Diameter Maintenance and Extensions (DIME)
Internet-Draft
Intended status: Standards Track
Expires: March 9, 2009

J. Korhonen
TeliaSonera
J. Bournelle
Orange Labs
H. Tschofenig
Nokia Siemens Networks
C. Perkins
WiChorus
K. Chowdhury
Starent Networks
September 5, 2008

Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction
draft-ietf-dime-mip6-integrated-10.txt

Status of this Memo

Copyright Notice

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. 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 MIPv6 bootstrapping using the Diameter Network Access Server (NAS) to home Authentication, Authorization and Accounting server (HAAA) interface.

Table of Contents

1. Introduction

The Mobile IPv6 (MIPv6) specification [1] 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 the 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 information may be statically configured. However, static provisioning becomes an administrative burden for an operator. Moreover, it does not address load balancing, failover, opportunistic home link assignment or assignment of local HAs in close proximity to the MN. Also the ability to react to sudden environmental or topological changes is minimal. Static provisioning may not be desirable, in light of these limitations.

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 the Access Service Provider's (ASP) or in the 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 [7]. The terms integrated and split are described in the terminology section and were introduced in [8] and [9].

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 [2].

General mobility terminology can be found in [10]. The following additional terms below are either borrowed from [8][7] or introduced 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 i.e., in the home realm.

Local AAA (LAAA):

An authentication, authorization and accounting proxy located in the local (ASP) network.

Visited AAA (VAAA):

An authentication, authorization and accounting proxy located in a visited network i.e., in the visited realm. In a roaming case, the local Diameter proxy has the VAAA role (see Figure 1).

3. Overview

This document addresses the authentication, authorization and accounting functionality required for the MIPv6 bootstrapping solutions outlined in [8] and focuses on the Diameter based AAA functionality for the NAS to HAAA communication.

In the integrated scenario MIPv6 bootstrapping is provided as part of the network access authentication procedure. Figure 1 shows the participating entities.

```
                    +---------------------------+  +-----------------+
                    |Access Service Provider    |  |ASA/MSA/(MSP)    |
                    |(Mobility Service Provider)|  |                 |
```

```
                      |                           |  |                 |
                      | +--------+                |  |    +--------+   |
                      | |Local   |      Diameter  |  |    |Home    |   |
                      | |Diameter|<---------------------->|Diameter|   |
                      | |Proxy   |         (*)    |  |    |Server  |   |
                      | +--------+                |  |    +--------+   |
                      |     ^ ^                   |  |        ^        |
                      |     | |                   |  |        |(+)     |
                      |     | |                   |  |        |        |
                      |   Diameter                |  |        v        |
                      |     | |(+)      +-------+ |  |    +-------+    |
                      |     | |         |Home   | |  |    |Home   |    |
                      |     | +-------->|Agent  | |  |    |Agent  |    |
                      |  (*)|           |in ASP | |  |    |in MSP |    |
                      |     v           +-------+ |  |    +-------+    |
   +-------+ IEEE     | +-----------+   +-------+ |  +-----------------+
   |Mobile | 802.1X   | |NAS/Relay  |   |DHCPv6 | |
   |Node   |------------|Diameter   |---|Server | |
   |       | PANA,... | |Client     |(+)|       | |
   +-------+ DHCP     | +-----------+   +-------+ |
             (+)      +---------------------------+
```

Legend:
  (*): Functionality in scope of this specification
  (+): Extensions described in other documents.

Figure 1: Mobile IPv6 Bootstrapping in the Integrated Scenario

In a typical MIPv6 access scenario, a MN is attached to an ASP's network. During the network attachment procedure, the MN interacts with the NAS/Diameter client. Subsequently, the NAS/Diameter client interacts with the Diameter server over the NAS to HAAA interface.

When the Diameter server performs the authentication and authorization for the network access it also determines whether the user is authorized to the MIPv6 service. Based on the MIPv6 service authorization and user's policy profile, the Diameter server may return several MIPv6 bootstrapping related parameters to the NAS. The NAS to HAAA interface described in this document is not tied to DHCPv6 as the only mechanism to convey MIPv6 related configuration parameters from the NAS/Diameter client to the mobile node.

4. Commands, Attribute Value Pairs and Advertising Application Support

4.1. Advertising Application Support

This document does not define a new application. On the other hand it defines a number of AVPs used in the interface between NAS to HAAA for the integrated scenario of MIPv6 bootstrapping. These AVPs can be used with any present and future Diameter applications, where permitted by the command ABNF. The examples using existing applications and their commands in the following sections are for informational purposes only. The examples in this document reuse the EAP [3] application and its respective commands.

4.2. Attribute Value Pair Definitions

4.2.1. MIP6-Agent-Info

The MIP6-Agent-Info AVP (AVP code TBD) is type of Grouped and contains necessary information to assign a HA to the MN. When the MIP6-Agent-Info AVP is present in a message, it MUST contain either the MIP-Home-Agent-Address AVP or the MIP-Home-Agent-Host AVP, or both AVPs. The grouped AVP has the following grammar:

```
<MIP6-Agent-Info> ::= < AVP Header: TBD >
                    *2[ MIP-Home-Agent-Address ]
                      [ MIP-Home-Agent-Host ]
                    * [ AVP ]
```

If both MIP-Home-Agent-Address and MIP-Home-Agent-Host APVs are present in the MIP6-Agent-Info, the MIP-Home-Agent-Address SHOULD have a precedence over the MIP-Home-Agent-Host. The reason for this

recommendation is that the MIP-Home-Agent-Address points to a specific home agent, where as the MIP-Home-Agent-Host may point to a group of HAs located at within the same realm. A Diameter client or an agent may use the MIP-Home-Agent-Host AVP, for instance, to find out the realm where the HA is located.

This AVP MAY also be attached by the NAS or by intermediating Diameter proxies in a request message when sent to the Diameter

server as a hint of a locally assigned HA. This AVP MAY also be attached by the intermediating Diameter proxies in a reply message from the Diameter server, if locally assigned HAs are authorized by the Diameter server.

4.2.2. MIP-Home-Agent-Address AVP

The MIP-Home-Agent-Address AVP (AVP Code 334 [4]) is of type Address and contains IPv6 or IPv6 address of the HA. The Diameter server MAY decide to assign a HA to the MN that is in close proximity to the point of attachment (e.g., determined by the NAS-Identifier AVP). There may be other reasons for dynamically assigning HAs to the MN, for example to share the traffic load.

4.2.3. MIP-Home-Agent-Host AVP

The MIP-Home-Agent-Host AVP (AVP Code 348 [4]) is of type Grouped and contains the identity of the assigned HA. Both the Destination-Realm and the Destination-Host AVPs of the HA are included in the grouped AVP. The usage of the MIP-Home-Agent-Host AVP is equivalent to the MIP-Home-Agent-Address AVP but offers an additional level of indirection by using the DNS infrastructure.

Depending on the actual deployment and DNS configuration the Destination-Host AVP MAY represent one or more home agents. It is RECOMMENDED that the Destination-Host AVP identifies exactly one HA.

It is RECOMMENDED that the MIP-Home-Agent-Host AVP is always included in the MIP6-Agent-Info AVP. In this way the HA address can be associated with the corresponding realm the HA belongs to.

4.2.4. MIP6-Home-Link-Prefix AVP

The MIP6-Home-Link-Prefix AVP (AVP Code TBD) is of type OctetString and contains the Mobile IPv6 home network prefix information in network byte order. The home network prefix MUST be encoded as the 8-bit prefix length information followed by the 128-bit field for the available home network prefix.

4.2.5. MIP6-Feature-Vector AVP

The MIP6-Feature-Vector AVP (AVP Code TBD) is of type Unsigned64 and contains a 64 bit flags field of supported capabilities of the NAS/ASP. Sending and receiving the MIP6-Feature-Vector AVP with value 0 MUST be supported, although that does not provide much guidance about specific needs of bootstrapping.

The NAS MAY include this AVP to indicate capabilities of the NAS/ASP to the Diameter server. For example, the NAS may indicate that a local HA can be provided. Similarly, the Diameter server MAY include this AVP to inform the NAS/ASP about which of the NAS/ASP indicated capabilities are supported or authorized by the ASA/MSA(/MSP).

The following capabilities are defined in this document:

MIP6_INTEGRATED (0x0000000000000001)

When this flag is set by the NAS then it means that the Mobile IPv6 integrated scenario bootstrapping functionality is supported by the NAS. When this flag is set by the Diameter server then the Mobile IPv6 integrated scenario bootstrapping is supported by the Diameter server.

LOCAL_HOME_AGENT_ASSIGNMENT (0x0000000000000002)

When this flag is set in the request message, a local home agent outside the home realm is requested and may be assigned to the MN. When this flag is set by the Diameter server in the answer message, then the assignment of local HAs is authorized by the Diameter server.

A local HA may be assigned by the NAS, LAAA or VAAA depending on the network architecture and the deployment.

The following examples show how the LOCAL_HOME_AGENT_ASSIGNMENT (referred as LOCAL-bit in the examples) capability and the MIP-Agent-Info AVP (referred as HA-Info in the examples) are used to assign HAs, either a local HA (L-HA) or a home network HA (H-HA). Below is an example of a request message combinations as seen by the HAAA:

LOCAL-bit	HA-Info	Meaning
0	-	ASP or [LV]AAA is not able to assign a L-HA
0	L-HA	Same as above. HA-Info must be ignored
1	-	ASP or [LV]AAA can/wishes to assign a L-HA
1	L-HA	Same as above but ASP or [LV]AAA also

provides a hint of the assigned L-HA

Then the same as above for an answer message combinations as seen by the NAS:

LOCAL-bit	HA-Info	Meaning
0	-	No HA allowed -> no mobility
0	H-HA	L-HA is not allowed. HAAA assigns a H-HA
1	-	L-HA is allowed. No HAAA or [LV]AAA assigned HA
1	L-HA	L-HA is allowed. [LV]AAA also assigns a L-HA
1	H-HA	L-HA is allowed. HAAA also assigns a HA
1	H-HA + L-HA	L-HA is allowed. HAAA assigns a H-HA and [LV]AAA also assigns also a L-HA

A NAS should expect to possible receive multiple of the MIP6-Agent-Info AVPs.

5. Examples

5.1. Home Agent Assignment by the NAS

In this scenario we consider the case where the NAS wishes to allocate a local HA to the MN. The NAS will also inform the Diameter server about the HA address it has assigned to the visiting MN (e.g., 2001:db8:1:c020::1). The Diameter-EAP-Request message therefore has the MIP6-Feature-Vector with the LOCAL_HOME_AGENT_ASSIGNMENT and the MIP6_INTEGRATED set. The MIP6-Agent-Info AVP contains the MIP-Home-Agent-Address AVP with the address of the proposed HA.

```
                                                                Diameter
   NAS/VAAA                                                       Server
    |                                                                 |
    |  Diameter-EAP-Request                                           |
    |  MIP6-Feature-Vector=(LOCAL_HOME_AGENT_ASSIGNMENT               |
    |                       | MIP6_INTEGRATED)                        |
    |  MIP6-Agent-Info{                                               |
    |       MIP-Home-Agent-Address(2001:db8:1:c020::1)}               |
    |  }                                                              |
    |  Auth-Request-Type=AUTHORIZE_AUTHENTICATE                       |
    |  EAP-Payload(EAP Start)                                         |
    |---------------------------------------------------------------->|
    |                                                                 |
    |                                                                 |
    :              ...more EAP Request/Response pairs...              :
    |                                                                 |
    |                                                                 |
    |                                            Diameter-EAP-Answer  |
    |               MIP6-Feature-Vector=(LOCAL_HOME_AGENT_ASSIGNMENT  |
    |                                    | MIP6_INTEGRATED)           |
    |                                   Result-Code=DIAMETER_SUCCESS  |
    |                                       EAP-Payload(EAP Success)  |
    |                                         EAP-Master-Session-Key  |
    |                                           (authorization AVPs)  |
    |                                                           ...   |
    |<----------------------------------------------------------------|
    |                                                                 |
```

Figure 2: Home Agent Assignment by NAS

Depending on the Diameter server configuration and user's subscription profile, the Diameter server either accepts or rejects the local HA allocated by the NAS. In our example, the Diameter server accepts the proposal and the the MIP6-Feature-Vector AVP with LOCAL_HOME_AGENT_ASSIGNMENT flag (together with the MIP6_INTEGRATED flag) is set and returned to the NAS.

5.2. Home Agent Assignment by the Diameter Server

In this scenario we consider the case where the NAS supports the Diameter MIPv6 integrated scenario as defined in this document but does not offer local HA assignment. Hence, the MIP6-Feature-Vector AVP only has the MIP6_INTEGRATED flag set. The Diameter server allocates a HA to the mobile node and conveys the address in the MIP-Home-Agent-Address AVP that is encapsulated in the MIP6-Agent-Info AVP. Additionally, the MIP6-Feature-Vector AVP has the MIP6_INTEGRATED flag set.


```
                                                            Diameter
 NAS                                                          Server
  |                                                                |
  |  Diameter-EAP-Request                                          |
  |  MIP6-Feature-Vector=(MIP6_INTEGRATED)                         |
  |  Auth-Request-Type=AUTHORIZE_AUTHENTICATE                      |
  |  EAP-Payload(EAP Start)                                        |
  |--------------------------------------------------------------->|
  |                                                                |
  |                                                                |
  :                 ...more EAP Request/Response pairs...          :
  |                                                                |
  |                                                                |
  |                                            Diameter-EAP-Answer |
  |                                               MIP6-Agent-Info{ |
  |          MIP-Home-Agent-Address(2001:db8:6000:302::1/64)       |
  |                                                              } |
  |                            MIP6-Feature-Vector=(MIP6_INTEGRATED) |
  |                                   Result-Code=DIAMETER_SUCCESS |
  |                                       EAP-Payload(EAP Success) |
  |                                         EAP-Master-Session-Key |
  |                                           (authorization AVPs) |
  |                                                           ...  |
  |<---------------------------------------------------------------|
  |                                                                |
```

Figure 3: Home Agent Assignment by Diameter Server

5.3. Home Agent Assignment by NAS or Diameter Server

This section shows another message flow for the MIPv6 integrated scenario bootstrapping where the NAS informs the Diameter server that

it is able to locally assign a HA to the MN. The Diameter server is able to provide a HA to the MN but also authorizes the assignment of local HA. The Diameter server then replies to the NAS with HA related bootstrapping information.

Whether the NAS/ASP then offers a locally assigned HA or the Diameter server assigned HA to the MN is, in this example, based on the local ASP policy.


```
                                                                Diameter
   NAS/VAAA                                                       Server
    |                                                                 |
    |  Diameter-EAP-Request                                           |
    |  MIP6-Feature-Vector=(LOCAL_HOME_AGENT_ASSIGNMENT               |
    |                       | MIP6_INTEGRATED)                         |
    |  MIP6-Agent-Info{                                               |
    |       MIP-Home-Agent-Address(2001:db8:1:c020::1)}               |
    |  }                                                              |
    |  Auth-Request-Type=AUTHORIZE_AUTHENTICATE                       |
    |  EAP-Payload(EAP Start)                                         |
    |---------------------------------------------------------------->|
    |                                                                 |
    |                                                                 |
    :              ...more EAP Request/Response pairs...              :
    |                                                                 |
    |                                                                 |
    |                                            Diameter-EAP-Answer  |
    |                                               MIP6-Agent-Info{  |
    |               MIP-Home-Agent-Address(2001:db8:6000:302::1/64)}  |
    |               MIP6-Feature-Vector=(LOCAL_HOME_AGENT_ASSIGNMENT  |
    |                                    | MIP6_INTEGRATED)           |
    |                                   Result-Code=DIAMETER_SUCCESS  |
    |                                       EAP-Payload(EAP Success)  |
    |                                         EAP-Master-Session-Key  |
```

```
   |                                           (authorization AVPs)  |
   |                                                          ...    |
   |<----------------------------------------------------------------|
   |                                                                 |
```

Figure 4: Home Agent Assignment by NAS or Diameter Server

If the Diameter server does not allow the MN to use a locally assigned HA, the Diameter returns the MIP6-Feature-Vector AVP with the LOCAL_HOME_AGENT_ASSIGNMENT bit unset and HA address it allocated to the MN.

6. Attribute Value Pair Occurrence Tables

Figure 5 lists the MIPv6 bootstrapping NAS to HAAA interface AVPs, along with a specification determining how many of each new AVP may be included in a Diameter command. They may be present in any Diameter application request and answer commands, where permitted by the command ABNF.

Attribute Name	Command Req	Command Ans
MIP6-Agent-Info	0+	0+
MIP6-Feature-Vector	0-1	0-1
MIP6-Home-Link-Prefix	0+	0+

Figure 5: Generic Request and Answer Commands AVP Table

7. IANA Considerations

7.1. Registration of new AVPs

This specification defines the following new AVPs:

MIP6-Agent-Info	is set to TBD
MIP6-Feature-Vector	is set to TBD
MIP6-Home-Link-Prefix	is set to TBD

7.2. New Registry: Mobility Capability

IANA is requested to create a new registry for the Mobility Capability as described in Section 4.2.5.

Token	Value	Description
MIP6_INTEGRATED	0x0000000000000001	[RFC TBD]
LOCAL_HOME_AGENT_ASSIGNMENT	0x0000000000000002	[RFC TBD]
Available for Assignment via IANA	2^x	

Allocation rule: Only numeric values that are 2^x (power of two, where x >= 2) are allowed based on the allocation policy described below.

Following the example policies described in [11] new values for the MIP6-Feature-Vector AVP will be assigned based on the "Specification Required" policy. No mechanism to mark entries as "deprecated" is envisioned.

8. Security Considerations

The security considerations for the Diameter interaction required to accomplish the integrated scenario are described in [12].

Additionally, the security considerations of the Diameter base protocol [5], Diameter NASREQ application [6] / Diameter EAP [3] application (with respect to network access authentication and the transport of keying material) are applicable to this document. Developers should insure that special attention is paid to configuring the security associations protecting the messages that enables the global positioning and allocation of home agents, for instance, as outlined in section 5.

9. 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. Furthermore, the author would like to thank the authors of draft-le-aaa-diameter-mobileipv6 (Franck Le, Basavaraj Patil, Charles E. Perkins, Stefano Faccin) for their work in context of MIPv6 Diameter interworking. Their work influenced this document. Jouni Korhonen would like to thank Academy of Finland and TEKES MERCoNe Project for providing funding to work on this document. Julien Bournelle would like to thank GET/INT since he began to work on this document while he was in their employ. Authors would also like to acknowledge Raymond Hsu for his valuable feedback on local HA assignment and Wolfgang Fritsche for his thorough review. Finally, we would like to Domagoj Premec for his review comments.

We would like to thank Alper Yegin, Robert Marks, David Frascone for their comments at the second WGLC.

10. References

10.1. Normative References

[1] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[3] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[4] Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application", RFC 4004, August 2005.

[5] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[6] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter

Network Access Server Application", RFC 4005, August 2005.

10.2. Informative References

[7] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[8] Patel, A. and G. Giaretta, "Problem Statement for bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September 2006.

[9] Giaretta, G., Guardini, I., Demaria, E., Bournelle, J., and R. Lopez, "AAA Goals for Mobile IPv6", draft-ietf-mext-aaa-ha-goals-01 (work in progress), May 2008.

[10] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[11] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[12] Chowdhury, K. and A. Yegin, "MIP6-bootstrapping for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-06 (work in progress), April 2008.

Authors' Addresses

Jouni Korhonen
TeliaSonera
Teollisuuskatu 13
Sonera FIN-00051
Finland

Email: jouni.korhonen@teliasonera.com

Julien Bournelle
Orange Labs
38-40 rue du general Leclerc
Issy-Les-Moulineaux 92794
France

Email: julien.bournelle@orange-ftgroup.com

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@nsn.com
URI: http://www.tschofenig.priv.at

Charles E. Perkins
WiChorus

Phone: +1-650-496-4402
Email: charliep@wichorus.com

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury MA 01876
US

Phone: +1 214 550 1416
Email: kchowdhury@starentnetworks.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).