

3GPP2 X.S0044-0

Version 1.0

Date: September 17, 2010



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

Mobile IPv4 Enhancements

©2010 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.

Revision History

Revision		Date
Rev. 0 v1.0	Initial Publication	September 2010

Document Title: Mobile IPv4 Enhancements

CONTENTS

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	Definitions, Symbols and Abbreviations.....	3
7	3.1 Definitions	3	
8	3.2 Symbols and Abbreviations	3	
9	4	General Requirements and Backward Compatibility	5
10	5	MIP4 Key Derivation.....	6
11	5.1 MN-AAA Key and associated SPI.....	6	
12	5.2 MN-HA key and associated SPI	6	
13	6	MS Requirements.....	8
14	7	PDSN Requirements	9
15	8	AAA Requirements	10
16	9	HA Requirements.....	11
17	10	Allocation of Home Agent in Visited Network.....	12
18	10.1 Dynamic MIP4 HA Assignment in the Visited Network using RADIUS	12	
19	11	FA-HA Mobility Security Association.....	14
20	11.1 Call Flow Example for Using RADIUS to Distribute FA-HA MSA	15	
21	12	AAA VSAs and Version Capability Extensions	18
22	12.1 RADIUS VSAs	18	
23	12.1.1 MIP4-HA-Local-Assignment-Capability	18	
24	12.1.2 HA-Realm.....	19	
25	12.1.3 FA-HA-MSA-Request.....	19	
26	12.1.4 FA-HA-MSA	20	
27	12.1.5 MIP4-Enhancements-Support.....	20	
28	12.2 Version Capability Extension	21	
29			
30			
31			
32			
33			
34			
35			
36			
37			
38			
39			
40			
41			
42			
43			
44			
45			
46			
47			
48			
49			
50			
51			
52			
53			
54			
55			
56			
57			
58			
59			
60			

LIST OF FIGURES

<i>Figure 1</i>	Dynamic Allocation of an HA in a Visited Network Using RADIUS Protocol	12
<i>Figure 2</i>	HA assignment by VAAA in Visited Network A and handoff to Visited Network B if RADIUS is used to distribute FA-HA MSA.....	16
<i>Figure 3</i>	MIP4-HA-Local-Assignment-Capability VSA.....	18
<i>Figure 4</i>	HA-Realm VSA	19
<i>Figure 5</i>	FA-HA-MSA-Request VSA	19
<i>Figure 6</i>	FA-HA-MSA VSA	20
<i>Figure 7</i>	MIP4-Enhancemnts-Support VSA.....	20

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

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

<i>Table 1</i>	VSA Cross Reference	18
<i>Table 2</i>	List of PDSN Capabilities.....	21

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 contains enhancements to X.S0011-D and later versions for the ability to dynamically allocate a Mobile IPv4 Home Agent in a visited network. This document supplements the functionality as specified in X.S0011-D and later versions and supersedes those documents where indicated. The protocols used to implement this functionality are defined by several IETF RFCs as listed in the References section. This document ties together the use of those protocols in a cdma2000® network to accomplish the functionality needed to allocate a Home Agent in a visited network to an MS.

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.S0044-X-n

where:

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

This document uses the following conventions:

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

1 Introduction

X.S0011-D [2] describes how a Mobile IPv4 MS can request and be granted or denied the dynamic allocation of a Home Agent in its home network. This document describes the following aspects of this functionality.

1. How the MS can indicate its willingness to accept a Home Agent in the visited network
2. How the visited network signals its willingness (or not) to allocate a Home Agent
3. How the MS user's home network signals its willingness (or not) to allow visited network allocation of a Home Agent
4. How the keys needed to establish a security association between the MS and visited network Home Agent are derived and distributed

This document describes methods for the dynamic allocation of a Home Agent in a visited network using RADIUS [1]. This document does not define Diameter based protocols.

Chapter 2, section 4 of [2] specifies the use of Mobile IPv4 by an MS and the interactions/interfaces between the MS, PDSN and other elements of the access network involved in the establishment of a Mobile IPv4 session. The same method used for allocating a Home Agent in a visited network is also applicable for allocating a Home Agent in an MS user's home network. Implementations of Mobile IPv4 Enhancements presented in this document are expected to conform to the RFCs referenced in this document with any extensions or limitations as given in this document.

1.1 Scope

This document provides additional functionality to the functionality specified in [2] and later versions. It supports the allocation of a Home Agent in a visited network when a user is operating in a network that is not its home network.

2 References

2.1 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Specification. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- For non-specific reference, the latest version applies. In the case of a reference to a 3GPP2 document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

- [1] IETF: RFC 2865; C. Rigney, ‘*Remote Authentication Dial In User Service (RADIUS)*’, June 2000.
- [2] 3GPP2: X.S0011-D v2.0; ‘*cdma2000 Wireless IP Network Standard*’, October 2008.
- [3] IETF: RFC 5295; J. Salowey, et. al., ‘*Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)*’, August 2008.
- [4] National Institute of Standards and Technology: ‘*“Secure Hash Standard”, FIPS 180-2, With Change Notice 1 dated February 2004*’, August 2002.
- [5] IETF: RFC 2002; Perkins, ‘*IPv4 Mobility*’, May 1995.
- [6] 3GPP2: X.S0028-200; ‘*Access to Operator Service and Mobility for WLAN Interworking*’.

2.2 Informative References

There is no informative reference specified in this document.

3 Definitions, Symbols and Abbreviations

This section contains definitions, symbols and abbreviations that are used throughout the document.

3.1 Definitions

Home Network

A mobile station's home network is the network owned by the operator with whom the mobile station user has a business relationship via a service subscription.

Visited Network

A visited network is a network with a coverage area which includes the current location of a mobile station, and that network is not the mobile station's home network. A visited network may or may not provide service to the mobile station depending on the business relationship between the user's home network and the visited network, as well as the mobile station's (and its user) authentication and authorization status.

Serving Network

The serving network can be the home network or the visited network.

MIP4 Enhancements Capable

Refers to a capability of a cdma2000^{®1} network element to support the functionality required to request or dynamically allocate a Home Agent in a visited network as described in this document.

3.2 Symbols and Abbreviations

The following are examples of the appearance of abbreviations:

IETF	Internet Engineering Task Force
IK	Integrity Key
HoA	Home Address
RRQ	Registration Request message
FA	Foreign Agent
RRP	Registration Reply message
HA	Home Agent
MN	Mobile Node
MS	Mobile Station (this includes HRPD Access Terminals (AT))

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.

MSA	Mobility Security Association	1
MIP4	Mobile IPv4	2
SPI	Security Parameter Index	3
H-AAA	Home Authentication, Authorization and Accounting Server	4
V-AAA	Visited Authentication, Authorization and Accounting Server	5
VSA	Vendor-Specific Attribute	6
		7
		8
		9
		10
		11
		12
		13
		14
		15
		16
		17
		18
		19
		20
		21
		22
		23
		24
		25
		26
		27
		28
		29
		30
		31
		32
		33
		34
		35
		36
		37
		38
		39
		40
		41
		42
		43
		44
		45
		46
		47
		48
		49
		50
		51
		52
		53
		54
		55
		56
		57
		58
		59
		60

4 General Requirements and Backward Compatibility

All requirements in this document apply only to specific network elements when operating on behalf of a MIP4 Enhancements Capable MS.

The network shall be able to distinguish between

- a legacy mobile which may use 0.0.0.0 and 255.255.255.255 interchangeably in the HA Address Field of the RRQ when requesting dynamic allocation of an HA, and
- an MS conforming to this document which can make a more specific request for the location of the HA.

Profile information (containing device information) stored in the AAA shall include a MIP4 Enhancements Capable capability indicator that will indicate that the mobile conforms to this document and is able to distinguish between home agent addresses set to 0.0.0.0 (indicating willingness to accept an HA in either home or visited network) and 255.255.255.255 (indicating mobile's preference for an HA in the home network) in the RRQ.

A MIP4 Enhancements Capable MS will always use dynamic MN-HA keying versus static MN-HA keying. Therefore, when a mobile station with this indicator set is allocated an HA (either in the home or visited network) both the MS and H-AAA shall derive the key as described in section 5, and the H-AAA shall distribute the derived key to the allocated HA.

5 MIP4 Key Derivation

This section describes the method that shall be used to derive the MN-AAA key and the MN-HA key from a secret shared between an MS and the Home AAA. The shared secret is denoted as MIP4-MN-RK.

The MIP4-MN-RK key shall be 64 octets and is derived from Extended Master Session Key (EMSK) as specified in [3] with the following considerations:

- The Key Derivation Function (KDF) function shall be HMAC-SHA256 as per [4].
- If EMSK is available, the EMSK shall be used as specified in [3].
- If EMSK is not available, the MN-AAA key shall be used as the EMSK in the formulas specified in [3].
- If neither EMSK nor MN-AAA is available, the CHAP-SS (Shared Secret) shall be used as the EMSK in the formulas specified in [3].
- The key label shall be “mip4mnrk@cdma2000.3gpp2.org” specified in lower case printable ASCII and the string shall not be null terminated.
- Optional Data is not used.
- The length shall be 0x0040 in network byte order.

5.1 MN-AAA Key and associated SPI

From the MIP4-MN-RK, the MN-AAA key and its associated MN-AAA-SPI shall be derived as follows:

MN-AAA key = HMAC-SHA-256 (MIP4-MN-RK, “mnaaakey@cdma2000.3gpp2.org”)

MN-AAA-SPI = HMAC-SHA-256 (MN-AAA key, “mnaaspi@cdma2000.3gpp2.org”)

The MN-AAA-SPI indicates the specific security association between the MS 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 MS, then the SPI value shall be monotonically incremented until the SPI value has no collision for that MS.

5.2 MN-HA key and associated SPI

From the MIP4-MN-RK, the MN-HA key and its associated MN-HA-SPI shall be derived as follows:

MN-HA key = HMAC-SHA-256 (MIP4-MN-RK, Nonce, “mnhakey@cdma2000.3gpp2.org”, HA IP Address), where Nonce shall be equal to the value set by the MS in the Identification field of the RRQ during the initial MIP4 registration [5]. The H-AAA obtains the Identification field Value from the HA via the MIP4-Mesg-ID VSA [6].

1 MN-HA-SPI = HMAC-SHA-256 (MN-HA key, “mnhaspi@cdma2000.3gpp2.org”)
2

3 The MN-HA-SPI indicates the specific security association between the MS and HA and
4 algorithm used in computation of the MN-HA Authentication Extension. If the value of this
5 computed MN-HA-SPI is equal to or smaller than 255, then an integer value of 256 shall be
6 added to the computed value. If the MN-HA-SPI collides with another SPI value already
7 allocated for the MS, then the SPI value shall be monotonically incremented until the SPI
8 value has no collision for that MS.
9

10
11 Using the same rules for SPI calculation at the MS and the HAAA results in same unique SPI
12 value at both ends.
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 MS Requirements

Mobile Stations that comply to this document shall comply to [2] with the following exceptions and additions:

- The MS shall perform access authentication procedures during PPP establishment.
- During PPP setup, when the MS receives the MS-PDSN Version Capability Indication packet from the PDSN and if the MIP4 enhancements bit in the List of PDSN capabilities field is set, the MS should initiate MIP4 registration according to this document. Otherwise, the MS should initiate MIP4 registration according to [2].
- During initial MIP4 registration when the MS does not have a valid MN-HA key with an assigned HA, the MS shall include the MN-AAA Authentication Extension in the RRQ without the MN-HA Authentication Extension. During subsequent MIP4 re-registrations with the same assigned HA, the MS shall include both the MN-AAA Authentication Extension and the MN-HA Authentication Extension in the RRQ. Upon receiving RRP, the MS shall derive the MN-HA key and verify the MN-HA Authentication Extension. If RRP authentication is successful, the MS shall save the MN-HA AE SPI to track the session MN-HA MSA. The MS shall use this SPI in the SPI field of the MN-HA AE in all future re-registration RRQ messages with the same HA.

7 PDSN Requirements

The requirements set forth in this section are for PDSNs that comply to this document. The PDSNs that comply to this document shall comply to [2] with the following exceptions and additions.

- During PPP setup, the PDSN shall perform access authentication procedures. Upon receiving MIP4-Enhancements-Support VSA from the AAA, the PDSN should indicate its MIP4 enhancements support to the MS. The PDSN should set the MIP4 enhancements bit in the List of PDSN capabilities field when it sends the MS-PDSN Version Capability Indication packet to the MS. If the MIP4-Enhancements-Support VSA is not received from the AAA, the PDSN shall not set C6 bit to '1' in MS-PDSN Version Capability Indication packet.
- The absence of the MN-HA AE in the initial RRQ is the indication that the MS is compliant to this specification. During the initial RRQ, the PDSN shall not remove the MN-AAA AE contained in the RRQ before forwarding it to the HA regardless of the presence of MN-AAA Removal Indication VSA in the Access-Accept.
- If the PDSN receives initial RRQ without the MN-HA AE and the PDSN has not communicated MIP4 enhancements support to the MS via C6 bit in MS-PDSN Version Capability Indication packet, the PDSN shall send RRP with code field set to "poorly formed request" (code 70).
- If the HA address field is set to 0.0.0.0 (indicating willingness to accept an HA in either home or visited network) in the RRQ, and if the MN-HA Authentication Extension is absent from the RRQ (indicating that the MS is MIP4 Enhancements capable and is capable of deriving MN-HA key per section 5), then based on the local policy the PDSN may include the MIP4-HA-Local-Assignment-Capability VSA in the RADIUS Access-Request message to indicate a request for dynamic HA assignment in the visited network.

If the PDSN receives the HA-Authorized VSA in the RADIUS Access-Accept message, based on the local policy the PDSN may assign an HA to the MS. If the PDSN assigns an HA, the PDSN shall forward the RRQ to that HA. If the local policy dictates that the V-AAA assigns the HA in the visited network, the PDSN shall forward the RRQ to the HA address given in the Home Agent VSA [2] from the V-AAA.

8 AAA Requirements

AAA servers that comply to this document shall also support [2], subject to the following additions/exceptions.

- During access authentication, the AAA shall perform the following:
 - If profile information (containing device information) stored in the HAAA includes a MIP4 Enhancements Capable capability indicator, upon receiving the RADIUS Access-Request from the PDSN, the HAAA shall include MIP4-Enhancement-Support VSA in the Access-Accept message if the HAAA and at least one of HAs support MIP4 enhancements specified in this document.
 - If the VAAA receives MIP4-Enhancements-Support VSA in the Access-Accept message from the HAAA, and the VAAA and at least one of HAs support MIP4 enhancements, the VAAA shall forward the Access-Accept message including the MIP4-Enhancements-Support VSA to the PDSN. Otherwise, the VAAA shall remove MIP4-Enhancements-Support VSA if any and forward the Access-Accept message to the PDSN.
- Upon receiving the RADIUS Access-Request with the MIP4-HA-Local-Assignment-Capability VSA from a PDSN, if the MS's Foreign Agent Challenge response is authenticated successfully, and dynamic HA assignment in the visited network is authorized, the H-AAA shall include the HA-Authorized VSA in the RADIUS Access-Accept.
- If the H-AAA includes the HA-Authorized VSA in the RADIUS Access-Accept message, based on the local policy the V-AAA should assign an HA which supports MIP4 enhancements to the MS based on local policy. If the V-AAA assigns an HA, the V-AAA shall include the Home Agent VSA [2] in the Access-Accept before forwarding the Access-Accept message to the PDSN.
- When the H-AAA receives a RADIUS Access-Request with the MIP4-Mesg-ID VSA from an HA, the H-AAA server shall authenticate the user based on the MN-AAA key via the MN-AAA Authentication Extension. The presence of the MIP4-Mesg-ID VSA in the Access Request shall indicate to the H-AAA that the MS is MIP4 Enhancements capable. The MIP4-Mesg-ID shall be used to calculate the MN-HA key. If the MS is authenticated based on the MN-AAA AE, and the MN-HA SPI VSA with a value of 5 was received in the RADIUS Access-Request, the H-AAA shall generate the MN-HA key and a unique MN-HA SPI for this session. The H-AAA shall send to the HA a RADIUS Access-Accept that includes the MN-HA-Shared-Key VSA containing MN-HA key, MN-HA SPI VSA containing the unique dynamically generated MN-HA-SPI and the Message Authenticator attribute.
- If the MS is a MIP4 enhanced MS, the H-AAA shall not send the MN-AAA Removal Indication VSA in the RADIUS Access-Accept to the PDSN to remove the MN-AAA AE from an RRQ delivered by that MS.
- The H-AAA shall not assign an HA address in a visited network.

9 HA Requirements

The HA allocated in a visited or home network shall process an RRQ and RRP according to [2] with the following exceptions.

- If the MN-HA Authentication Extension is absent in the RRQ, the HA shall include the MN-HA SPI VSA with a value 5 in the RADIUS Access-Request to request for the MN-HA Security Association. In this document, it is limited to the MN-HA key, and the MN-HA SPI. The HA shall copy the Identification field value of the RRQ into the MIP4-Mesg-ID VSA of the RADIUS Access-Request. (The value of the Identification field is needed for the H-AAA to derive the MN-HA key per section 5).
- The HA shall process the MN-AAA authentication extension using the method indicated in [2]. The RRP shall be processed according to [2].
- When an HA is using RADIUS and an MS is allocated an HA, for the first MIP4 registration from the MS when the MS and HA do not have a session key, the HA shall include the MN-HA SPI VSA with a value of 5 to receive a newly generated MN-HA key and MN-HA SPI from the H-AAA. For subsequent MIP4 registrations to the same HA from the same MS, the HA shall not include the MN-HA SPI with a value of 5 and MIP4-Mesg-ID VSA in the RADIUS Access-Request.
- For the subsequent MIP4 re-registrations from the MS, the HA shall determine via local network policy if the MN-AAA AE is sent to the H-AAA for validation.
- When the HA receives RADIUS Access-Accept with the MN-HA-Shared-Key VSA and the MN-HA SPI VSA, the HA shall use the MN-HA SPI to index the MN-HA MSA for the MN session for the rest of the session lifetime. The HA shall use the received SPI in the MN-HA AE SPI field in the RRP message sent to MS.

10 Allocation of Home Agent in Visited Network

10.1 Dynamic MIP4 HA Assignment in the Visited Network using RADIUS

Figure 1 shows an example call flow for dynamic MIP4 HA assignment in a visited network. In this call flow example, the H-AAA authorizes the visited network to assign an HA to the MS. The MN-HA key is derived per section 5 based on the MIP4-MN-RK secret shared between the MS and H-AAA, and is distributed from the H-AAA to the assigned HA via RADIUS.

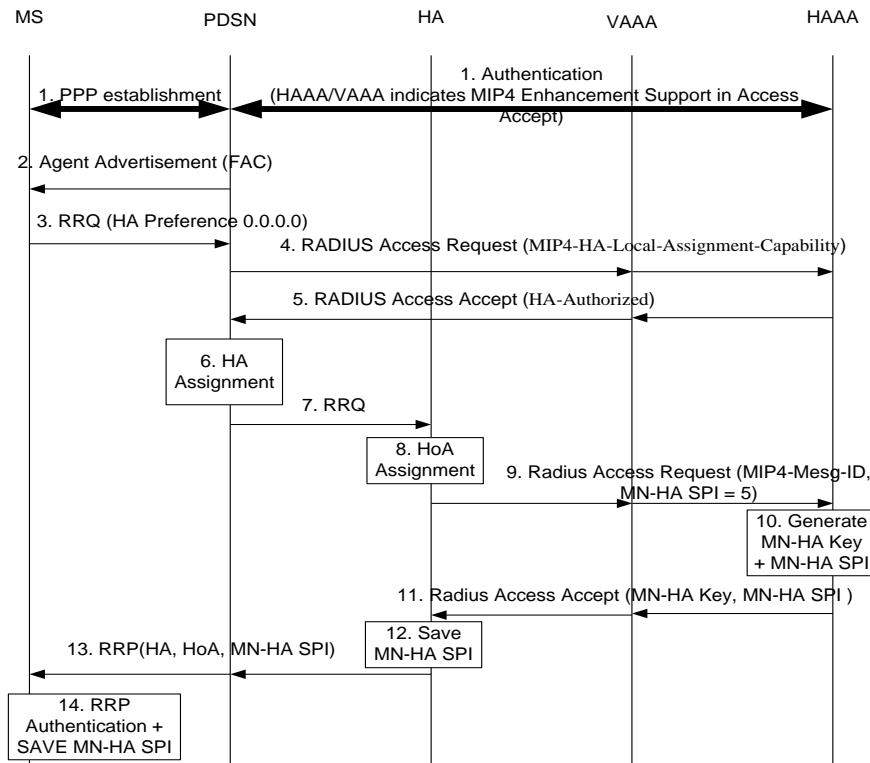


Figure 1 Dynamic Allocation of an HA in a Visited Network Using RADIUS Protocol

1. PPP session is established between the MS and PDSN. During PPP establishments, the access authentication procedures (EAP, CHAP, or PAP) are performed. The HAAA/VAAA indicates the capability on MIP4 enhancements support to the PDSN via MIP4-Enhancements-Support VSA. If both the PDSN and AAA support MIP4 enhancements, the PDSN indicates it to the MS through MS-PDSN Version Capability Indication.
2. The PDSN sends Agent Advertisements that include the MN-FA Challenge Extension.
3. The MS sends MIP RRQ with MN-NAI Extension, MN-FA Challenge Extension, and MN-AAA Authentication Extension. The Home Address (HoA) field of the RRQ is set to zero to request a dynamic HoA. The HA field of RRQ is set to 0.0.0.0.

- 1 4. The PDSN sends a RADIUS Access-Request via the V-AAA to the H-AAA to
2 authenticate the MS's MN-AAA authenticator received in the RRQ. The RADIUS
3 Access-Request also includes the MIP4-HA-Local-Assignment-CapabilityVSA
4 indicating a request for dynamic HA assignment in the visited network.
- 5 5. The H-AAA authenticates the MS successfully and sends the RADIUS Access-Accept
6 that contains the HA-Authorized VSA to authorize the visited network to assign an HA to
7 the MS.
- 8 6. Based on the visited network policy, the PDSN assigns an HA that supports MIP4
9 enhancements from the visited network.
- 10 7. The PDSN forwards the RRQ to the assigned HA.
- 11 8. The HA assigns an HoA for the MS.
- 12 9. The HA in the visited cdma2000 system sends a RADIUS Access-Request, via the V-
13 AAA, to the H-AAA to authenticate the MS's MN-AAA authenticator received in the
14 RRQ. The RADIUS Access-Request also contains the MN-HA SPI VSA with a value of
15 5 for requesting an MN-HA MSA, which is limited to the MN-HA key, the unique
16 dynamically allocated MN-HA SPI,, and the MIP4-Mesg-ID VSA containing the
17 timestamp value from the Identification field of the RRQ.
- 18 10. The H-AAA authenticates the user via the MN-AAA Authentication extension. The H-
19 AAA calculates the MN-HA key and generates a unique MN-HA SPI.
- 20 11. The H-AAA sends a RADIUS Access-Accept with the MN-HA-Shared-Key VSA
21 containing the MN-HA key (IK) and the MN-HA SPI VSA containing the unique MN-
22 HA SPI. The attributes in the RADIUS Access-Accept are protected by the Message
23 Authentication attribute.
- 24 12. The HA saves the received MN-HA SPI and uses it to track this session MN-HA MSA.
- 25 13. The HA generates the RRP which includes the MN-HA Authentication Extension
26 computed by the HA based on the MN-HA-Shared key with the SPI field is set to the
27 MN-HA SPI value, which was received from H-AAA. The HA sends the RRP to the
28 PDSN that forwards it to the MS.
- 29 14. The MS derives the MN-HA key and verifies the MN-HA Authentication Extension in
30 the received RRP. If RRP authentication is successful, the MS saves the MN-HA AE SPI
31 to track the session MN-HA MSA. The MS uses this SPI in the SPI field of the MN-HA
32 AE in all future re-registration RRQ messages with the same HA.

11 FA-HA Mobility Security Association

The requirements in this section are applicable only if FA-HA Mobility Security Association (MSA) is required to protect MIP signaling messages exchanged between PDSN and HA, and the PDSN and HA do not have a MSA. Alternatively, an IPsec SA may be used to protect MIP signaling messages exchanged between the PDSN and HA, but the establishment of the IPsec SA is outside the scope of this document.

If RADIUS is used, the following requirements are applicable for the distribution of FA-HA MSA:

- During initial MIP4 registration, upon receiving an RRQ with the HA address field equal to 0.0.0.0, the PDSN shall send a RADIUS Access Request that includes User-Name attribute, MIP4-HA-Local-Assignment-Capability VSA, and FA-HA-MSA-Request VSA. The MIP4-HA-Local-Assignment-Capability VSA shall contain the realm of the visited network to which the PDSN belongs. The User-Name attribute shall contain the MS's NAI from the RRQ. If the HAAA authorizes the visited network to assign a dynamic HA, the HAAA shall not include the FA-HA-MSA VSA in the RADIUS Access-Accept. Otherwise, the HAAA shall include the FA-HA-MSA VSA in the RADIUS Access-Accept.
- During MIP4 handoff, upon receiving an RRQ with the HA address field equal to a non-zero value, the PDSN shall send a RADIUS Access Request destined for the HAAA to verify the MN-AAA authenticator. If the authentication is successful, the HAAA shall send a RADIUS Access Accept that includes HA-Realm VSA. The HAAA shall set the HA-Realm VSA equal to the realm of the visited network, which was received previously in the MIP4-HA-Local-Assignment-Capability VSA.
- Upon receiving a RADIUS Access-Accept that includes HA-Realm VSA (containing the HA's realm) from the HAAA as a result of successful MN-AAA authentication, the PDSN shall check whether the HA is in the same realm as the PDSN. If the HA and PDSN are in the same realm, the PDSN shall send RADIUS Access Request that includes FA-HA-MSA-Request VSA and User-Name attribute set equal to "PDSN|HA" which is the concatenation of the PDSN's address and HA's address, and each address is encoded using eight hexadecimal ASCII characters. If the HA and PDSN are in the different realms, the PDSN shall send RADIUS Access Request that includes FA-HA-MSA-Request VSA and User-Name attribute that is set equal to "PDSN|HA@realm", where the "realm" is the HA's realm.
- If the VAAA receives from the HAAA a RADIUS Access-Accept that includes HA-Authorized VSA, and the VAAA previously received from the PDSN the RADIUS Access-Request that includes FA-HA-MSA-Request VSA, the VAAA shall send a RADIUS Access-Accept that includes FA-HA-MSA VSA.
- If VAAA receives a RADIUS Access-Request that includes FA-HA-MSA-Request VSA and User-Name attribute set equal to "PDSN|HA" or "PDSN|HA@realm", the VAAA shall send a RADIUS Access-Accept that includes FA-HA-MSA VSA.
- Upon receiving an RRQ with FA-HA Authentication Extension, the HA shall send a RADIUS Access-Request that includes FA-HA-MSA-Request VSA and User-Name attribute set equal to "PDSN|HA".
- The PDSN and HA shall use the FA-HA MSA to compute the FA-HA Authentication Extension in RRQ and RRP.

- If the FA-HA MSA is about to expire in the HA, the HA shall send a RADIUS Access-Request that includes FA-HA-MSA-Request and User-Name attribute set equal to “PDSN|HA”. If the FA-HA MSA is about to expire in the PDSN/FA, it shall send RADIUS Access-Request that includes FA-HA-MSA-Request and User-Name attribute. In this latter case, if the FA and HA are in the same realm, the User-Name attribute shall be set equal to “PDSN|HA”; otherwise, the User-Name attribute shall be set equal to “PDSN|HA@realm”, where the “realm” is the HA’s realm.

11.1 Call Flow Example for Using RADIUS to Distribute FA-HA MSA

Figure 2 depicts a call flow example when the MS is dynamically assigned an HA by the VAAA in Visited Network A, and later the MS is handed off to a PDSN in Visited Network B while maintaining the same MIP session with the HA in Visited Network A. In this example, RADIUS is used to distribute FA-HA MSA.

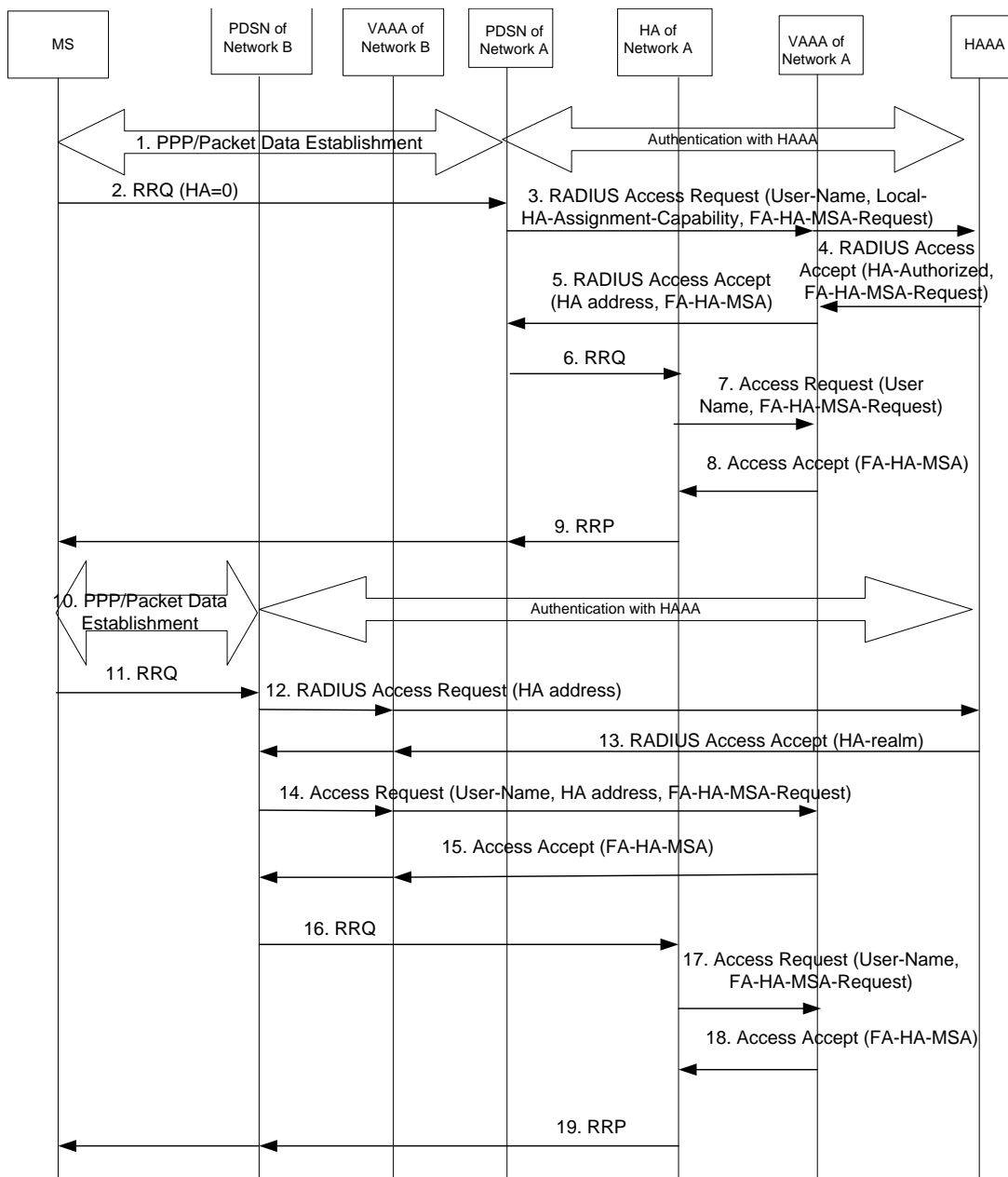


Figure 2 HA assignment by VAAA in Visited Network A and handoff to Visited Network B if RADIUS is used to distribute FA-HA MSA

1. The MS and PDSN establish PPP in Visited Network A.
2. The MS sends RRQ to PDSN.
3. Upon receiving the RRQ, the PDSN sends RADIUS Access Request containing the User-Name attribute (containing MS's NAI), MIP4-HA-Local-Assignment-CapabilityVSA, and FA-HA-MSA-Request (requesting FA-HA MSA) to the HAAA. The MIP4-HA-Local-Assignment-CapabilityVSA contains the realm of the Visited Network A.
4. The HAAA sends RADIUS Access-Accept containing FA-HA-MSA-Request VSA and Local-HA-Assignment-Authorized VSA that authorizes the visited network A to assign a

1 local HA. Therefore, the HAAA does not distribute FA-HA MSA in the RADIUS
2 Access Accept but include the FA-HA-MSA-Request VSA that was received in the
3 RADIUS Access-Request.

- 4
- 5 5. The VAAA in Visited Network A assigns a HA. V-AAA includes the Home-Agent VSA
6 [2] and FA-HA-MSA VSA in the RADIUS Access Request sent to the PDSN. The FA-
7 HA-MSA is unique per pair of PDSN and HA.
- 8
- 9 6. The PDSN forwards the RRQ to the HA. The RRQ contains the FA-HA Authentication
10 Extension computed using the FA-HA-MSA.
- 11
- 12 7. The HA sends RADIUS Access-Request containing the User-Name attribute (set equal to
13 "PDSN|HA", i.e., concatenation of the PDSN's address and HA address) and the FA-HA-
14 MSA VSA. Since the User-Name attribute content doesn't contain any realm, the
15 RADIUS message will be routed and terminated at the VAAA in the visited network A.
- 16
- 17 8. Based on the pair of PDSN and HA addresses, the VAAA sends the appropriate FA-HA-
18 MSA to the HA via the RADIUS Access-Accept.
- 19
- 20 9. The HA processes the RRQ and returns RRP to the MS via the PDSN in Visited Network
21 A. The RRP contains the FA-HA Authentication Extension computed using the FA-HA
22 MSA.
- 23
- 24 10. The MS is handoff to a PDSN in Visited Network B. The MS and PDSN establish PPP
25 in Visited Network B.
- 26
- 27 11. The MS sends RRQ to PDSN.
- 28
- 29 12. Upon receiving the RRQ, the PDSN sends RADIUS Access Request, including the
30 Home-Agent VSA according to [2], to the HAAA for the authentication of the FA
31 challenge response.
- 32
- 33 13. The HAAA sends RADIUS Access Accept to the PDSN in Visited Network B. Since
34 HAAA from step 3 knows the realm of the Visited Network A where the MS's HA is
35 resided, the HAAA returns the HA-Realm VSA in the RADIUS Access-Accept.
- 36
- 37 14. The PDSN checks whether it already has FA-HA MSA with the HA. If the PDSN does
38 not have it, the PDSN needs to obtain the FA-HA MSA from the VAAA in the Visited
39 Network A. The PDSN sends RADIUS Access-Request that contains User-Name
40 attribute, Home-Agent VSA, and FA-HA-MSA-Request VSA. The User-Name attribute
41 is set to "PDSN|HA@realm", where "realm" is the HA's realm obtained in step 13. This
42 ensures that the RADIUS Access Request will be routed to the VAAA in network A.
- 43
- 44 15. The VAAA in network A sends RADIUS Access-Accept containing the FA-HA MSA.
- 45
- 46 16. ~ 19. Similar to steps 6 ~ 9.
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60

12 AAA VSAs and Version Capability Extensions

This section covers the definition of VSAs that are created for the MIP4 Enhancements capability. This section also provides references to the documents that define other vendor specific VSAs used by this capability.

Table 1 VSA Cross Reference

VSA Name	Reference
MIP4-Mesg-ID VSA	[6]
MN-AAA Removal Indication VSA	[2]
MIP4-HA-Local-Assignment-Capability VSA	Section 12.1.1
HA-Request VSA	[6]
HA-Authorized VSA	[6]
Home Agent VSA	[2]
MIP4-Enhancements-Support VSA	Section 12.1.5
HA-Realm VSA	Section 12.1.2
FA-HA-MSA-Request VSA	Section 12.1.3
FA-HA-MSA VSA	Section 12.1.4
MN-HA-Shared-Key VSA	[2]
MN-HA SPI VSA	[2]

12.1 RADIUS VSAs

12.1.1 MIP4-HA-Local-Assignment-Capability

The presence of this 3GPP2-specific VSA in the RADIUS Access-Request message indicates that the visited network supports local HA assignment function and requests the authorization to assign a HA for the MS. This VSA contains the realm of the visited network. This VSA may be included in the RADIUS Access-Request message.

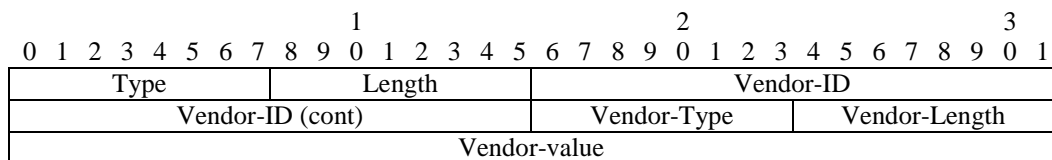


Figure 3 MIP4-HA-Local-Assignment-Capability VSA

Type: 26

Length \geq 12

Vendor ID: 5535

Vendor-Type = 175
 Vendor-Length ≥ 6
 Vendor-Value = Realm of the visited network

12.1.2 HA-Realm

This 3GPP2-specific VSA contains the realm of the visited network where the HA resides. This VSA may be included in the RADIUS Access-Accept message.

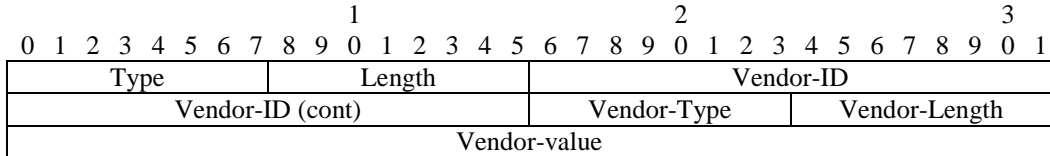


Figure 4 HA-Realm VSA

Type: 26
 Length ≥ 12
 Vendor ID: 5535
 Vendor-Type = 176
 Vendor-Length ≥ 6
 Vendor-Value = Realm of the visited network where the HA resides

12.1.3 FA-HA-MSA-Request

This 3GPP2-specific VSA is used by the PDSN or HA to request a FA-HA MSA. This VSA may be included in the RADIUS Access-Request message.

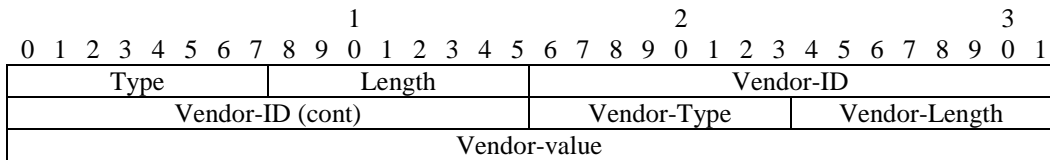


Figure 5 FA-HA-MSA-Request VSA

Type: 26
 Length = 12
 Vendor ID: 5535
 Vendor-Type = 177
 Vendor-Length = 6
 Vendor-Value =
 1: The PDSN wants a FA-HA MSA.
 Other values are reserved.

12.1.4 FA-HA-MSA

This 3GPP2-specific VSA contains the MSA for a pair of FA and HA. This VSA may be included in the RADIUS Access-Accept message.

1										2										3											
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										Length										Vendor-ID											
Vendor-ID (cont)															Vendor-Type										Vendor-Length						
SPI																															
MSA																															

Figure 6 FA-HA-MSA VSA

Type: 26

Length ≥ 16

Vendor ID: 5535

Vendor-Type = 178

Vendor-Length ≥ 10

SPI = The SPI of the MSA

MSA = FA-HA MSA

12.1.5 MIP4-Enhancements-Support

The presence of this 3GPP2-specific VSA in the RADIUS Access-Accept message indicates that the home network or visited network supports MIP4 enhancements specified in this document. This VSA may be included in the RADIUS Access-Request message.

1										2										3											
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										Length										Vendor-ID											
Vendor-ID (cont)															Vendor-Type										Vendor-Length						
Vendor-value																															

Figure 7 MIP4-Enhancemnts-Support VSA

Type: 26

Length ≥ 12

Vendor ID: 5535

Vendor-Type = 218

Vendor-Length ≥ 6

Vendor-Value =

1: The AAA and at least one of HAs under the AAA domain support MIP4 enhancements specified in this document.

Other values are reserved.

12.2 Version Capability Extension

The List of PDSN Capabilities is coded as a bit mask defined in Table 2. C0 is the most-significant bit in the list. Each bit in the list indicates whether a PDSN capability is supported. C6 is the MIP4 enhancements bit. Table 1 contains additions and changes to the “List of MS Capabilities” table in [2] and does not reflect additions or changes via other documents.

Table 2 List of PDSN Capabilities

Bits	PDSN	Description
C6	MIP4 enhancements	Set to 1 if network supports the MIP4 enhancements