Diameter Maintenance and
Extensions (DIME)
Internet-Draft
Intended status: Standards Track
Expires: March 19, 2009

J. Korhonen
TeliaSonera
J. Bournelle
Orange Labs
A. Muhanna
Nortel
K. Chowdhury
Starent Networks
U. Meyer
RWTH Aachen
September 15, 2008

Diameter Proxy Mobile IPv6: Support For Mobile Access Gateway and Local Mobility Anchor to Diameter Server Interaction

draft-korhonen-dime-pmip6-04.txt

Status of this Memo

Copyright Notice

Abstract

This specification defines the Diameter support for the Proxy Mobile IPv6 and the corresponding mobility service session setup. The policy information needed by the Proxy Mobile IPv6 is defined in mobile node's policy profile, which could be downloaded from the Diameter server to the Mobile Access Gateway once the mobile node roams into a Proxy Mobile IPv6 Domain and performs access authentication.

Table of Contents

1. Introduction 4
2. Terminology and Abbreviations 4
3. Solution Overview 5
4. Attribute Value Pair Definitions 7
4.1. MIP6-Agent-Info AVP 7
4.2. PMIP6-IPv4-Home-Address AVP 7
4.3. PMIP6-DHCP-Address AVP 8
4.4. PMIP6-Home-Prefix AVP 8
4.5. MIP6-Feature-Vector AVP 8
4.6. Mobile-Node-Identifier AVP 10
4.7. Calling-Station-Id AVP 10
4.8. Service-Selection AVP 10
4.9. Session-Timeout AVP 10
5. MAG to HAAA Interface Application Support 10
5.1. Application Support and Command Codes 11
5.2. Accounting at MAG 11
6. LMA to HAAA Interface Application Support 11
6.1. Application Support and Command Codes 11
6.2. Authorization of the Proxy Binding Update 12
6.2.1. LHA-Request 13
6.2.2. LHA-Answer 13
6.3. Accounting at LMA 14
7. Proxy Mobile IPv6 Session Management 14
7.1. Session-Termination-Request 15
7.2. Session-Termination-Answer 15
7.3. Abort-Session-Request 15
7.4. Abort-Session-Answer 15
8. Attribute Value Pair Occurrence Tables 15
8.1. MAG to HAAA Interface 15
8.2. LMA to HAAA Interface 17
9. IANA Considerations 17
9.1. Attribute Value Pair Codes 17
9.2. Namespaces 17
9.3. Application Identifiers 18
9.4. Command Codes 18
9.5. Result-Code AVP Values 18
10. Security Considerations 18
11. Acknowledgements 19
12. References 19
12.1. Normative References 19
12.2. Informative References 19
Authors' Addresses 20
Intellectual Property and Copyright Statements 22

1. Introduction

In the Proxy Mobile IPv6 (PMIPv6) protocol [1] and its IPv4 support [2] a Mobile Access Gateway (MAG) performs a proxy registration with a Local Mobility Anchor (LMA) on behalf of the mobile node (MN). In order to perform the proxy registration the PMIPv6 MAG needs the address of the LMA, possibly MN's home network prefix (MN-HNP), possibly MN's IPv4 home address (IPv4-HoA), DHCP server address and other PMIPv6 specific information such as allowed address configuration modes and possible roaming related policies. All this information is defined in MN's policy profile that gets downloaded from the Diameter server to the MAG once the MN roams into a Proxy Mobile IPv6 Domain (PMIPv6-Domain) and performs the access authentication.

Dynamic assignment and downloading of PMIPv6 policy profile information is a desirable feature to ease the deployment and network maintenance of larger PMIPv6 deployments. 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 Mobility Service authorizer's (MSA) or in the Mobility Service Provider's (MSP) network may return these parameters to the Network Access Server (NAS).

Once the MN authenticates to the network the MAG sends a Proxy Binding Update (PBU) towards the LMA on behalf of the MN. Upon arrival of the PBU the LMA needs to interact with the Diameter server and fetch the MN's policy related information that was already partially downloaded to the MAG.

This specification defines the Diameter support for the PMIPv6 and the corresponding mobility service session setup. The generic requirements for the mobility service session setup and the related AAA interactions are defined in [9]. In the context of this specification the location of the subscriber policy profile equals to the home Diameter server, which is also referred as the home AAA server (HAAA). The NAS functionality of the MAG may be co-located or an integral part of the MAG. The access authentication procedure into a PMIPv6-Domain resembles the Mobile IPv6 integrated scenario bootstrapping [3]. The assumption is that the Access Service Authenticator (ASA) is the same entity as the MSA/MSP. This specification leverages the work already done for the Mobile IPv6 integrated scenario bootstrapping [3].

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 [4].

General mobility terminology can be found in [10]. The following additional or clarified terms are used in this document:

Network Access Server (NAS):

A device that provides an access service for a user to a network. In the context of this document the NAS may be integrated into or co-located to a MAG. The NAS contains a Diameter client function.

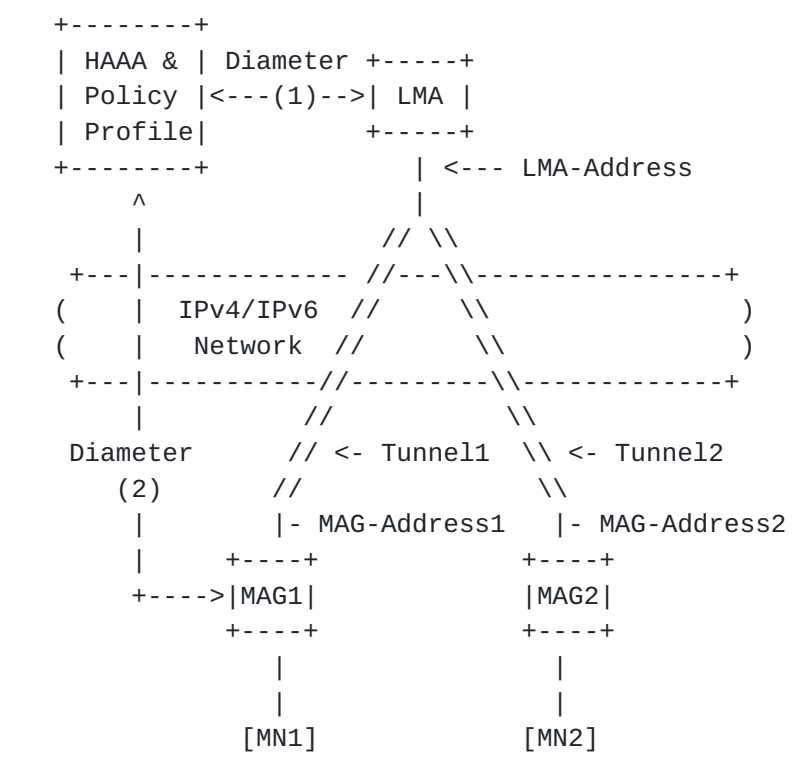
Home AAA (HAAA):

An authentication, authorization and accounting server located in user's home network. A HAAA is essentially a Diameter server.

3. Solution Overview

This document addresses the authentication, authorization, accounting and session management functionality needed by the PMIPv6 protocol. This document defines Diameter based interfaces between the PMIPv6 two entities, MAG and HAAA, to the HAAA. The intention of this document is only to extend existing Diameter Mobile IPv6 specifications such as [3] and define the needed additional AVPs and functionality to fully support PMIPv6 deployment.

The policy profile download from the HAAA to the MAG is part of the network access authentication procedure when a MN roams into or within a PMIPv6 Domain. Figure 1 shows the participating network entities. This document, however, only concentrates on the MAG, LMA, possible local Diameter proxies and the home Diameter server. When aligned with [3] the MAG acts as the NAS located in ASP, the HAAA acts as the Diameter server located in ASA/MSA/MSP and the LMA acts as the HA in ASP/MSP.



Legend:

(1): LMA <-> HAAA interaction is described in Section 6

(2): MAG <-> HAAA interaction is described in Section 5

Figure 1: Diameter Proxy Mobile IPv6 Support with MAG to HAAA and LMA to HAAA Interfaces

In a PMIPv6 access scenario a MN attaches to a PMIPv6-Domain and starts a network access authentication procedure. The choice of the authentication mechanism is specific to the access network deployment, but could be based on the Extensible Authentication Protocol (EAP) [11]. During the network access authentication procedure, the MAG acting as a NAS queries the HAAA through the AAA infrastructure using the Diameter protocol. If the HAAA detects that the subscriber is also authorized for the PMIPv6 service, the subscriber policy is returned along with the successful network access authentication answer to the MAG.

After the MN access is successfully authenticated, the MAG sends a PBU to the LMA. Upon receiving the PBU the LMA interacts with the HAAA and fetches the relevant subscriber policy, authorization and security information related to the PMIPv6 session. This

specification assumes that the HAAA is the central node for managing everything related to PMIPv6 subscription and session, possibly even including the allocation of prefixes.

Prior to sending the PBU there might be a need to dynamically setup the MAG to LMA Security Association (SA), for example using IKEv2/ IPSec [12]. The dynamic SA setup procedure may be triggered by the MN attaching to the MAG that does not have an existing SA with the correspondent LMA. The details of the dynamic SA setup procedure is out of scope of this specification. However, the SA is between the MAG and the corresponding LMA, thus it can be created using any security mechanism that is applicable for PMIPv6 security such as IKEv2 IPSec with an EAP-based authentication. It should be noted that the identity used by the MAG during the SA creation is the MAG's own identity and the credentials are for authenticating the MAG toward the LMA and possibly for authorizing the MAG to offer Proxy Mobile IPv6 service with the same LMA.

4. Attribute Value Pair Definitions

This section describes both new AVPs defined in this specification and re-used AVPs that are used in a PMIPv6 specific way. The AVPs described here are applicable for both MAG to HAAA and LMA to HAAA interfaces.

4.1. MIP6-Agent-Info AVP

The MIP6-Agent-Info grouped AVP is defined in [3]. This specification reuses the said AVP and its sub-AVPs to carry the LMA IP address and/or FQDN.

4.2. PMIP6-IPv4-Home-Address AVP

The PMIP6-IPv4-Home-Address AVP (AVP Code TBD) is of type Address and contains the IPv4-HoA of the MN. The primary use of this AVP is to carry the IPv4 Home Address, if available, from the HAAA to the MAG.

The PMIP6-IPv4-Home-Address AVP may also be used on the LMA to HAAA interface. In this scenario the AVP contains the IPv4 Home Address the LMA has assigned to the MN. If the LMA delegates assignment of the Home Address to the HAAA, the AVP MUST contain all zeroes address (i.e., 0.0.0.0) in the request message. The answer message SHOULD in all cases contain the assigned IPv4 Home Address value.

4.3. PMIP6-DHCP-Address AVP

The PMIP6-DHCP-Address AVP (AVP Code TBD) is of type Address and contains the IP address of the DHCPv4 and/or DHCPv6 server assigned to the MAG serving the newly attached MN. If the AVP contains a DHCPv4 server address, then the Address type MUST be IPv4. If the AVP contains a DHCPv6 server address, then the Address type MUST be IPv6. The HAAA MAY assign a DHCP server to the MAG in deployments where the MAG acts as a DHCP Relay and the DHCP Server is not co-located with the LMA [2].

4.4. PMIP6-Home-Prefix AVP

The PMIP6-Home-Prefix AVP (AVP Code TBD) is of type Address and contains the MN-NHP. The low 64 bits of the IPv6 address MUST be all zeroes. The high 64 bits of the IPv6 address are used as the MN-HNP. The primary use of this AVP is to carry the IPv6 Home Network Prefix, if available, from the HAAA to the MAG.

The PMIP6-Home-Prefix AVP may also be used on the LMA to HAAA interface. In this scenario the AVP contains the prefix the LMA has assigned to the MN. If the LMA delegates assignment of the home network prefix to the HAAA, the AVP MUST contain all zeroes address (i.e., 0::0) in the request message. The answer message SHOULD in all cases contain the assigned home prefix value.

4.5. MIP6-Feature-Vector AVP

The MIP6-Feature-Vector AVP is originally defined in [3]. This document only reserves new capability bits according to the rules in [3]. The new reserved bits contain PMIPv6 capability announcement of the MAG and the HAAA(/LMA)). Using the capability announcement it is possible to perform a simple capability negotiation between the MAG and the HAAA. Those capabilities that are announced by both parties are also known to be mutually supported. The following capability bits are defined in this document:

PMIP6_SUPPORTED (0x0000010000000000)

When the MAG/NAS sets this bit in the MIP6-Feature-Vector AVP, it is an indication to the HAAA that the NAS supports PMIPv6. When the HAAA sets this bit in the response MIP6-Feature-Vector AVP, it indicates that the HAAA also has PMIPv6 support. This capability bit can also be used to allow PMIPv6 mobility support in a subscription granularity.

IP4_HOA_SUPPORTED (0x0000020000000000)

Assignment of the IPv4-HoA is supported. When the MAG sets this bit in the MIP6-Feature-Vector AVP, it indicates that the MAG implements a minimal functionality of a DHCP server (and a relay) and is able to deliver IPv4-HoA to the MN. When the HAAA sets this bit in the response MIP6-Feature-Vector AVP, it indicates that the HAAA has authorized the use of IPv4-HoA for the MN. If this bit is unset in the returned MIP6-Feature-Vector AVP, the HAAA does not authorize the configuration of IPv4 address.

LOCAL_MAG_ROUTING_SUPPORTED (0x0000040000000000)

Direct routing of IP packets between MNs anchored to the same MAG is supported. When a MAG sets this bit in the MIP6-Feature-Vector, it indicates that routing IP packets between MNs anchored to the same MAG is supported, without reverse tunneling packets via the LMA or requiring any Route Optimization related signaling (e.g. the Return Routability Procedure in [13]) prior direct routing. If this bit is unset in the returned MIP6-Feature-Vector AVP, the HAAA does not authorize direct routing of packets between MNs anchored to the same MAG. This policy feature MUST be supported per MN and subscription basis.

MD_IDENTIFIER_REQUIRED (0x0000080000000000)

If the MAG does not have a valid MN-Identifier that it could use in the subsequent PBUs, then the MAG solicits the HAAA for the MN-Identifier by setting the MD_IDENTIFIER_REQUIRED capability bit in the feature vector. If the HAAA is able to provide the MAG with a MN-Identifier (that supposedly guarantees PMIPv6 session continuity after the handover) then the HAAA also sets the MD_IDENTIFIER_REQUIRED capability bit in reply feature vector and also provides the MN-Identifier in the Mobile-Node-Identifier AVP. If the HAAA is not able to provide the MAG with a MN-Identifier, then the MD_IDENTIFIER_REQUIRED capability bit MUST be unset in the reply feature vector and the Mobile-Node-Identifier AVP MUST NOT be returned either.

The MIP6-Feature-Vector AVP is also used on the LMA to HAAA interface. Using the capability announcement AVP it is possible to perform a simple capability negotiation between the LMA and the HAAA. Those capabilities that are announced by both parties are also known to be mutually supported. The capabilities listed in earlier are also supported in the LMA to HAAA interface. The LMA to HAAA interface does not define any new capability values.

4.6. Mobile-Node-Identifier AVP

The Mobile-Node-Identifier AVP (AVP Code TBD) is of type UTF8String and contains the mobile node identifier (MN-Identifier, see [1]) in a NAI [5] format. This AVP is used on the MAG to HAAA interface.

The usage of the Mobile-node-Identifier AVP is the following. If the MAG does not have a valid MN-Identifier that it could use in the subsequent PBUs, then the MAG informs the HAAA of this using the MN_IDENTIFIER_REQUIRED MIP6-Feature-Vector AVP capability bit in the initial Diameter request message from the MAG to the HAAA. Including the feature vector with the MN_IDENTIFIER_REQUIRED capability bit set in the request message indicates to the HAAA that the MAG solicits the HAAA for a valid MN-Identifier.

The Mobile-Node-Identifier AVP is returned in the answer message that ends a successful authentication (and possibly an authorization) exchange between the MAG and the HAAA, assuming the HAAA is also able to provide the MAG with the MN-Identifier in the first place. The MAG MUST use the received MN-Identifier, if it solicited one in the request message. If the MAG receives the Mobile-Node-Identifier AVP from the HAAA unsolicited then the MAG is not required to use the received MN-identifier.

4.7. Calling-Station-Id AVP

The Calling-Station-Id AVP (AVP Code 31) is of type UTF8String and contains a Link-Layer Identifier of the MN. This identifier may correspond to a real physical interface or something that the MAG has generated.

4.8. Service-Selection AVP

The Service-Selection AVP (AVP Code TBD) is of type UTF8String and contains a LMA provided service identifier on the LMA to HAAA interface. The service identifier may be used to assist the PBU authorization. The identifier MUST be unique within the PMIPv6 domain. This AVP is re-used from [14].

4.9. Session-Timeout AVP

The Session-Timeout AVP (AVP Code 27) is of type Unsigned32 and contains lifetime of the Binding Cache Entry in a unit of seconds.

5. MAG to HAAA Interface Application Support

5.1. Application Support and Command Codes

This specification does not define a new Application-ID for the MAG to HAAA interface. Rather, this specification re-uses any Diameter application and its commands that are used to authenticate and authorize the MN for the network access and mobility service. Example applications include NASREQ [6] and EAP [7]. The MAG acts as a Diameter client.

The MAG to HAAA interface is primarily used for bootstrapping PMIPv6 mobility service session when a MN attaches and authenticates to a PMIPv6 domain. This includes the bootstrapping of PMIPv6 session related information and possibly PMIPv6 security related information retrieval. The same interface may also be used for accounting.

Whenever the MAG sends a Diameter request message to the HAAA the User-Name AVP MUST contain the MN identity. At minimum the home realm of the MN MUST be available at the MAG when the network access authentication takes place. Otherwise the MAG is not able to route the Diameter request messages towards the correct HAAA. The MN identity MUST be in Network Access Identifier (NAI) [5] format.

The Diameter response messages MAY contain Framed-IPv6-Prefix and/or Framed-IPv4-Address AVPs. For example a local Diameter proxy MAY add those in order to advertise locally available prefixes and addresses as well [15]. It is also possible that PMIPv6 mobility support is not allowed for a subscription. In this case, a MAG may still provide normal IP connectivity to the MN using, for example, local address pools.

5.2. Accounting at MAG

The accounting at the MAG to HAAA interface is based on the [6]. The application identifier used for accounting is the Diameter Base Accounting (3) [8].

TBD.

6. LMA to HAAA Interface Application Support

6.1. Application Support and Command Codes

The LMA to HAAA interface may be used for multiple purposes. These include the authorization of the incoming PBU, possible PMIPv6 security related information retrieval, accounting and PMIPv6 session management.

This specification defines a new Application-ID for the LMA to HAAA interface and specifically for the authorization of the Proxy Binding Updates. The new application identifier is TBD BY IANA. The new application also defines two new commands and respective Command Codes: LHA-Request (value of TBD) and LHA-Answer (value of TBD). The LMA acts as a Diameter client.

6.2. Authorization of the Proxy Binding Update

Whenever the LMA sends a Diameter request message to the HAAA, the User-Name AVP MUST contain the MN identity. The identity MUST be in a NAI format. The LMA MAY retrieve the MN identity information from the PBU MN-ID [16][1] mobility option. The identity SHOULD be the same as used on the MAG to HAAA interface, but in a case those identities differ the HAAA MUST have a mechanism of mapping the MN identity used on the MAG to HAAA interface to the identity used on the LMA to HAAA interface.

If the PBU contains the MN Link-Layer Identifier option, the Calling-Station-Id AVP SHOULD be included in the request message containing the received Link-Layer Identifier. Furthermore, if the PBU contains the Service Selection mobility option [17], the Service-Selection AVP SHOULD be included in the request message containing the received service identifier.

The LMA and the HAAA use the PMIP6-Home-Prefix AVP to exchange the MN-HNP when appropriate. The low 64 bits of the prefix must be all zeroes. Similarly, the LMA and the HAAA use the PMIP6-IPv4-Home-Address AVP to exchange the MN IPv4-HoA when appropriate. If the PMIP6-Home-Prefix is set to an all zeroes address (i.e., 0::0) in the request message, it is an indication that the HAAA needs to assign the MN-HNP and return it to the LMA in the response message. If the PMIP6-IPv4-Home-Address is set to all zeroes (i.e., 0.0.0.0) in the request message, it is an indication that the HAAA needs to assign the MN IPv4-HoA and return it to the LMA in the response message.

The Auth-Request-Type AVP MUST be set to the value AUTHORIZE_ONLY. If the HAAA is not able to authorize the subscriber's mobility service session, then the reply message to the LMA MUST have the Result-Code AVP set to value DIAMETER_PMIP6_AUTHORIZATION_FAILED (TBD BY IANA) indicating a permanent failure.

The LMA to HAAA interface can also be used to update the selected LMA address to the HAAA. This applies to the case where the MAG, for example, discovers the LMA address using the DNS.

6.2.1. LHA-Request

The LHA-Request (LHAR, value of TBD) message is sent by the LMA to the Diameter server to initiate a mobility service session authorization procedure. The LHAR message format is defined below:

```
<LHA-Request> ::= < Diameter Header: TBD, REQ, PXY >
                  < Session-ID >
                  { Auth-Application-Id }
                  { User-Name }
                  { Destination-Realm }
                  { Origin-Host }
                  { Origin-Realm }
                  { Auth-Request-Type }
                  [ Destination-Host ]
                  [ Origin-State-Id ]
                  [ NAS-Identifier ]
                  [ NAS-IP-Address ]
                  [ NAS-IPv6-Address ]
                  [ NAS-Port-Type ]
                  [ Called-Station-Id ]
                  [ Calling-Station-Id ]
                  { MIP6-Feature-Vector }
                  { MIP6-Agent-Info }
                * [ PMIP6-Home-Prefix ]
                  [ PMIP6-IPv4-Home-Address ]
                  [ Service-Selection ]
                  [ Authorization-Lifetime ]
                  [ Auth-Session-State ]
                * [ Proxy-Info ]
                * [ Route-Record ]
                * [ AVP ]
```

6.2.2. LHA-Answer

The LHA-Answer (LHAA, value of TBD) message is sent in response to the LHA-Request (LHAR) message. If the mobility service session authorization procedure was successful then the response MAY include PMIPv6 LMA to HAAA interface AVPs. The PMIP6-Home-Prefix AVP contains MN-HNP and the PMIP6-IPv4-Home-Address AVP contains IPv4-HoA, if such information are needed. The LHAA message format is defined below:

```
<LHA-Answer> ::= < Diameter Header: TBD, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Result-Code }
                 { Origin-Host }
                 { Origin-Realm }
                 { Auth-Request-Type }
                 [ User-Name ]
                 [ Authorization-Lifetime ]
                 [ Auth-Session-State ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                 [ Re-Auth-Request-Type ]
                 [ MIP6-Feature-Vector ]
               * [ PMIP6-Home-Prefix ]
                 [ PMIP6-IPv4-Home-Address ]
                 [ Session-Timeout ]
                 [ Chargeable-User-Identity ]
                 [ Origin-State-Id ]
               * [ Proxy-Info ]
               * [ Redirect-Host ]
                 [ Redirect-Host-Usage ]
                 [ Redirect-Max-Cache-Time ]
               * [ Failed-AVP ]
               * [ AVP ]
```

6.3. Accounting at LMA

The accounting at the LMA to HAAA interface is based on the [6]. The application identifier used for accounting is the Diameter Base Accounting (3) [8].

TBD.

7. Proxy Mobile IPv6 Session Management

Concerning a PMIPv6 session, the HAAA MAY maintain a state. The LMA and the MAG MUST support the Authorization Session State Machine defined in [8]. Diameter session termination related commands described in the following sections may be exchanged between the LMA and the HAAA.

The actual PMIPv6 session termination procedures take place at PMIPv6 protocol level and are out of scope of this document.

7.1. Session-Termination-Request

The LMA or the MAG MAY send the Session-Termination-Request (STR) command [8] to the HAAA and inform the termination of an ongoing PMIPv6 session is in progress.

7.2. Session-Termination-Answer

The Session-Termination-Answer (STA) [8] is sent by the HAAA to acknowledge the termination of a PMIPv6 session.

7.3. Abort-Session-Request

The HAAA MAY send the Abort-Session-Request (ACR) command [8] to the LMA or to the MAG and request termination of a PMIPv6 session.

7.4. Abort-Session-Answer

The Abort-Session-Answer (ASA) command [8]is sent by the LMA or the MAG to acknowledge that the termination of a PMIPv6 session.

8. Attribute Value Pair Occurrence Tables

The following tables list the PMIPv6 MAG to HAAA interface and LMA to HAAA interface AVPs including those that are defined in [3].

The Figure 2 contains the AVPs and their occurrences on the MAG to HAAA interface. The AVPs that are part of grouped AVP are not listed in the table, rather only the grouped AVP is listed.

8.1. MAG to HAAA Interface

Attribute Name	Command-Code REQ	Command-Code ANS
PMIP6-DHCP-Address	0	0+
MIP6-Agent-Info	0	0+
MIP6-Feature-Vector	0-1	0-1
PMIP6-IPv4-Home-Address	0	0-1
PMIP6-Home-Prefix	0	0+
Mobile-Node-Identifier	0-1	0-1
Calling-Station-Id	0-1	0

Figure 2: MAG to HAAA Interface Generic Diameter Request and Answer Commands AVPs

The following table describes the Diameter AVPs code values, types, possible flag values, and whether the AVP MAY be encrypted. The Diameter base protocol specification [8] specifies the AVP Flags rules for AVPs in section 4.5. Due to space constraints, the short form DiamIdent is used to represent DiameterIdentity and OctetStr is used to represent OctetString.

Attribute Name	AVP Code	Section Defined	Data Type	AVP Flag rules MUST	MAY	SHLD NOT	MUST NOT	Encr
MIP6-Agent-Info	TBD	4.1	Grouped		P		M,V	Y
PMIP6-IPv4-Home-Address	TBD	4.2	Address		P		M,V	Y
PMIP6-DHCP-Address	TBD	4.3	Address		P		M,V	Y
PMIP6-Home-Prefix	TBD	4.4	Address		P		M,V	Y
MIP6-Feature-Vector	TBD	4.5	Unsigned64		P		M,V	Y
Calling-Station-Id	31	4.7	UTF8String		P		M,V	Y
Mobile-Node-Identifier	TBD	4.6	UTF8String		P		M,V	Y

Figure 3: AVP Flag Rules Table

8.2. LMA to HAAA Interface

The AVP occurrences are defined in the ABNFs for the LHA-Request (see Section 6.2.1) and LHA-Answer (see Section 6.2.2) commands.

The following table describes the Diameter AVPs code values, types, possible flag values, and whether the AVP MAY be encrypted. The Diameter base protocol specification [8] specifies the AVP Flags rules for AVPs in section 4.5. Due to space constraints, the short form DiamIdent is used to represent DiameterIdentity and OctetStr is used to represent OctetString.

				AVP Flag rules				
Attribute Name	AVP Code	Section Defined	Data Type	MUST	MAY	SHLD NOT	MUST NOT	Encr
MIP6-Agent-Info	TBD	4.1	Grouped	M	P		V	Y
PMIP6-IPv4-Home-Address	TBD	4.2	Address	M	P		V	Y
PMIP6-Home-Prefix	TBD	4.4	Address	M	P		V	Y
MIP6-Feature-Vector	TBD	4.5	Unsigned64	M	P		V	Y
Calling-Station-Id	31	4.7	UTF8String	M	P		V	Y
Service-Selection	TBD	4.8	UTF8String	M	P		V	Y
Session-Timeout	27	4.9	Unsigned32	M	P		V	Y

Figure 4: AVP Flag Rules Table

9. IANA Considerations

9.1. Attribute Value Pair Codes

This specification defines the following new AVPs:

PMIP6-DHCP-Address	is set to TBD
PMIP6-Home-Prefix	is set to TBD
PMIP6-IPv4-Home-Address	is set to TBD
Mobile-Node-Identifier	is set to TBD

9.2. Namespaces

This specification defines new values to the Mobility Capability registry (see [3]) for use with the MIP6-Feature-Vector AVP:

Token	Value	Description
PMIP6_SUPPORTED	0x0000010000000000	[RFC TBD]
IP4_HOA_SUPPORTED	0x0000020000000000	[RFC TBD]
LOCAL_MAG_ROUTING_SUPPORTED	0x0000040000000000	[RFC TBD]
MD_IDENTIFIER_REQUIRED	0x0000080000000000	[RFC TBD]

9.3. Application Identifiers

This specification requires IANA to allocate a new value for "Diameter Proxy Mobile IPv6" (PMIP6) from the Application Identifier namespace defined in [8].

9.4. Command Codes

IANA is requested to allocate new command code values for the following new commands from the Command Code namespace defined in [8].

Command Code	Value
LHA-Request (LHAR)	TBD
LHA-Answer (LHAA)	TBD

9.5. Result-Code AVP Values

This specification requests IANA to allocate a new value to the Result-Code AVP (AVP Code 268) address space within the Permanent Failures category (5xxx) defined in [8]:

DIAMETER_PMIP6_AUTHORIZATION_FAILED is set to TBD

10. Security Considerations

The security considerations for the Diameter interaction required by PMIPv6 mobility service setup are described in [9]. Additionally, the security considerations of the Diameter Base protocol [8], Diameter EAP application [7] are applicable to this document. This document does not introduce new security vulnerabilities.

The Diameter messages may be transported between the HA and the Diameter server via one or more AAA brokers or Diameter agents. In this case the HA to the Diameter server AAA communication rely on the security properties of the intermediate AAA brokers and Diameter agents (such as proxies).

11. Acknowledgements

Jouni Korhonen would like to thank TEKES MERCoNe project for providing funding to work on this document.

12. References

12.1. Normative References

[1] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[2] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", draft-ietf-netlmm-pmip6-ipv4-support-04 (work in progress), July 2008.

[3] Korhonen, J., Bournelle, J., Tschofenig, H., Perkins, C., and K. Chowdhury, "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction", draft-ietf-dime-mip6-integrated-10 (work in progress), September 2008.

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

[5] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[6] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

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

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

12.2. Informative References

[9] Korhonen, J. and A. Muhanna, "Policy Profile and AAA Interfaces Requirements for PMIPv6", draft-korhonen-netlmm-pp-aaa-reqs-00 (work in progress), February 2008.

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

[11] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[12] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

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

[14] Korhonen, J., Tschofenig, H., Bournelle, J., Giaretta, G., and M. Nakhjiri, "Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction", draft-ietf-dime-mip6-split-10 (work in progress), July 2008.

[15] Damic, D., Premec, D., Patil, B., Sahasrabudhe, M., and S. Krishnan, "Proxy Mobile IPv6 indication and discovery", draft-damic-netlmm-pmip6-ind-discover-03 (work in progress), February 2008.

[16] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

[17] Korhonen, J., Nilsson, U., and V. Devarapalli, "Service Selection for Mobile IPv6", RFC 5149, February 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

Ahmad Muhanna
Nortel
2221 Lakeside Blvd.
Richardson, TX 75082
USA

Email: amuhanna@nortel.com

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury MA 01876
US

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

Ulrike Meyer
RWTH Aachen

Email: meyer@umic.rwth-aachen.de

Full Copyright Statement

Intellectual Property

Acknowledgment

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