Internet Engineering Task Force (IETF)
Request for Comments: 5779
Category: Standards Track
ISSN: 2070-1721

J. Korhonen, Ed.
Nokia Siemens Network
J. Bournelle
Orange Labs
K. Chowdhury
Cisco Systems
A. Muhanna
Ericsson
U. Meyer
RWTH Aachen

February 2010

Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server

Abstract

This specification defines Authentication, Authorization, and Accounting (AAA) interactions between Proxy Mobile IPv6 entities (both Mobile Access Gateway and Local Mobility Anchor) and a AAA server within a Proxy Mobile IPv6 Domain. These AAA interactions are primarily used to download and update mobile node specific policy profile information between Proxy Mobile IPv6 entities and a remote policy store.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5779.

Table of Contents

1. Introduction

This specification defines Authentication, Authorization, and Accounting (AAA) interactions between a Mobile Access Gateway (MAG) and a AAA server, and between a Local Mobility Anchor (LMA) and a AAA server within a Proxy Mobile IPv6 (PMIPv6) Domain [RFC5213]. These AAA interactions are primarily used to download and update mobile node (MN) specific policy profile information between PMIPv6 entities (a MAG and an LMA) and a remote policy store.

Dynamic assignment and downloading of an MN's policy profile information to a MAG from a remote policy store is a desirable feature to ease the deployment and network maintenance of larger PMIPv6 domains. For this purpose, the same AAA infrastructure that is used for authenticating and authorizing the MN for a network access can be leveraged to download some or all of the necessary policy profile information to the MAG.

Once the network has authenticated the MN, the MAG sends a Proxy Binding Update (PBU) to the LMA in order to set up a mobility session on behalf of the MN. When the LMA receives the PBU, the LMA may need to authorize the received PBU against the AAA infrastructure. The same AAA infrastructure that can be used for the authorization of the PBU, is also used to update the remote policy store with the LMA-provided MN specific mobility session-related information.

In the context of this specification, the home AAA (HAAA) server functionality is co-located with the remote policy store. The NAS functionality may be co-located with the MAG function in the network access router. Diameter [RFC3588] is the used AAA protocol.

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 RFC 2119 [RFC2119].

The general terminology used in this document can be found in [RFC5213] and [NETLMM-PMIP6]. The following additional or clarified terms are also 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.

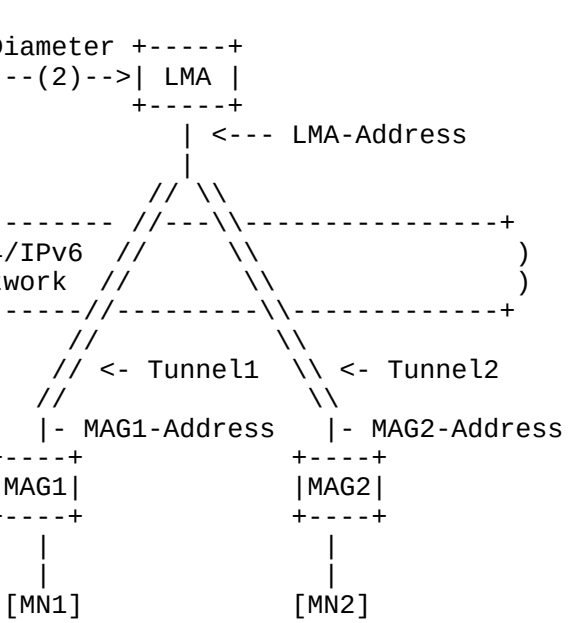
Home AAA (HAAA):

An Authentication, Authorization, and Accounting (AAA) server located in user's home network. A HAAA is essentially a Diameter server.

3. Solution Overview

This document addresses the AAA interactions and AAA-based session management functionality needed in the PMIPv6 Domain. This document defines Diameter-based AAA interactions between the MAG and the HAAA, and between the LMA and the HAAA.

The policy profile is downloaded from the HAAA to the MAG during the MN attachment to the PMIPv6 Domain. Figure 1 shows the participating network entities. This document, however, concentrates on the MAG, LMA, and the HAAA (the home Diameter server).



Legend:

(1): MAG-to-HAAA interaction is described in Section 7.1
(2): LMA-to-HAAA interaction is described in Section 7.2

Figure 1: Proxy Mobile IPv6 Domain Interaction with Diameter HAAA Server

When an MN attaches to a PMIPv6 Domain, a network access authentication procedure is usually started. The choice of the authentication mechanism is specific to the access network deployment, but could be based on the Extensible Authentication Protocol (EAP) [RFC3748]. 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, PMIPv6 specific information is returned along with the successful network access authentication answer to the MAG.

After the MN has been successfully authenticated, the MAG sends a PBU to the LMA based on the MN's policy profile information. Upon receiving the PBU, the LMA interacts with the HAAA and fetches the relevant parts of the subscriber policy profile and authorization information related to the mobility service session. In this specification, the HAAA has the role of the PMIPv6 remote policy store.

4. Generic Application Support and Command Codes

This specification does not define new Application-IDs or Command Codes for the MAG-to-HAAA or for the LMA-to-HAAA Diameter connections. Rather, this specification is generic to any Diameter application (and their commands) that is suitable for a network access authentication and authorization. Example applications include NASREQ [RFC4005] and EAP [RFC4072].

4.1. MAG-to-HAAA Interface

The MAG-to-HAAA interactions are primarily used for bootstrapping PMIPv6 mobility service session when an MN attaches and authenticates to a PMIPv6 Domain. This includes the bootstrapping of PMIPv6 session-related information. The same interface may also be used for accounting. The MAG acts as a Diameter client.

Whenever the MAG sends a Diameter request message to the HAAA, the User-Name AVP SHOULD contain the MN's identity unless the identity is being suppressed for policy reasons -- for example, when identity hiding is in effect. The MN identity, if available, MUST be in Network Access Identifier (NAI) [RFC4282] format. 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 used on the MAG-to-HAAA interface and in the User-Name AVP MAY entirely be related to the network access authentication, and

therefore not suitable to be used as the MN-ID mobility option value in the subsequent PBU / Proxy Binding Acknowledgement (PBA) messages. See the related discussion on MN identities in Sections 4.2 and 5.6.

For the session management and service authorization purposes, session state SHOULD be maintained on the MAG-to-HAAA interface. See the discussion in Section 5.8.

4.2. LMA-to-HAAA Interface

The LMA-to-HAAA interface may be used for multiple purposes. These include the authorization of the incoming PBU, updating the LMA address to the HAAA, delegating the assignment of the MN-HNP (home network prefix) or the IPv4-HoA (home address) to the HAAA, and for accounting and PMIPv6 session management. The primary purpose of this interface is to update the HAAA with the LMA address information in case of dynamically assigned LMA, and exchange the MN address assignment information between the LMA and the HAAA.

The LMA-to-HAAA interface description is intended for different types of deployments and architectures. Therefore, this specification only outlines AVPs and considerations that the deployment specific Diameter applications need to take into account from the PMIPv6 and LMA's point of view.

4.2.1. General Operation and Authorization of PBU

Whenever the LMA sends a Diameter request message to the HAAA, the User-Name AVP SHOULD contain the MN's identity. The LMA-provided identity in the User-Name AVP is strongly RECOMMENDED to be the same as the MN's identity information in the PBU MN-ID [RFC4283] [RFC5213] mobility option. The identity SHOULD also be the same as used on the MAG-to-HAAA interface, but in 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 [RFC5149], the Service-Selection AVP SHOULD be included in the request message containing the received service identifier. Both the MN link-layer identifier and the service selection can be used to provide more information for the PBU authorization step in the HAAA.

The Auth-Request-Type AVP MUST be set to the value AUTHORIZE_ONLY. The Diameter session-related aspects discussed in Section 6 need to be taken into consideration when designing the Diameter application

for the LMA-to-HAAA interface. 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_AUTHORIZATION_REJECTED (5003) indicating a permanent failure. A failed authorization obviously results in a rejection of the PBU, and a PBA with an appropriate error Status Value MUST be sent back to the MAG.

The authorization step MUST be performed at least for the initial PBU session up to a mobility session, when the LMA-to-HAAA interface is deployed. For the subsequent re-registration and handover PBUs, the authorization step MAY be repeated (in this case, the LMA-to-HAAA interface should also maintain an authorization session state).

4.2.2. Updating LMA Address to HAAA

In case of a dynamic LMA discovery and assignment [NETLMM-LMA], the HAAA and the remote policy store may need to be updated with the selected LMA address information. The update can be done during the PBU authorization step using the LMA-to-HAAA interface. This specification uses the MIP6-Agent-Info AVP and its MIP-Home-Agent-Address and MIP-Home-Agent-Host sub-AVPs for carrying the LMA's address information from the LMA to the HAAA. The LMA address information in the request message MUST contain the IP address of the LMA or the Fully Qualified Domain Name (FQDN) identifying uniquely the LMA, or both. The LMA address information refers to the PMIPv6 part of the LMA, not necessarily the LMA part interfacing with the AAA infrastructure.

This specification does not define any HAAA-initiated LMA relocation functionality. Therefore, when the MIP6-Agent-Info AVP is included in Diameter answer messages sent from the HAAA to the LMA, the HAAA indicates this by setting the MIP-Home-Agent-Address AVP to all zeroes address (e.g., 0::0) and not including the MIP-Home-Agent-Host AVP.

4.2.3. Mobile Node Address Update and Assignment

The LMA and the HAAA use the MIP6-Home-Link-Prefix AVP to exchange the MN-HNP when appropriate. Similarly, the LMA and the HAAA use the PMIP6-IPv4-Home-Address AVP to exchange the IPv4-MN-HoA when appropriate. These AVPs are encapsulated inside the MIP6-Agent-Info AVP. The MN address information exchange is again done during the PBU authorization step. The HAAA MAY also use the LMA-provided MN address information as a part of the information used to authorize the PBU.

Which entity is actually responsible for the address management is deployment specific within the PMIPv6 Domain and MUST be pre-agreed on per deployment basis. When the LMA is responsible for the address management, the MIP6-Agent-Info AVP is used to inform the HAAA and the remote policy store of the MN-HNP/IPv4-MN-HoA assigned to the MN.

It is also possible that the LMA delegates the address management to the HAAA. In this case, the MN-HNP/IPv4-MN-HoA are set to undefined addresses (as described in Section 5.1) in the Diameter request message sent from the LMA to the HAAA. The LMA expects to receive the HAAA assigned HNP/IPv4-MN-HoA in the corresponding Diameter answer message.

5. Attribute Value Pair Definitions

This section describes Attribute Value Pairs (AVPs) defined by this specification or re-used from existing specifications in a PMIPv6 specific way. Derived Diameter AVP Data Formats such as Address and UTF8String are defined in Section 4.3 of [RFC3588]. Grouped AVP values are defined in Section 4.4 of [RFC3588].

5.1. MIP6-Agent-Info AVP

The MIP6-Agent-Info grouped AVP (AVP Code 486) is defined in [RFC5447]. The AVP is used to carry LMA addressing-related information and an MN-HNP. This specification extends the MIP6-Agent-Info with the PMIP6-IPv4-Home-Address AVP using the Diameter extensibility rules defined in [RFC3588]. The PMIP6-IPv4-Home-Address AVP contains the IPv4-MN-HoA.

The extended MIP6-Agent-Info AVP results in the following grouped AVP. The grouped AVP has the following modified ABNF (as defined in [RFC3588]):

```
MIP6-Agent-Info ::= < AVP-Header: 486 >
                    *2[ MIP-Home-Agent-Address ]
                      [ MIP-Home-Agent-Host ]
                      [ MIP6-Home-Link-Prefix ]
                      [ PMIP6-IPv4-Home-Address ]
                    * [ AVP ]
```

If the MIP-Home-Agent-Address is set to all zeroes address (e.g., 0::0), the receiver of the MIP6-Agent-Info AVP MUST ignore the MIP-Home-Agent-Address AVP.

5.2. PMIP6-IPv4-Home-Address AVP

The PMIP6-IPv4-Home-Address AVP (AVP Code 505) is of type Address and contains an IPv4 address. This AVP is used to carry the IPv4-MN-HoA, if available, from the HAAA to the MAG. This AVP SHOULD only be present when the MN is statically provisioned with the IPv4-MN-HoA. Note that proactive dynamic assignment of the IPv4-MN-HoA by the HAAA may result in unnecessary reservation of IPv4 address resources, because the MN may considerably delay or completely bypass its IPv4 address configuration.

The PMIP6-IPv4-Home-Address AVP is also used on the LMA-to-HAAA interface. The AVP contains the IPv4-MN-HoA assigned to the MN. If the LMA delegates the assignment of the IPv4-MN-HoA to the HAAA, the AVP MUST contain all zeroes IPv4 address (i.e., 0.0.0.0) in the request message. If the LMA delegated the IPv4-MN-HoA assignment to the HAAA, then the AVP contains the HAAA assigned IPv4-MN-HoA in the response message.

5.3. MIP6-Home-Link-Prefix AVP

The MIP6-Home-Link-Prefix AVP (AVP Code 125) is defined in [RFC5447]. This AVP is used to carry the MN-HNP, if available, from the HAAA to the MAG. The low 64 bits of the prefix MUST be all zeroes.

The MIP6-Home-Link-Prefix AVP is also used on the LMA-to-HAAA interface. The AVP contains the prefix assigned to the MN. If the LMA delegates the assignment of the MN-HNP to the HAAA, the AVP MUST contain all zeroes address (i.e., 0::0) in the request message. If the LMA delegated the MN-HNP assignment to the HAAA, then the AVP contains the HAAA-assigned MN-HNP in the response message.

5.4. PMIP6-DHCP-Server-Address AVP

The PMIP6-DHCP-Server-Address AVP (AVP Code 504) is of type Address and contains the IP address of the Dynamic Host Configuration Protocol (DHCP) server assigned to the MAG serving the newly attached MN. If the AVP contains a DHCPv4 [RFC2131] server address, then the Address type MUST be IPv4. If the AVP contains a DHCPv6 [RFC3315] 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 [NETLMM-PMIP6].

5.5. MIP6-Feature-Vector AVP

The MIP6-Feature-Vector AVP is originally defined in [RFC5447]. This document defines new capability flag bits according to the IANA rules in RFC 5447.

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-MN-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-MN-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-MN-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 as described in Sections 6.10.3 and 9.2 of [RFC5213]. 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 [RFC3775]) prior direct routing. If this bit is cleared in the returned MIP6-Feature-Vector AVP, the HAAA does not authorize direct routing of packets between MNs anchored to the same MAG. The MAG SHOULD support this policy feature on a per-MN and per-subscription basis.

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.

5.6. Mobile-Node-Identifier AVP

The Mobile-Node-Identifier AVP (AVP Code 506) is of type UTF8String and contains the mobile node identifier (MN-Identifier; see [RFC5213]) in the NAI [RFC4282] format. This AVP is used on the MAG-to-HAAA interface. The Mobile-Node-Identifier AVP is designed for

deployments where the MAG does not have a way to find out such MN identity that could be used in subsequent PBU/PBA exchanges (e.g., due to identity hiding during the network access authentication) or the HAAA wants to assign periodically changing identities to the MN.

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 has not been able to get the mobile node identifier through other means. If the MAG already has a valid mobile node identifier, then the MAG MUST silently discard the received MN-Identifier.

5.7. 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 corresponds to the link-layer identifier as defined in RFC 5213, Sections 2.2 and 8.6. The Link-Layer Identifier is encoded in ASCII format (upper case only), with octet values separated by a "-". Example: "00-23-32-C9-79-38". The encoding is actually the same as the MAC address encoding in Section 3.21 of RFC 3580.

5.8. Service-Selection AVP

The Service-Selection AVP (AVP Code 493) is of type UTF8String and contains an LMA-provided service identifier on the LMA-to-HAAA interface. This AVP is re-used from [RFC5778]. The service identifier may be used to assist the PBU authorization and the assignment of the MN-HNP and the IPv4-MN-HoA as described in RFC 5149 [RFC5149]. The identifier MUST be unique within the PMIPv6 Domain. In the absence of the Service-Selection AVP in the request message, the HAAA may want to inform the LMA of the default service provisioned to the MN and include the Service-Selection AVP in the response message.

It is also possible that the MAG receives the service selection information from the MN, for example, via some lower layer mechanism. In this case, the MAG MUST include the Service-Selection AVP also in the MAG-to-HAAA request messages. In the absence of the Service-Selection AVP in the MAG-to-HAAA request messages, the HAAA may want to inform the MAG of the default service provisioned to the MN and include the Service-Selection AVP in the response message.

Whenever the Service-Selection AVP is included either in a request message or in a response message, and the AAA interaction with HAAA completes successfully, it is an indication that the HAAA also authorized the MN to some service. This should be taken into account when considering what to include in the Auth-Request-Type AVP.

The service selection concept supports signaling one service at time. However, the MN policy profile MAY support multiple services being used simultaneously. For this purpose, the HAAA MAY return multiple LMA and service pairs (see Section 5.9) to the MAG in a response message that ends a successful authentication (and possibly an authorization) exchange between the MAG and the HAAA. Whenever the MN initiates an additional mobility session to another service (using a link layer or deployment specific method), the provisioned service information is already contained in the MAG. Therefore, there is no need for additional AAA signaling between the MAG and the HAAA.

5.9. Service-Configuration AVP

The Service-Configuration AVP (AVP Code 507) is of type Grouped and contains a service and an LMA pair. The HAAA can use this AVP to inform the MAG of the MN's subscribed services and LMAs where those services are hosted in.

```
Service-Configuration ::= < AVP-Header: 507 >
                          [ MIP6-Agent-Info ]
                          [ Service-Selection ]
                        * [ AVP ]
```

6. Proxy Mobile IPv6 Session Management

Concerning a PMIPv6 mobility session, the HAAA, the MAG, and the LMA Diameter entities SHOULD be stateful and maintain the corresponding Authorization Session State Machine defined in [RFC3588]. If a state is maintained, then a PMIPv6 mobility session that can be identified by any of the Binding Cache Entry (BCE) Lookup Keys described in RFC 5213 (see Sections 5.4.1.1, 5.4.1.2, and 5.4.1.3) MUST map to a single Diameter Session-Id. If the PMIPv6 Domain allows further separation of sessions, for example, identified by the RFC 5213 BCE Lookup Keys and the service selection combination (see Section 5.8 and [RFC5149]), then a single Diameter Session-Id MUST map to a PMIPv6 mobility session identified by the RFC 5213 BCE Lookup Keys and the selected service.

If both the MAG-to-HAAA and the LMA-to-HAAA interfaces are deployed in a PMIPv6 Domain, and a state is maintained on both interfaces, then one PMIPv6 mobility session would have two distinct Diameter

sessions on the HAAA. The HAAA needs to be aware of this deployment possibility and SHOULD allow multiple Diameter sessions for the same PMIPv6 mobility session.

Diameter session termination-related commands described in the following sections may be exchanged between the LMA and the HAAA, or between the MAG and the HAAA. The actual PMIPv6 session termination procedures take place at the PMIPv6 protocol level and are described in more detail in RFC 5213 and [MEXT-BINDING].

6.1. Session-Termination-Request

The LMA or the MAG MAY send the Session-Termination-Request (STR) command [RFC3588] to inform the HAAA that the termination of an ongoing PMIPv6 session is in progress.

6.2. Session-Termination-Answer

The Session-Termination-Answer (STA) [RFC3588] is sent by the HAAA to acknowledge the termination of a PMIPv6 session.

6.3. Abort-Session-Request

The HAAA MAY send the Abort-Session-Request (ASR) command [RFC3588] to the LMA or to the MAG and request termination of a PMIPv6 session.

6.4. Abort-Session-Answer

The Abort-Session-Answer (ASA) command [RFC3588] is sent by the LMA or the MAG to acknowledge the termination of a PMIPv6 session.

7. 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 [RFC5447].

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.

7.1. MAG-to-HAAA Interface

Attribute Name	Command-Code REQ	Command-Code ANS
PMIP6-DHCP-Server-Address	0	0+
MIP6-Agent-Info	0+	0+
MIP6-Feature-Vector	0-1	0-1
Mobile-Node-Identifier	0-1	0-1
Calling-Station-Id	0-1	0
Service-Selection	0-1	0
Service-Configuration	0	0+

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

7.2. LMA-to-HAAA Interface

Attribute Name	Command-Code REQ	Command-Code ANS
MIP6-Agent-Info	0-1	0-1
MIP6-Feature-Vector	0-1	0-1
Calling-Station-Id	0-1	0
Service-Selection	0-1	0-1
User-Name	0-1	0-1

Figure 3: LMA-to-HAAA Interface Generic Diameter Request and Answer Commands AVPs

8. Example Signaling Flows

Figure 4 shows a signaling flow example during PMIPv6 bootstrapping using the AAA interactions defined in this specification. In step (1) of this example, the MN is authenticated to the PMIPv6 Domain using EAP-based authentication. The MAG to the HAAA signaling uses the Diameter EAP Application. During step (2), the LMA uses the Diameter NASREQ application to authorize the MN with the HAAA server.

The MAG-to-HAAA AVPs, as listed in Section 7.1, are used during step (1). These AVPs are included only in the Diameter EAP Request (DER) message which starts the EAP exchange and in the corresponding Diameter EAP Answer (DEA) message which successfully completes this EAP exchange. The LMA-to-HAAA AVPs, as listed in Section 7.2, are used during step (2). Step (2) is used to authorize the MN request for the mobility service and update the HAAA server with the assigned LMA information. In addition, this step may be used to dynamically assist in the assignment of the MN-HNP.

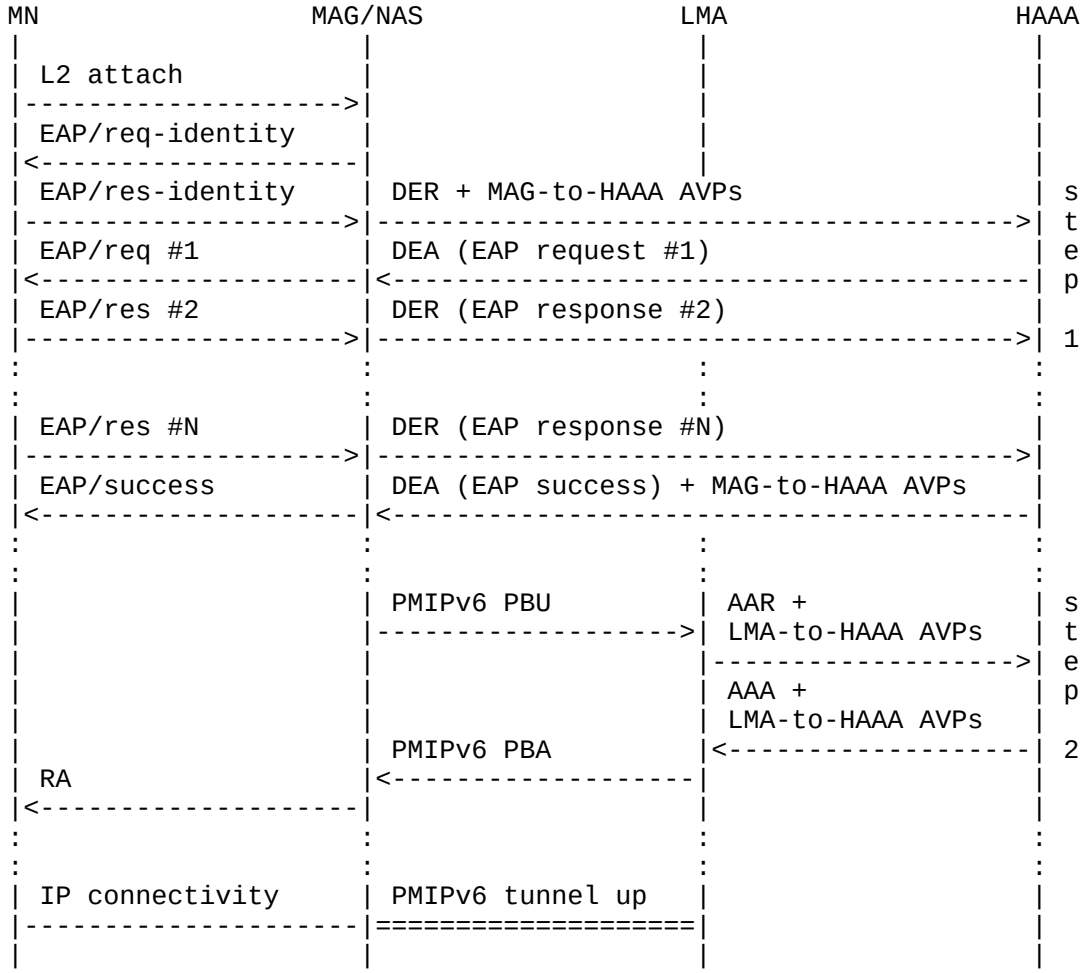


Figure 4: MAG and LMA Signaling Interaction with AAA Server during PMIPv6 Bootstrapping

9. IANA Considerations

9.1. Attribute Value Pair Codes

This specification defines the following new AVPs:

PMIP6-DHCP-Server-Address	504
PMIP6-IPv4-Home-Address	505
Mobile-Node-Identifier	506
Service-Configuration	507

9.2. Namespaces

This specification defines new values to the Mobility Capability registry (see [RFC5447]) for use with the MIP6-Feature-Vector AVP:

Token	Value	Description
PMIP6_SUPPORTED	0x0000010000000000	[RFC5779]
IP4_HOA_SUPPORTED	0x0000020000000000	[RFC5779]
LOCAL_MAG_ROUTING_SUPPORTED	0x0000040000000000	[RFC5779]

10. Security Considerations

The security considerations of the Diameter Base protocol [RFC3588], Diameter EAP application [RFC4072], Diameter NASREQ application [RFC4005], and Diameter Mobile IPv6 integrated scenario bootstrapping [RFC5447] are applicable to this document.

In general, the Diameter messages may be transported between the LMA and the Diameter server via one or more AAA brokers or Diameter agents. In this case, the LMA 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 the TEKES GIGA program MERCoNe-project for providing funding to work on this document while he was with TeliaSonera. The authors also thank Pasi Eronen, Peter McCann, Spencer Dawkins, and Marco Liebsch for their detailed reviews of this document.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC4005] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[RFC4072] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5447] Korhonen, J., Bournelle, J., Tschofenig, H., Perkins, C., and K. Chowdhury, "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction", RFC 5447, February 2009.

[RFC5778] Korhonen, J., Ed., Tschofenig, H., Bournelle, J., Giaretta, G., and M. Nakhjiri, "Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction", RFC 5778, February 2010.

12.2. Informative References

[MEXT-BINDING] Muhanna, A., Khalil, M., Gundavelli, S., Chowdhury, K., and P. Yegani, "Binding Revocation for IPv6 Mobility", Work in Progress, October 2009.

[NETLMM-LMA] Korhonen, J. and V. Devarapalli, "LMA Discovery for Proxy Mobile IPv6", Work in Progress, September 2009.

[NETLMM-PMIP6] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", Work in Progress, September 2009.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

[RFC5149] Korhonen, J., Nilsson, U., and V. Devarapalli, "Service Selection for Mobile IPv6", RFC 5149, February 2008.

Authors' Addresses

Jouni Korhonen (editor)
Nokia Siemens Network
Linnoitustie 6
Espoo FI-02600
Finland

EMail: jouni.nospam@gmail.com

Julien Bournelle
Orange Labs
38-4O rue du general Leclerc
Issy-Les-Moulineaux 92794
France

EMail: julien.bournelle@orange-ftgroup.com

Kuntal Chowdhury
Cisco Systems
30 International Place
Tewksbury, MA 01876
USA

EMail: kchowdhury@cisco.com

Ahmad Muhanna
Ericsson, Inc.
2201 Lakeside Blvd.
Richardson, TX 75082
USA

EMail: Ahmad.muhanna@ericsson.com

Ulrike Meyer
RWTH Aachen

EMail: meyer@umic.rwth-aachen.de