Diameter Mobile IPv6: NAS <-> HAAA Support
draft-ietf-dime-mip6-integrated-03.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any
applicable patent or other IPR claims of which he or she is aware
have been or will be disclosed, and any of which he or she becomes
aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering
Task Force (IETF), its areas, and its working groups. Note that
other groups may also distribute working documents as Internet-
Drafts.

Internet-Drafts are draft documents valid for a maximum of six months
and may be updated, replaced, or obsoleted by other documents at any
time. It is inappropriate to use Internet-Drafts as reference
material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at

This Internet-Draft will expire on August 16, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

A Mobile IPv6 node requires a Home Agent address, a home address, and
a security association with its Home Agent before it can start utilizing Mobile IPv6. RFC 3775 requires that some or all of these parameters are statically configured. Ongoing Mobile IPv6 bootstrapping work aims to make this information dynamically available to the Mobile Node. An important aspect of the Mobile IPv6 bootstrapping solution is to support interworking with existing authentication, authorization and accounting infrastructure. This document describes the MIPv6 bootstrapping using the Diameter Network Access Server (NAS) <-> home Authentication, Authorization and Accounting server (HAAA) interface.
# Table of Contents

1. Introduction ........................................... 4
2. Terminology and Abbreviations ........................... 4
3. Overview ................................................ 5
4. Commands, AVPs and Advertising Application Support ....... 7
   4.1. Advertising Application Support .................. 7
   4.2. Command Codes .................................... 7
   4.3. Diameter-EAP-Request (DER) ......................... 7
   4.4. Diameter-EAP-Answer (DEA) ........................ 8
   4.5. AA-Request (AAR) ................................ 9
   4.6. AA-Answer (AAA) ................................ 10
   4.7. Attribute Value Pair Definitions .................. 11
      4.7.1. MIP6-Home-Agent-Address AVP ................. 11
      4.7.2. MIP6-Home-Agent-FQDN AVP .................... 11
      4.7.3. MIP6-Home-Link-Prefix AVP .................... 12
      4.7.4. MIP4-Home-Agent-Address AVP ................. 12
      4.7.5. MIP6-Home-Address AVP ........................ 12
   4.8. Capability Advertisement ........................... 12
5. Diameter Client and Server Behavior During MIPv6 ........ 13
   5.1. Client (NAS) Behavior ............................ 13
   5.2. Server Behavior .................................. 14
6. Example Message Flows .................................. 15
   6.1. EAP-based authentication ........................... 15
   6.2. Integrated scenario and HA allocation in MSP ....... 16
   6.3. Integrated scenario and HA allocation in ASP ....... 18
7. AVP Occurrence Tables ................................... 19
   7.1. DER and DEA Commands AVP Table ................... 19
   7.2. AAR and AAA Commands AVP Table ................... 20
8. MIPv6 Bootstrapping NAS - HAAA Interface AVPs ........... 21
9. IANA Considerations ..................................... 22
10. Security Considerations .................................. 22
11. Acknowledgements ...................................... 22
12. Revision history ....................................... 23
13. References ............................................. 24
   13.1. Normative References .............................. 24
   13.2. Informative References ............................ 24
Authors’ Addresses ........................................ 25

Intellectual Property and Copyright Statements ............... 27
1. Introduction

The Mobile IPv6 (MIPv6) specification [RFC3775] requires a Mobile Node (MN) to perform registration with a Home Agent (HA) with information about its current point of attachment (Care-of Address). The HA creates and maintains binding between the MN’s Home Address and the MN’s Care-of Address.

In order to register with a HA, the MN needs to know some information such as, the Home Link prefix, the HA address, the Home Address(es), the Home Link prefix Length and security association related information.

The aforementioned set of information may be statically provisioned in the MN. However, static provisioning of this information becomes easily provisioning and network administration burden for an operator. Moreover, static provisioning does not address load balancing, failover, opportunistic home link assignment and assignment of local home agents in close proximity to the MN. Also the ability to react on sudden environmental or topological changes is minimal. In a light of above issues static provisioning may not be desirable.

Dynamic assignment of MIPv6 home registration information is a desirable feature for ease of deployment and network maintenance. For this purpose, the AAA infrastructure, which is used for access authentication, can be leveraged to assign some or all of the necessary parameters. The Diameter server in Access Service Provider’s (ASP) or in Mobility Service Provider’s (MSP) network may return these parameters to the AAA client. Regarding the bootstrapping procedures, the AAA client might either be the NAS, in case of the integrated scenario, or the HA, in case of the split scenario [I-D.ietf-mip6-bootstrapping-split]. The terms integrated and split are described in the terminology section and were introduced in [RFC4640] and [I-D.iotf-mip6-aaa-ha-goals].

2. Terminology and Abbreviations

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119].

General mobility terminology can be found in [RFC3753]. The following additional terms, as defined in [RFC4640], are used in this document:
Access Service Authorizer (ASA):

A network operator that authenticates a MN and establishes the MN’s authorization to receive Internet service.

Access Service Provider (ASP):

A network operator that provides direct IP packet forwarding to and from the MN.

Mobility Service Authorizer (MSA):

A service provider that authorizes MIPv6 service.

Mobility Service Provider (MSP):

A service provider that provides MIPv6 service. In order to obtain such service, the MN must be authenticated and authorized to obtain the MIPv6 service.

Split scenario:

A scenario where the mobility service and the network access service are authorized by different entities.

Integrated Scenario:

A scenario where the mobility service and the network access service are authorized by the same entity.

Network Access Server (NAS):

A device that provides an access service for a user to a network.

Home AAA (HAAA):

An authentication, authorization and accounting server located in user’s home network.

3. Overview

This document addresses the authentication, authorization and accounting functionality required by for the MIPv6 bootstrapping as outlined in the MIPv6 bootstrapping problem statement document [RFC4640]. This document focuses on the Diameter based AAA functionality for the NAS - HAAA interface.
In the integrated scenario MIPv6 bootstrapping is provided as part of the network access authentication procedure. Figure 1 shows the participating entities. This document, however, only concentrates on the NAS, possible local Diameter proxies and the home Diameter server.

![Diagram of Mobile IPv6 Bootstrapping in the Integrated Scenario]

Figure 1: Mobile IPv6 Bootstrapping in the Integrated Scenario

In a typical MIPv6 access scenario the MN is attached to an ASP’s network. During the network attachment procedure, the NAS/Diameter client interacts with the MN.

During the time of authentication the Diameter server in the MSA detects that the user is also authorized for MIPv6 access. Based on the MSA’s policy, the Diameter server may return several MIPv6 bootstrapping related parameters.

Depending on the details of the bootstrapping solution interaction with the DHCPv6 server may be required, as described in [I-D.ietf-mip6-bootstrapping-integrated-dhc]. However, the Diameter based NAS - HAAA interface described in this document is not tied to DHCPv6 as the only possible MIPv6 bootstrapping method.
4. Commands, AVPs and Advertising Application Support

This section describes command codes, defines AVPs and advertised application identifiers for the Diameter MIPv6 bootstrapping in the NAS - HAAA interface.

4.1. Advertising Application Support

Diameter nodes conforming to this specification SHOULD include the value of 1 (NASREQ application) or 5 (EAP application) in the Auth-Application-Id or the Acct-Application-Id AVP in the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands [RFC3588].

4.2. Command Codes

This document re-uses the Diameter NASREQ application [RFC4072] and the EAP application commands [RFC4005]. The following commands are used to carry MIPv6 related bootstrapping AVPs:

<table>
<thead>
<tr>
<th>Command-Name</th>
<th>Abbrev.</th>
<th>Code</th>
<th>Reference</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diameter-EAP-Request</td>
<td>DER</td>
<td>268</td>
<td>RFC 4072</td>
<td>EAP</td>
</tr>
<tr>
<td>Diameter-EAP-Answer</td>
<td>DEA</td>
<td>268</td>
<td>RFC 4072</td>
<td>EAP</td>
</tr>
<tr>
<td>AA-Request</td>
<td>AAR</td>
<td>265</td>
<td>RFC 4005</td>
<td>NASREQ</td>
</tr>
<tr>
<td>AA-Answer</td>
<td>AAA</td>
<td>265</td>
<td>RFC 4005</td>
<td>NASREQ</td>
</tr>
</tbody>
</table>

Figure 2: MIPv6 Bootstrapping NAS - HAAA Interface Command Codes

When the Re-Auth-Request (RAR), Re-Auth-Answer (RAA), Session-Termination-Request (STR), Session-Termination-Answer (STA), Abort-Session-Request (ASR), Abort-Session-Answer (ASA), Accounting-Request (ACR), and Accounting-Answer (ACA) commands are used together with the MIPv6 bootstrapping NAS - HAAA interface, they follow the rules in the Diameter NASREQ [RFC4005], EAP [RFC4072] and RFC 3588 [RFC3588] applications. The accounting commands use the Application Identifier value of 3 (Diameter Base Accounting); the others use 0 (Diameter Common Messages).

4.3. Diameter-EAP-Request (DER)

The Diameter-EAP-Request (DER) command [RFC4072], indicated by the Command-Code field set to 268 and the ‘R’ bit set in the Command Flags field, may be sent by the NAS to the Diameter server providing network access authentication and authorization services. At the same time with the network access authentication and authorization
the NAS MAY indicate the access network capability of MIPv6 bootstrapping and optionally also the capability of a local HA assignment.

The message format is the same as defined in [RFC4072] with an addition of optional MIPv6 bootstrapping NAS - HAAA interface AVPs to indicate capabilities of the NAS and the ASP:

\[
\text{\texttt{<Diameter-EAP-Request> ::= < Diameter Header: 268, REQ, PXY >}}
\]
\[
\text{\texttt{< Session-Id >}}
\]
\[
\text{\texttt{\{ Auth-Application-Id \}}}
\]
\[
\text{\texttt{\{ Origin-Host \}}}
\]
\[
\text{\texttt{\{ Origin-Realm \}}}
\]
\[
\text{\texttt{\{ Destination-Realm \}}}
\]
\[
\text{\texttt{\{ Auth-Request-Type \}}}
\]
\[
\text{\texttt{\[ MIP6-Home-Agent-Address \]}}
\]
\[
\text{\texttt{\[ MIP6-Home-Agent-FQDN \]}}
\]
\[
\text{\texttt{\[ MIP6-Home-Link-Prefix \]}}
\]
\[
\text{\texttt{\[ MIP6-Home-Address \]}}
\]
\[
\text{\texttt{\[ MIP4-Home-Agent-Address \]}}
\]
\[
\text{\texttt{\{ Destination-Host \}}}
\]
\[
\text{\texttt{\ldots}}
\]
\[
\text{\texttt{\* \[ AVP \]}}
\]

\begin{figure}[h]
\centering
\texttt{Figure 3: Diameter EAP Request Command}
\end{figure}

4.4. Diameter-EAP-Answer (DEA)

The Diameter-EAP-Answer (DEA) message define in [RFC4072], indicated by the Command-Code field set to 268 and ‘R’ bit cleared in the Command Flags field is sent in response to the Diameter-EAP-Request message (DER). If the network access authentication procedure was successful then the response MAY include any set of MIP6-Home-Agent-Address AVP, MIP6-Home-Link-Prefix, MIP6-Home-Agent-FQDN, MIP6-Home-Address and MIP4-Home-Agent-address AVPs.

The message format is the same as defined in [RFC4072] with an addition of optional MIPv6 bootstrapping NAS - HAAA AVPs:
<Diameter-EAP-Answer> ::= < Diameter Header: 268, PXY >
< Session-Id >
{ Auth-Application-Id }
{ Auth-Request-Type }
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }

[ MIP6-Home-Agent-Address ]
[ MIP6-Home-Agent-FQDN ]
[ MIP6-Home-Link-Prefix ]
[ MIP6-Home-Address ]
[ MIP4-Home-Agent-Address ]

[ User-Name ]
...
* [ AVP ]

Figure 4: Diameter EAP Answer Command

4.5. AA-Request (AAR)

The AA-Request (AAR) message, indicated by the Command-Code field set to 265 and ‘R’ bit set in the Command Flags field, may be sent by the NAS to the Diameter server providing network access configuration services. At the same time with the network access configuration the NAS MAY request HA assignment, to authorize for mobility service usage and optionally to indicate the support of possible local HA assignment.

The message format is the same as defined in [RFC4005] with an addition of optional MIPv6 bootstrapping NAS - HAAA AVPs:
<AA-Request> ::= < Diameter Header: 265, REQ, PXY >
    < Session-Id >
    { Auth-Application-Id }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Auth-Request-Type }

    [ MIP6-Home-Agent-Address ]
    [ MIP6-Home-Agent-FQDN ]
    [ MIP6-Home-Link-Prefix ]
    [ MIP6-Home-Address ]
    [ MIP4-Home-Agent-Address ]

    [ Destination-Host ]
    ...
* [ AVP ]

Figure 5: AA Request Command

4.6. AA-Answer (AAA)

The AA-Answer (AAA) message, indicated by the Command-Code field set to 265 and ‘R’ bit cleared in the Command Flags field is sent in response to the AA-Request (AAR) message for confirmation of the result of MIPv6 HA bootstrapping. If the network access authentication procedure was successful then the response MAY include any set of MIP6-Home-Agent-Address AVP, MIP6-Home-Link-Prefix, MIP6-Home-Agent-FQDN, MIP6-Home-Address and MIP4-Home-Agent-address AVPs.

The message format is the same as defined in [RFC4005] with an addition of optional MIPv6 bootstrapping NAS - HAAA interface AVPs:
4.7. Attribute Value Pair Definitions

4.7.1. MIP6-Home-Agent-Address AVP

The MIP6-Home-Agent-Address AVP (AVP Code TBD) is of type OctetString and contains the MIPv6 HA address and the prefix length of the said address. The AVP is a discriminated union, representing IPv6 address in network byte order. The first two octets of this AVP represents the home link prefix length followed by 16 octets of the IPv6 address.

The Diameter server MAY decide to assign a MIPv6 HA to the MN that is in close proximity to the point of attachment (e.g. determined by the NAS-Identifier). There may be other reasons for dynamically assigning HAs to the MN, for example to share the traffic load. The AVP also contains the prefix length so that the MN can easily infer one of the possible Home Link prefixes from the HA address.

This AVP MAY also be sent by the NAS to the Diameter server in a request message as a hint to suggest a dynamic HA may be assigned to the MN. Based on local policy information the Diameter server may decide to follow the hint or to override this suggestion with its preferred HA IP address.

4.7.2. MIP6-Home-Agent-FQDN AVP

The MIP6-Home-Agent-FQDN AVP (AVP Code TBD) is of type UTF8String and contains the FQDN of a MIPv6 HA. The usage of this AVP is equivalent
4.7.3. MIP6-Home-Link-Prefix AVP

The MIP6-Home-Link-Prefix AVP (AVP Code TBD) is of type OctetString and contains the MIPv6 home link prefix. There may be reasons for the Diameter server to dynamically assigning home link prefix to the MN, for example one that is in close proximity to the point of attachment.

The MN can perform RFC 3775 [RFC3775] specific procedures to discover other information for MIPv6 registration.

4.7.4. MIP4-Home-Agent-Address AVP

The MIP4-Home-Agent-Address AVP (AVP Code TBD) is of type OctetString and contains the IPv4 HA address and the prefix length of the said address. The AVP is a discriminated union, representing IPv4 address in network byte order. The first two octets of this AVP represents the home link prefix length followed by 4 octets of the IPv4 address.

The Diameter server MAY decide to assign a MIPv4 HA to the MN in a case where dual stack Mobile IP is supported [I-D.ietf-mip6-nemo-v4traversal].

4.7.5. MIP6-Home-Address AVP

The MIP6-Home-Address AVP (AVP Code TBD) is of type OctetString and contains the MIPv6 Home Address and the prefix length of the said address. The AVP is a discriminated union, representing IPv6 address in network byte order. The first two octets of this AVP represents the Home Address prefix length followed by 16 octets of the IPv6 address.

The Diameter server MAY assign a home address to the MN. This allows the network operator to support MNs that are not configured with static addresses. The attribute also contains the prefix length so that the MN can easily infer the home link prefix from the HA address.

4.8. Capability Advertisement

The NAS/ASP may include any MIPv6 bootstrapping AVPs in the DER or AAR messages in order to advertise its MIPv6 bootstrapping capabilities to the Diameter server. This capability advertisement may also be used to propose locally allocated mobility agents.
locally allocated prefix or home address to the Diameter server. As an example the MIP6-Home-Agent-Address AVP could contain the IP address of the locally allocated HA.

If the MIP6-Home-Agent-Address AVP is only used as a MIPv6 bootstrapping capability indicator then the IP address MUST be set to unspecified address (::/128). The MIP6-Home-Agent-FQDN AVP SHOULD NOT be used for the capability advertisement if it does not name a locally allocated HA.

5. Diameter Client and Server Behavior During MIPv6 Bootstrapping

This section describes the Diameter server and client behavior in case of the MIPv6 bootstrapping in the integrated scenario. The text makes several assumptions.

- The Diameter server supports at least the Diameter BASE, EAP and NASREQ applications.
- The Diameter client (i.e., the NAS) supports at least the Diameter BASE, EAP and NASREQ applications.
- The MN uses such network access authentication method and credentials that are supported by the NAS/ASP and ASA/MSA.
- The MN has been provisioned with a MIPv6 service.

5.1. Client (NAS) Behavior

If the ASP/NAS does not support MIPv6 integrated scenario bootstrapping then the NAS either selects the basic Diameter NASREQ or EAP application depending on which authentication method gets used. Naturally after a successful or a failed authentication the NAS does not have to carry out any MIPv6 bootstrapping related procedures.

Next, we describe two different scenarios for the network access authentication when the ASP/NAS supports MIPv6 integrated scenario bootstrapping.

1) The MN uses some EAP-based method for network access authentication. In this scenario the NAS uses commands originally defined for the EAP application.

2) The MN uses a non-EAP-based network access authentication procedure. In this scenario the NAS uses the Diameter NASREQ application commands.

The NAS may include the MIPv6 NAS - HAAA AVPs in the DER or in the AAR messages. This serves two purposes. Firstly the NAS/ASP may advertise its MIPv6 bootstrapping capability to the Diameter server.
Secondly the NAS/ASP may suggest locally allocated HAs to the Diameter server. Whether the locally allocated HAs are allowed for the forthcoming MIPv6 session depends on the MN’s subscription and the ASA/MSA/(MSP) policies. If the NAS/ASP only wants to advertise its capability for local agent allocation but does not want to provide any specific agent at this point of time (e.g. that is left for later steps during the actual Mobile IP registration) the AVPs MUST contain values described in Section 4.8.

If the network access authentication failed the NAS receives appropriate error codes as defined for the Diameter EAP or NASREQ applications. The NAS does not allow the MN to access the network and does not do any MIPv6 bootstrapping related procedures.

If the network access authentication completed successfully, the NAS looks for HA defining AVPs in the reply messages (either DEA or AAA depending on the used authentication method). The NAS associates the received bootstrapping information to the MN that initiated the access authentication and stores the information internally (storing time is determined by the ASP policy). The stored bootstrapping information is then available for the NAS and the DHCP relay for later step during the MN bootstrapping process.

The actual bootstrapping from the MN point of view takes place after the network access authentication has completed. The bootstrapping may be realized e.g. using DHCP as defined in [I-D.ietf-mip6-bootstrapping-integrated-dhc] and [RFC2132].

The MN has no consistent way of indicating to the NAS that it supports MIPv6 integrated scenario way of bootstrapping during the network access authentication. Subsequently the NAS has no possibilities to find out whether the terminal attempting to authenticate is actually a MN with MIPv6 bootstrapping functionality prior the network access authentication has completed. Thus, it is possible that the NAS initiates MIPv6 integrated scenario bootstrapping configuration even if the MN is not able to make any use of it later. The Diameter server in the ASA/MSA might be able to detect this situation during the authentication phase based on the information in the subscriber database assuming the ASA is able to verify whether the MN has been provisioned with a MIPv6 service (from the MSA/MSP).

5.2. Server Behavior

If the NAS/ASP does not support MIPv6 integrated scenario bootstrapping then the NAS either selects the Diameter NASREQ or EAP application depending on which access authentication method the MN has to use to authenticate. In this case the NAS does not either
include any MIPv6 NAS - HAAA interface AVPs as a hint of the bootstrapping capability in the NAS/ASP. The Diameter server in the ASA/MSA(/MSP) detects this case (based on AVPs that serve as a capability hint) and does not have to carry out any MIPv6 bootstrapping related procedures. However, as the capability advertisement mechanism described in this document serves only as an optional hint, the Diameter server should not entirely rely on the received capability hints but also base its working logic on subscription information and general MSA(/MSP) policies.

Next we describe two different scenarios for the network access authentication when the NAS/ASP supports MIPv6 integrated scenario bootstrapping.

1) The MN uses some EAP-based method to authenticate to the network and the NAS uses Diameter EAP application commands. Depending on the ASA/MSA(/MSP) policy the Diameter server SHOULD assign a MIPv6 HA to the MN and include corresponding MIP6-Home-Agent-Address, the MIP6-Home-Agent-FQDN AVPs and the MIP6-Home-Link-Prefix in the final DEA message.

2) The MN uses some other than EAP-based method to authenticate to the network and the NAS uses Diameter NASREQ application commands. Depending on the ASA/MSA(/MSP) policy the Diameter server SHOULD assign a MIPv6 HA to the MN and include corresponding MIP6-Home-Agent-Address, the MIP6-Home-Agent-FQDN AVPs and the MIP6-Home-Link-Prefix in the final AAA message.

If the Diameter request message contained any MIPv6 NAS-HAAA interface AVPs the Diameter server should regard them as a hint of the MIPv6 bootstrapping capability in the NAS/ASP. Any of these AVPs may contain values as described in Section 4.8 which indicate the NAS/ASP would like to locally allocate a HA or a home link to the MN. The Diameter server may or may not honor the NAS/ASP hint based on the MN's subscription and ASA/MAS(/MSP) policies.

6. Example Message Flows

6.1. EAP-based authentication

This section shows basic message flows of MIPv6 integrated scenario bootstrapping and dynamic HA assignment. In the Figure 7 network access authentication is based on EAP (e.g. 802.11i/802.1X). The NAS informs the home Diameter server that HA assignment in the foreign network is possible. The Diameter server assigns the MN a HA either in the home MSP or in the ASP. The assignment procedure is out of scope of this document. The Diameter server then replies to the NAS with HA related bootstrapping information.
6.2. Integrated scenario and HA allocation in MSP

Diameter is used to authenticate and authorize the MN for the mobility service, and to send information about the allocated HA to the NAS. In this example scenario the MN uses DHCP for its IP address configuration.
1) The MN executes the normal network access authentication procedure (IEEE 802.11i/802.1X, PANA, ...) with the NAS. The NAS acts as an authenticator in "pass-through" mode. The other endpoint of the authentication dialogue is the MN's home Diameter server. This is a typical scenario for e.g. EAP-based authentication methods. The NAS includes at least one of the NAS-HAAA interface AVPs in the DER or in the AAR messages to indicate MIPv6 bootstrapping capability. For example the NAS could include MIP6-Home-Agent-Address AVP with 0::/128 as the HA address (the NAS has no particular HA to propose to the Diameter server).

2) Depending on the Diameter server configuration and the subscription profile, the MIP6-Home-Agent-Address AVP or the MIP6-Home-Agent-FQDN AVP may be appended to the DEA or to the AAA message, assuming the home Diameter server knows or has allocated a HA to the MN. In case the MIP6-Home-Agent-FQDN AVP was returned the MN ultimately needs to perform a DNS query in order to discover the HA address. For example the home Diameter server
could return the following AVPs:

- MIP6-Home-Agent-Address = 2001:2001:6000:302::1/64

3) the MN sends a DHCPv6 Information Request message to the all_DHCP_Relay_Agents_and_Servers address. In the OPTION_ORO, Option Code for the Home Network Identifier Option shall be included in that message [I-D.ietf-mip6-bootstrapping-integrated-dhc]. The Home Network Identifier Option should have id-type of 1, the message is a request to discover home network information that pertains to the given realm, i.e., the user’s home domain (identified by the NAI of the MN). The OPTION_CLIENTID is set by the MN to identify itself to the DHCP server.

Steps 4 to 6 are not relevant in NAS-HAAA Diameter interface point of view and are not described in this document. Refer [I-D.ietf-mip6-bootstrapping-integrated-dhc] for detailed information about the rest of the integrated scenario bootstrapping procedure.

6.3. Integrated scenario and HA allocation in ASP

This scenario is similar to the one described in Section 6.2 and illustrated in Figure 8. There are slight differences in steps 2) and 3).

2) The NAS/ASP has allocated a local HA (e.g. with IP address 2001:788:1:c020::1/64) and a local prefix, and proposes those to MN’s home Diameter server. For example the NAS includes following AVPs in the DER or in the AAR messages:

- MIP6-Home-Agent-Address = 2001:788:1:c020::1/64
- MIP6-Home-Link-Prefix = 2001:788:1:c020::/64

Depending on the Diameter server configuration and the subscription profile, the Diameter server either accepts or rejects the HA IP address (or FQDN) proposed by the NAS/ASP. If the Diameter server accepts the proposed HA the AVP containing the HA information is returned as is back to the NAS. In this example the returned IP6-Home-Agent-Address AVP would contain the same 2001:788:1:c020::1/64 IP address value. On the other hand if the Diameter server does not accept the proposed HA, the Diameter server overwrites the MIP6-Home-Agent-Address AVP value with an IP address of the preferred HA (e.g. 2001:2001:6000::1/64) and returns the new IP address back to the NAS/ASP (the MIP6-Home-Agent-FQDN AVP is handled in the same way when present). This is
also an indication to the NAS/ASP that locally allocated HAs are not to be used. In a case when the home Diameter server accepted the NAS/ASP proposed local HA the home Diameter server would return e.g. the following AVPs:

- MIP6-Home-Agent-Address = 2001:788:1:c020::1/64
- MIP6-Home-Link-Prefix = 2001:788:1:c020::/64

3) The type-id field in the Home Network Identifier Option is set to zero, indicating that a HA is requested in the ASP instead of in the MSP. Depending on the result of the phase 2) the DHCP relay agent places in the OPTION_MIP6-RELAY-Option either the locally allocated HA information or the HA information that was returned (overwritten) by home Diameter server.

7. AVP Occurrence Tables

7.1. DER and DEA Commands AVP Table

The following table lists the additional MIPv6 bootstrapping NAS – HAAA interface AVPs that optionally may be present in the DER and DEA Commands, as defined in this document and in [RFC4072].
### AAR and AAA Commands AVP Table

The following table lists the additional MIPv6 bootstrapping NAS - HAAA interface AVPs that may optionally be present in the AAR and AAA Commands, as defined in this document and in [RFC4005].
8. MIPv6 Bootstrapping NAS - HAAA Interface AVPs

This section defines the AVPs that are specific to Diameter MIPv6 bootstrapping NAS - HAAA interface and MAY be included in the Diameter EAP [RFC4072] and the NASREQ [RFC4005] applications messages listed in Section 4 of this document. The Diameter AVP rules are defined in the Diameter Base [RFC3588], Section 4. These AVP rules are observed in AVPs defined in this section.

The following table describes the Diameter AVPs, their AVP Code values, types, possible flag values, and whether the AVP MAY be encrypted. The Diameter base [RFC3588] specifies the AVP Flag rules for AVPs in section 4.5.
9. IANA Considerations

This specification defines the following new AVPs:

- MIP6-Home-Agent-Address is set to TBD
- MIP6-Home-Agent-FQDN is set to TBD
- MIP4-Home-Agent-Address is set to TBD
- MIP6-Home-Link-Prefix is set to TBD
- MIP6-Home-Address is set to TBD

10. Security Considerations

The security considerations for the Diameter interaction required to accomplish the integrated scenario are described in [I-D.ietf-mip6-bootstrapping-integrated-dhc]. Additionally, the security considerations of the Diameter base protocol [RFC3588], Diameter NASREQ application [RFC4005] / Diameter EAP [RFC4072] application (with respect to network access authentication and the transport of keying material) are applicable to this document.

11. Acknowledgements

This document is heavily based on the ongoing work for RADIUS MIPv6 interaction. Hence, credits go to respective authors for their work with draft-ietf-mip6-radius-00.txt. Furthermore, the author would like to thank the authors of draft-le-aaa-diameter-mobileipv6-04.txt.
(Franck Le, Basavaraj Patil, Charles E. Perkins, Stefano Faccin) for their work in context of MIPv6 Diameter interworking. Their work influenced this document. Julien Bournelle would like to thank GET/INT since he began to work on this document while he was in their employ.

12. Revision history

The following changes were made to the -01 version of the draft:

- The document title was changed to "The NAS - HAAA Interface for MIPv6 Bootstrapping".
- Added HAAA and NAS to terminology section".
- Changed NAS application to NASREQ application.".
- Changed "Integrated Scenario" to NAS-HAAA interface".
- The separate Diameter Application-ID for MIPv6 bootstrapping (MIP6BSTI) got removed and all bootstrapping is based on Diameter EAP application and Diameter NAS application.
- MIPv6-Bootstrapping-Feature AVP was removed and General text regarding to the capability advertisement based on optional AVPs was added.
- The capability exchange was modified so that the NAS may suggest a specific HA to the AAAH. Original MIPv6-Bootstrapping-Feature AVP was replaces with a possibility to include any bootstrapping AVP to the Diameter AAR or DER messages as a capability and local allocation hint.

The following changes were made to the -02 version of the draft:

- Section 7 NAS - HAAA Interface AVPs flags were corrected. 'M' flag was listed as MUST even if it should have been MUST NOT.
- General shortening of the text.
- Addition of the MIP6-Home-Address AVP.
- Checked against draft-ietf-mip6-radius-01.
- Addition of noted & constrains to AVP tables.
- Miscellaneous corrections like Mobile IPv6 -> MIPv6.
- Added signaling examples for HA assignment from MSP, and local HA assignment.

The following changes were made to the -03 version of the draft:

- Section 7.1 corrected case [d] mixed AVPs.
- Section 7.2 corrected case [d] mixed AVPs.

13. References
13.1. Normative References

[I-D.ietf-mip6-aaa-ha-goals]
Giaretta, G., "AAA Goals for Mobile IPv6",
draft-ietf-mip6-aaa-ha-goals-03 (work in progress),
September 2006.

[I-D.ietf-mip6-bootstrapping-integrated-dhc]
Chowdhury, K. and A. Yegin, "MIP6-bootstrapping for the
Integrated Scenario",
draft-ietf-mip6-bootstrapping-integrated-dhc-02 (work in
progress), February 2007.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate


bootstrapping Mobile IPv6 (MIPv6)", RFC 4640,
September 2006.

13.2. Informative References

[I-D.ietf-mip6-bootstrapping-split]
Giaretta, G., "Mobile IPv6 bootstrapping in split
scenario", draft-ietf-mip6-bootstrapping-split-04 (work in
progress), December 2006.

[I-D.ietf-mip6-nemo-v4traversal]
Soliman, H., "Mobile IPv6 support for dual stack Hosts and
Routers (DSMIPv6)", draft-ietf-mip6-nemo-v4traversal-03
(work in progress), October 2006.


[RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology",

[RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton,
"Diameter Network Access Server Application", RFC 4005,
August 2005.
Authentication Protocol (EAP) Application", RFC 4072,
August 2005.

Authors' Addresses

Jouni Korhonen
TeliaSonera
Teollisuuskatu 13
Sonera  FIN-00051
Finland

Email: jouni.korhonen@teliasonera.com

Julien Bournelle
France Telecom R&D
38-40 rue du general Leclerc
Issy-Les-Moulineaux  92794
France

Email: julien.bournelle@orange-ftgroup.com

Hannes Tschofenig
Siemens Networks GmbH & Co KG
Otto-Hahn-Ring 6
Munich, Bavaria  81739
Germany

Email: Hannes.Tschofenig@siemens.com
URI: http://www.tschofenig.com

Charles E. Perkins
Nokia Research Center
313 Fairchild Drive
Mountain View  CA 94043
US

Phone: +1 650 625-2986
Email: charliep@iprg.nokia.com