the AGW does not support registration revocation.

3.5.1.1 Diameter

Diameter is not supported in this release.

3.5.1.2 RADIUS

During initial CMIP4 registration, upon receiving an RRQ with the MN-AAA Authentication extension but without the MN-HA Authentication extension, the HA shall send a RADIUS Access-Request message to the HAAA, which includes the User-Name attribute, CHAP-Password attribute, CHAP-Challenge attribute, and MIP4-Mesg-ID VSA. The HA shall set the values in the User-Name attribute, CHAP-Password attribute, and CHAP-Challenge attribute according to [7]. The HA shall set the MIP4-Mesg-ID VSA equal to the value in the Identification field of the RRQ. Upon receiving a RADIUS Access-Accept message, the HA shall use the MN-HA key received in the MN-HA Shared Key VSA, to compute the MN-HA Authentication extension for the RRP 0 and send the RRP to the AT. In the MN-HA Authentication extension of the RRP, the HA shall set the SPI field to the MN-HA SPI value received in the MN-HA SPI VSA of the RADIUS Access-Accept message.

For subsequent CMIP4 registrations or re-registrations, upon receiving an RRQ with both the MN-AAA Authentication extension and the MN-HA Authentication extension, the HA shall determine, based on local policy, whether or not to request the HAAA to verify the MN-AAA authenticator in the RRQ as follows.

- i. If verification of the MN-AAA authenticator is required, the HA shall send a RADIUS Access-Request message to the HAAA according to [7].
- ii. If the verification of the MN-AAA authenticator is not required, the HA shall verify MN-HA authentication extension using the MN-HA key associated with the MN-HA SPI received in the SPI field of the MN-HA Authentication extension of RRQ.
- iii. If HA does not have the MN-HA key associated with the received MN-HA SPI, the HA shall send RADIUS Access-Request to the HAAA according to [7].

Upon receiving the RADIUS Access-Accept from the HAAA, once the MN-HA Authentication extension is verified, the HA shall send the RRQ to the AT and add this new received MN-HA key and associated MN-HA-SPI as an additional binding for the duration of the registration.

For subsequent CMIP4 registrations or re-registrations, upon receiving an RRQ with the MN-HA Authentication extension included but without MN-AAA Authentication extension included, the HA shall verify MN-HA authentication extension using the MN-HA key associated with the MN-HA SPI received in the SPI field of the MN-HA Authentication extension of RRQ. If the RRQ verification is successful, the HA shall send the RRP to the AT including the MN-HA Authentication extension computed using the MN-HA key. If the HA does not have the MN-HA key associated with the MN-HA-SPI or the verification is not successful, the HA shall reject the re-registration and send appropriate RRP to the AT (see 0.

Table 3. RADIUS Attributes between HA and AAA for Supporting CMIP4 Registration

Attribute Name	Type	Access-Request	Access-Accept	Interface(s)
User-Name	1	1	0	HA -> AAA
CHAP-Password	3	1	0	HA -> AAA
NAS-IP-Address	4	1	0	HA -> AAA
CHAP-Challenge	60	1	0	HA -> AAA
MN-HA SPI	26/57	1	1	HA <-> AAA
MN-HA-Shared-Key	26/58	0	1	HA <- AAA
MIP4-Mesg-ID	26/173	0	1	HA -> AAA

0 This attribute shall not be present.

0-1 Zero or one instance of this attribute may be present.

1 Exactly one instance of this attribute shall be present.

3.5.2 FA-HA Security

An FA-HA Mobility Security Association (MSA) or IPsec Security Association (SA) may be used to protect the CMIP4 registration messages exchanged between the AGW and HA. The usage of an IPsec SA is outside the scope of this document. The use of an FA-HA MSA is specified in the following sections.

3.5.2.1 Diameter

Diameter is not supported in this release.

3.5.2.2 RADIUS

Upon receiving an RRQ with an FA-HA Authentication extension from an AGW, the HA shall send a RADIUS Access-Request message that includes the FA-HA-MSA-Request VSA and the User-Name attribute set equal to "AGW|HA@realm". The HA shall form the "AGW|HA" by concatenating the AGW's and HA's IP addresses encoded using eight hexadecimal ASCII characters. The HA shall set the "realm" equal to the realm of the network where the HA is assigned. Upon receiving the RADIUS Access-Accept message that includes the FA-HA-MSA VSA, the HA shall use the FA-HA MSA to verify the FA-HA Authentication extension in the received RRQ. The HA shall use the FA-HA MSA to compute the FA-HA Authentication extension in the RRP sent to the AGW 0.

Table 4. RADIUS Attributes between HA and AAA for Supporting FA-HA MSA distribution

Attribute Name	Type	Access-Request	Access-Accept	Interface(s)
User-Name	1	1	0	HA -> HAAA
NAS-IP-Address	4	1	0	HA -> HAAA

Attribute Name	Type	Access-Request	Access-Accept	Interface(s)
FA-HA-MSA-Request	26/177	1	0	HA -> HAAA
FA-HA-MSA	26/178	0	1	HA <- HAAA

0 This attribute shall not be present.

0-1 Zero or one instance of this attribute may be present.

1 Exactly one instance of this attribute shall be present.

3.5.3 DHCPv4 Support

The HA shall support DHCP Relay Agent. The HA shall relay the DHCP messages according to [9] and [10]. The HA shall include a DHCP Relay Agent Information option (see [10]) when relaying DHCP messages to the DHCP server and shall set the giaddr field to the relay agent IP address.

3.5.4 Registration Revocation

If the HA supports registration revocation and if it negotiated it with the AGW during CMIP4 registration, the HA may send Registration Revocation message to the AGW as specified in the [4].

If the HA receives the Registration Revocation message from the AGW, the HA shall validate the message. Upon successful validation, the HA shall clean up the resources associated with the AT's IP address that is being revoked and send a Registration Revocation Acknowledgment message to the AGW.

3.6 AAA Requirements

After successful initial EAP authentication, if HAAA does not have a static MN-AAA key for the AT, the HAAA shall generate a dynamic MN-AAA key and its associated MN-AAA-SPI as specified in Section 3.2.

3.6.1 CMIP4 Registration

3.6.1.1 Diameter

Diameter is not supported in this release.

3.6.1.2 RADIUS

3.6.1.2.1 VAAA

Upon receiving the Access Request message from the AGW, the VAAA may perform one of the following before sending the RADIUS Access-Request message to the HAAA:

- Include the VAAA-Assigned-MIP4-HA VSA in the access Request message if the VAAA-Assigned-MIP4-HA VSA is not received from the AGW);
- Replace HA IP address received in the VAAA-Assigned-MIP4-HA VSA with another HA IP address in the visited network;

- Forward the received VAAA-Assigned-MIP4-HA VSA without modifications.

The VAAA shall not modify the VAAA-Assigned-MIP4-HA VSA and the Home Agent VSA in the Access Accept message.

3.6.1.2.2 HAAA

During the EAP access authentication of a roaming AT, upon receiving a RADIUS Access-Request message containing the VAAA-Assigned-MIP4-HA VSA, if the HAAA authorizes the visited network to assign a local HA, the HAAA shall include the VAAA-Assigned-MIP4-HA VSA in the RADIUS Access-Accept message; otherwise, the HAAA shall not include the VAAA-Assigned-MIP4-HA VSA. In either case, the HAAA may include the Home Agent VSA in the RADIUS Access-Accept message, which contains the address of an HA assigned by the HAAA in the home network.

During the initial CMIP4 registration, upon receiving a RADIUS Access-Request message from an AGW, which contains the Home Agent VSA set to zero, the HAAA shall use an MN-AAA key [4] to verify the AT's RRQ credential (i.e., MN-AAA authentication extension) conveyed in the CHAP-Password attribute of the RADIUS Access-Request message [7]. If successful, the HAAA shall select a HA and include the HA's address in the RADIUS Access-Accept message to the AGW according to [7].

During the initial CMIP4 registration, upon receiving a RADIUS Access-Request message from an AGW, which contains the VAAA-Assigned-MIP4-HA VSA, the HAAA shall use an MN-AAA key [3] to verify the AT's RRQ credential (i.e., MN-AAA authentication extension) conveyed in the CHAP-Password attribute of the RADIUS Access-Request message [7]. If successful, the HAAA shall include the appropriate HA's address in the RADIUS Access-Accept message via the Home Agent VSA and/or the VAAA-Assigned-MIP4-HA VSA (if the HAAA authorizes the visited network to assign a local HA).

During the initial CMIP4 registration, upon receiving the RADIUS Access-Request message from an HA which contains the MN-HA SPI VSA and MIP4-Mesg-ID VSA, the HAAA shall retrieve the MN-AAA key indexed by SPI received from the Access-Request (MN-AAA-SPI) and use a MN-AAA key to verify the AT's RRQ credential (i.e., MN-AAA authenticator) conveyed in the CHAP-Password attribute of the RADIUS Access-Request message [7]. If successful, and the HAAA does not have a static MN-HA key for the AT, the HAAA shall generate a dynamic MN-HA key and associated MN-HA-SPI as specified in section 3.2.

3.6.2 FA-HA Security

The method of generating an FA-HA MSA is outside the scope of this document. The use of an FA-HA MSA is specified in the following sections.

3.6.2.1 Diameter

Diameter is not supported in this release.

3.6.2.2 RADIUS

During the EAP access authentication of an inter-AGW handoff, if the AT's CMIP4 session has not been terminated (as indicated by the accounting record), the HAAA shall include the HA-Realm VSA in the RADIUS Access-Accept message. The HAAA shall set the HA-Realm VSA to the realm where the HA is allocated.

If the RADIUS Access-Request message received directly from an AGW or HA includes the FA-HA-MSA-Request VSA, and the realm in the User Name attribute (i.e.,

1
2 AGW|HA@realm) indicates the network where the AAA belongs to, the AAA shall generate
3 an FA-HA MSA and includes it in the FA-HA-MSA VSA of the RADIUS Access-Accept
4 sent to the AGW or HA.
5
6

7 **3.6.3 Reverse Tunneling**

8
9 If the reverse tunneling [5] is required for the AT, based on policy, the HAAA during EAP
10 access authentication shall include the Reverse-Tunnel-Specification VSA in the RADIUS
11 Access-Accept message.
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

4 Call Flows

4.1 Mobile IPv4 Addressing with RADIUS

Figure 3 illustrates an example call flow for Mobile IPv4 addressing. This call flow is for the initial CMIP4 registration. In this particular example, the AT requests dynamic HA and HoA assignment and uses dynamic MN-HA key and dynamic MN-AAA key.

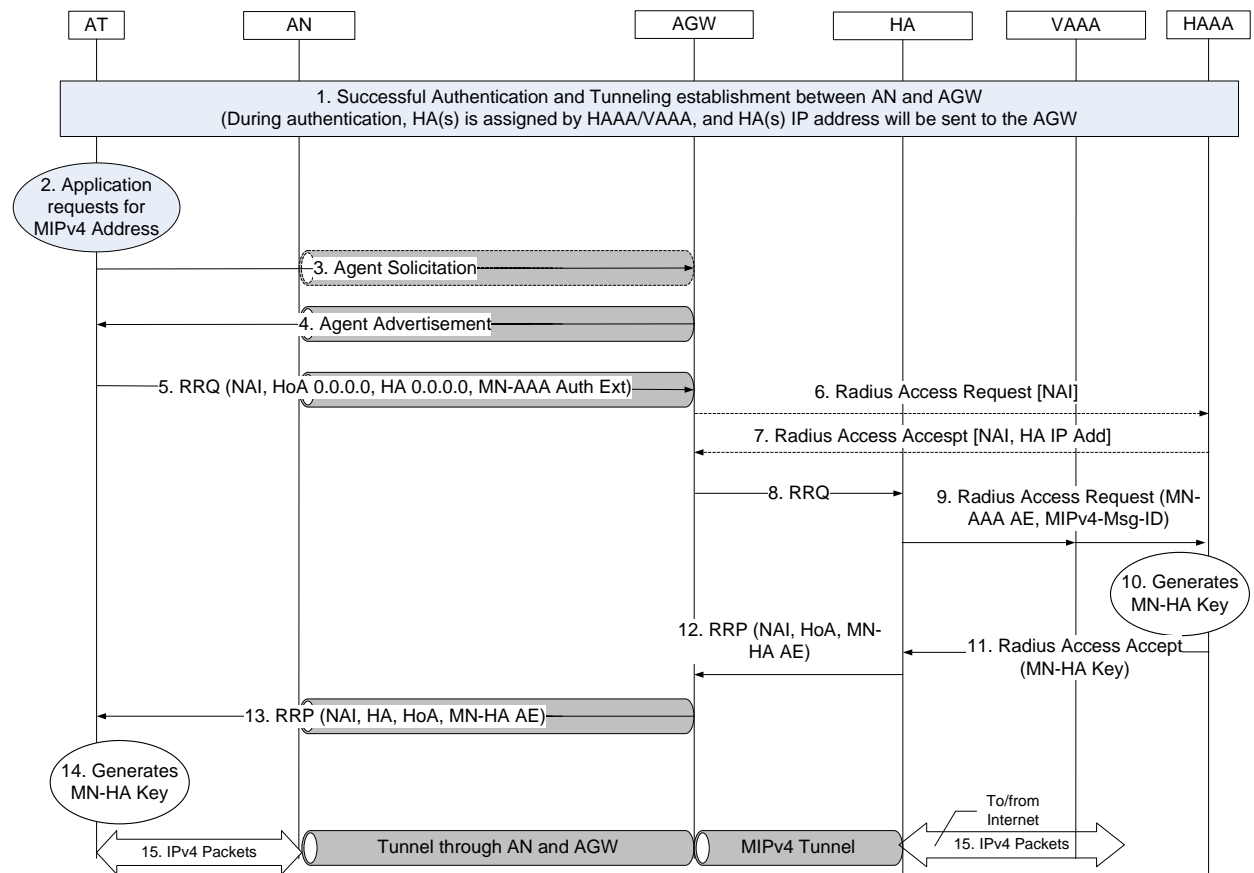


Figure 3 Mobile IPv4 Addressing with RADIUS

The steps in Figure 3 are described below.

- The AT performs a successful authentication and per AT tunnel is established between the eBS and AGW. During the EAP successful authentication and authorization, if the user profile and the policy of the HAAA allows the AT to access an HA in the visited network, the HAAA server sends the VAAA-Assigned-MIPv4-HA VSA (containing an assigned HA in the local network) along with the MIPv4-Home Agent Attribute (containing an assigned HA in the home network) to the AGW in the AAA message. If the user profile or the policy of the home network disallows the AT to access an HA in the visited network, the HAAA server omits the VAAA-Assigned-MIPv4-HA VSA Attribute but includes the MIPv4-Home Agent Attribute containing an assigned HA in the home network in the AAA message. The AGW or VAAA may insert VAAA-Assigned-MIPv4-HA Attribute containing an assigned HA in the visiting network in the Access Request message sent to the

1
2 HAAA. The details are shown up in the access authentication and authorization call
3 flow.
4

5 After successful initial EAP authentication, both AT and HAAA generate the MN-
6 AAA key and associated MN-AAA SPI as specified in Section 3.2 if the static MN-
7 AAA key is not used. Value of the SPI indicates specific security association
8 between AT and HAAA and algorithm used in computation of the MN-AAA
9 Authentication Extension.
10

- 11 2. The AT's application requests for CMIP4 address. Step 2 may occur during step 1.
- 12
- 13 3. The AT sends the Agent Solicitation message with the source IP address set to all 0
14 (if the AT doesn't have home address) and destination address set to "limited
15 Broadcast" Address (255.255.255.255). The Agent Solicitation message is sent to
16 AGW through the tunnel between the eBS and the AGW.
17
- 18 4. The AGW, acting as a CMIP4 foreign agent, sends an Agent Advertisement message
19 0 to the AT containing the AT's FA CoA and the Challenge extension [3]. The
20 Agent Advertisement message is sent to AT through the tunnel between the eBS and
21 the AGW.
22
- 23 5. The AT sends a Registration Request message 0 to the AGW through the tunneling
24 between the eBS and AGW requesting dynamic HA and HoA assignment containing
25 the MN-NAI extension [2], MN-FA Challenge extension [3], and the MN-AAA
26 Authentication extension [3]. The AT indicates that it has no preference for whether
27 the HA is assigned in the home or visited domain by specifying 0.0.0.0 in the HA
28 Address field of RRQ) or it prefers an HA in the home network (by specifying
29 255.255.255.255 in the HA Address field of RRQ). The AT also specifies an HoA of
30 0.0.0.0 in the RRQ. The AT may also indicate Reverse Tunneling by setting the "T"
31 bit in the RRQ.
32
- 33 6. If the AGW doesn't obtain HA IP address in step 1 or HA IP address is obsolete
34 based on local policy, the AGW can not determine the HA. In that case, the AGW
35 can send the RADIUS Access Request message to the HAAA. This step is optional.
36
- 37 7. Upon receiving the RADIUS Access Request message, the HAAA sends Access
38 Accept Message to AGW including HA assignment.
- 39 8. The AGW selects HA based on AT's request and authorization specified in step 1 or
40 step 7 and then sends RRQ to the proper HA.
41
- 42 9. The HA sends the RADIUS Access-Request message, via the VAAA, to the HAAA
43 to authenticate the AT's MN-AAA authenticator received in the RRQ. The RADIUS
44 Access-Request message also contains the MIP4-Mesg-ID VSA containing the
45 timestamp value from the Identification field of the RRQ.
46
- 47 10. The HAAA authenticates the user via the MN-AAA Authentication extension. The
48 HAAA calculates the MN-HA key and its associated SPI (MN-HA-SPI) if the static
49 MN-HA Key is not used for the AT.
50
- 51 11. The HAAA sends the RADIUS Access-Accept message with the MN-HA-Shared-
52 Key VSA containing the MN-HA-Shared key (IK) and MN-HA-SPI VSA containing
53 the related MN-HA-SPI. The attributes in the RADIUS Access-Accept message are
54 protected by the Message Authentication attribute.
55
- 56 12. The HA generates the RRP, which includes the Mobile-Home Authentication
57 Extension 0 computed by the HA based on the MN-HA-Shared key, AT's Home
58 Address, HA's address, and NAI. The HA sends the RRP to the AGW.
59
60

13. The AGW forwards the RRP to the AT after storing the received HoA of AT in the RRP.
14. Upon receiving the HA address in the RRP, the AT derives the MN-HA key and its associated MN-HA-SPI. The AT then verifies the Mobile-Home Authentication Extension in the received RRP.
15. The AT sends/receives IPv4 packets to/from the HA through the CMIP4 tunnel between the HA and AGW and the tunnel between the eBS and AGW.

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