netext
Internet-Draft
Intended status: Standards Track
Expires: August 3, 2012

F. Xia
B. Sarikaya
Huawei USA
J. Korhonen, Ed.
Nokia Siemens Networks
S. Gundavelli
Cisco
D. Damic
Siemens

January 31, 2012

RADIUS Support for Proxy Mobile IPv6
draft-ietf-netext-radius-pmip6-08

Abstract

This document defines new attributes to facilitate Proxy Mobile IPv6 operations using the RADIUS infrastructure. The protocol defined in this document uses Radius based interfaces of the mobile access gateway and the local mobility anchor with the AAA server for authentication, authorization and policy functions. The RADIUS interactions between the mobile access gateway and the RADIUS-based AAA server take place when the Mobile Node attaches, authenticates and authorizes to a Proxy Mobile IPv6 domain. Furthermore, this document defines the RADIUS-based interface between the local mobility anchor and the AAA RADIUS server for authorizing received Proxy Binding Update messages for the mobile node's mobility session. In addition to the mobility session setup related interactions, this document defines the baseline for the mobile access gateway and the local mobility anchor generated accounting.

Table of Contents

1. Introduction

Proxy Mobile IPv6 (PMIPv6) [RFC5213] is a network-based mobility management protocol which allows IP mobility support for a mobile node without requiring the mobile node's participation in any mobility-related signaling. The mobile management elements in the network, the mobile access gateway (MAG) and the local mobility anchor (LMA) are the two key functions in this network-based mobility system. The mobile access gateway is responsible for detecting the mobile node's movements in the network and for initiating the needed mobility management signaling with the local mobility anchor (LMA). Both the mobility management agents make use of the AAA infrastructure to retrieve the mobile node's Policy Profile and for performing service authorization.

This document defines a RADIUS-based [RFC2865] profile and corresponding attributes to be used on the AAA interface between the MAG and the AAA RADIUS server. This interface is used to carry the per-MN Policy Profile from the remote Policy Store to the MAG. Furthermore, this document also defines a RADIUS-based interface between the LMA and the AAA RADIUS server for authorization of the received Proxy Mobile IPv6 signaling messages. The AAA procedures defined in this document cover the following two scenarios:

- a mobile node connects to the Proxy Mobile IPv6 domain from the home network
- a mobile node connects to the Proxy Mobile IPv6 domain from a visited network

2. Terminology

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].

All the mobility related terms used in this document are to be interpreted as defined in the Proxy Mobile IPv6 specification [RFC5213] and [RFC5844]. Additionally, this document uses the following abbreviations:

Network Access Server (NAS):

A function that provides authorization services for a device/user access to the network as defined in [RFC2865]. This document makes an assumption that the NAS function is co-located with the MAG. In scenarios where the NAS function and MAG are decoupled,

the messaging interface needed between them for the operation of PMIP6 is beyond the scope of this document.

Home AAA (HAAA):

An Authentication, Authorization, and Accounting (AAA) server located in MN's home network. This sever has access to the mobile node's policy profiles.

Visited AAA (VAAA):

An Authentication, Authorization, and Accounting (AAA) server located in MN's visited network. The VAAA server takes the role of a proxy-server, forwarding the received AAA service request to the HAAA server in the mobile node's home network and relaying the response to the requesting node, after applying any local access network policies.

3. Solution Overview

This document defines the RADIUS-based AAA interactions with the two mobility management elements in the Proxy Mobile IPv6 domain.

- Interactions between a MAG and a RADIUS-based AAA Server
- Interactions between a LMA and a RADIUS-based AAA Server

The mobile node's Policy Profile [RFC5213] is present in a policy store and is needed by the PMIPv6 mobility management elements for authorizing the mobile node for mobility management service and for obtaining various service related parameters. This policy store could be locally collocated with the mobility management agents enabling direct local access, or could be available from a AAA server through a RADIUS-based AAA interface.

When a mobile node attaches to an access network, the NAS on that access network may activate the network access authentication procedure. The choice of the authentication mechanism is specific to the access network deployment, however it is typically based on the Extensible Authentication Protocol (EAP) [RFC3748]. The NAS performs the network access authentication and queries the HAAA using AAA protocol, such as RADIUS. If the network access authentication succeeds, the MN's Policy Profile is obtained as part of the RADIUS message exchange with the AAA server.

The mobile node may be an IPv4-only node, IPv6-only node, or a dual-stack (IPv4/v6) node. Based on the policy specified in the Policy

Profile, the network access authentication procedure SHOULD provide the unambiguous indication of the type of address(es) to be assigned for the MN in the network and with all other service related and policy parameters relevant to the mobility service.

After the successful network access authentication and obtaining the mobile node's Policy Profile, the MAG sends a Proxy Binding Update (PBU) to the LMA. Upon receiving the PBU, the LMA interacts with the HAAA for obtaining the mobile node's Policy Profile, which is required for authorizing and activating mobility service.

This document adds support for three distinct PMIPv6 mobility use cases, taking into account the administrative domains to which the MAG and the LMA belong to. The following are the three relevant deployment models.

1. the MAG and LMA are both in the home network,
2. the MAG and LMA are both in the visited network
3. the MAG is in the visited network while the LMA is in the home network.

Figure 1 shows participating network entities for the PMIPv6 mobility session which is located in the home network. The MAG and LMA interact only with the HAAA.

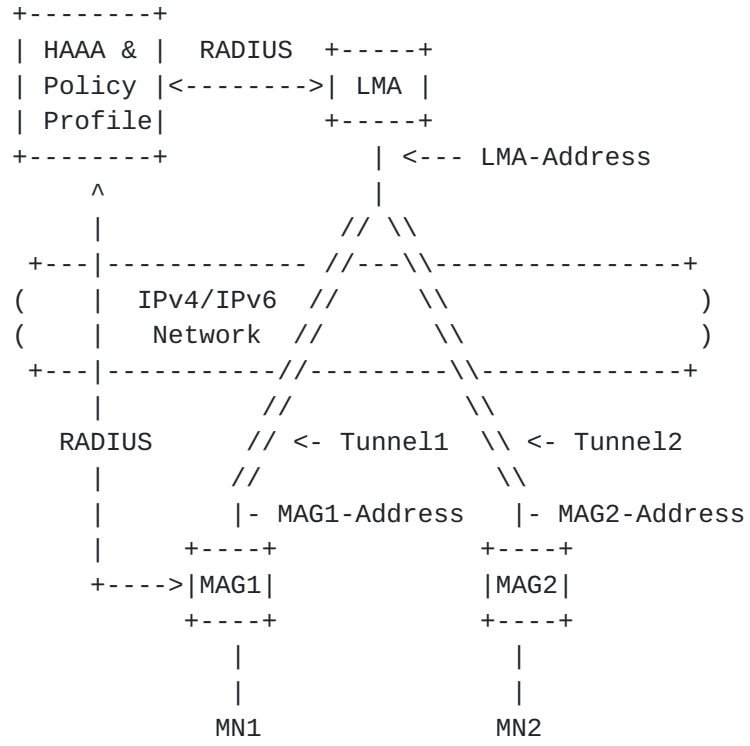


Figure 1: The MAG and LMA are both in the home network

Figure 2 shows both the LMA and MAG are in the visited network. The MAG and LMA exchange signaling with the HAAA through the VAAA which acts as a Proxy. The visited network may append additional information to the HAAA replies in order to reflect the local policy.

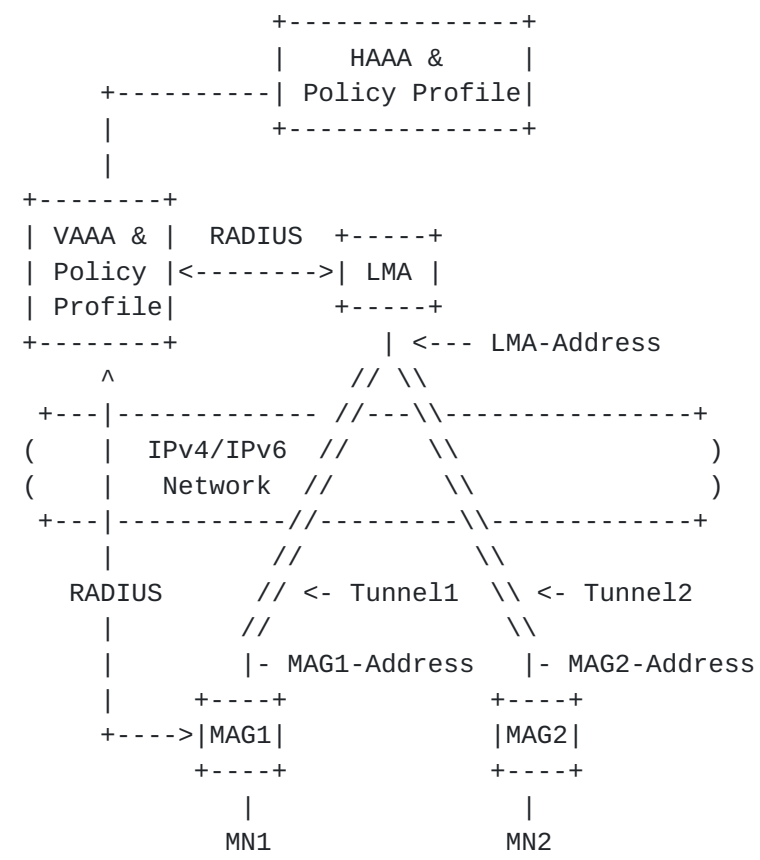


Figure 2: The MAG and LMA are both in the visited network

Figure 3 illustrates a topology where the MAG resides in the visited network while the associated LMA is in MN's home network. Any message between the MAG and the HAAA passes through the VAAA that acts as a Proxy. During the network authentication, the visited network's specific policy may also be propagated from the VAAA to the MAG. The LMA has a direct access to the HAAA.

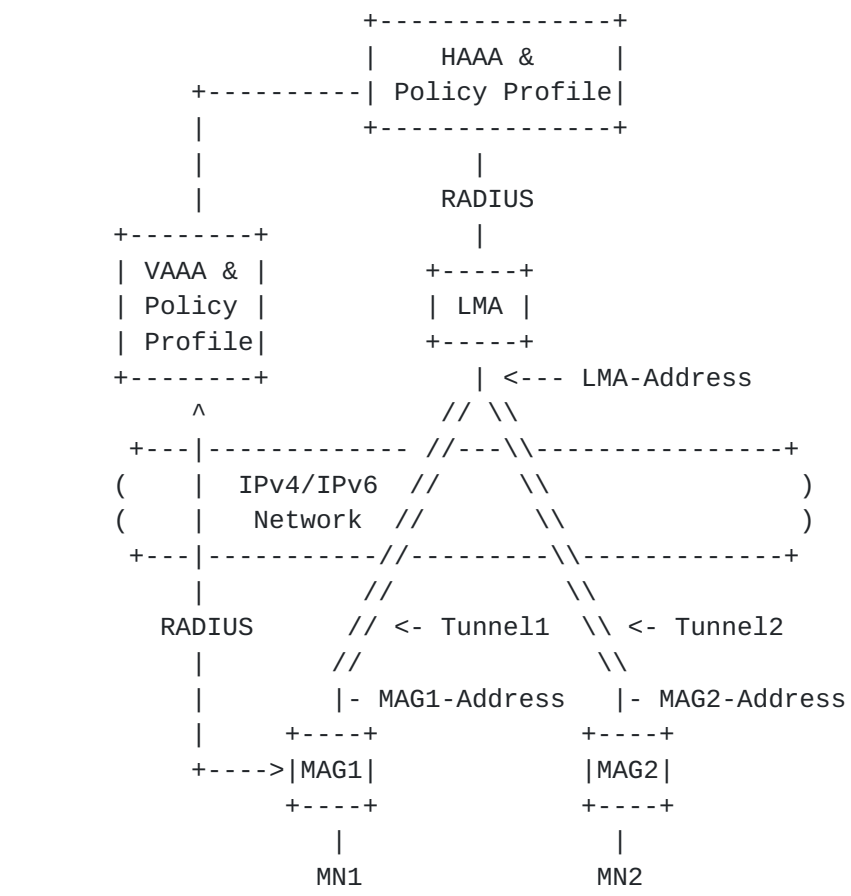


Figure 3: Visited MAG and home LMA topology

4. Attribute definitions

4.1. MIP6-Feature-Vector

Diameter [RFC3588] reserves AVP Code space 1-255 as RADIUS attribute compatibility space. The MIP6-Feature-Vector attribute (Type value 124) defined in [RFC5447] is of type OctetString and contains a 64 bit flags field of supported mobility capabilities. This document reserves two new capability bits according to the rules in [RFC5447], and reuses the PMIPv6 capability bits defined by [RFC5779]. The following capability flag bits are used or defined in this document:

PMIP6_SUPPORTED (0x0000010000000000)

This capability bit is used as defined in [RFC5779].

IP4_HOA_SUPPORTED (0x0000020000000000)

This capability bit is used as defined in [RFC5779]. Assignment of the IPv4-HoA is defined by [RFC5844].

LOCAL_MAG_ROUTING_SUPPORTED (0x0000040000000000)

This capability bit is used as defined in [RFC5779].

IP4_TRANSPORT_SUPPORTED (TBD17)

This capability bit is used for negotiation of the IPv4 transport support between the MAG and AAA. When the MAG sets this flag bit in the MIP6-Feature-Vector, it indicates ability of the MAG to provide IPv4 transport (i.e., IPv4-based encapsulation) for carrying IP traffic between the MAG and the LMA. If this flag bit is unset in the returned MIP6-Feature-Vector attribute, the AAA does not authorize the use of IPv4 transport on the MAG-to-LMA tunnel.

IP4_HOA_ONLY_SUPPORTED (TBD18)

This capability bit is used for determination of the authorized PMIPv6 mobility mode. When this bit is set by the AAA it indicates PMIPv6 mobility with IPv4 support has only been authorized for the MN. As a result, the RADIUS Access-Accept SHOULD NOT carry the IPv6 Home Network Prefix (IPv6 HNP). When this bit is set the PMIP6_SUPPORTED flag MUST also be set, and the

IP4_HOA_SUPPORTED flag MUST NOT be set.

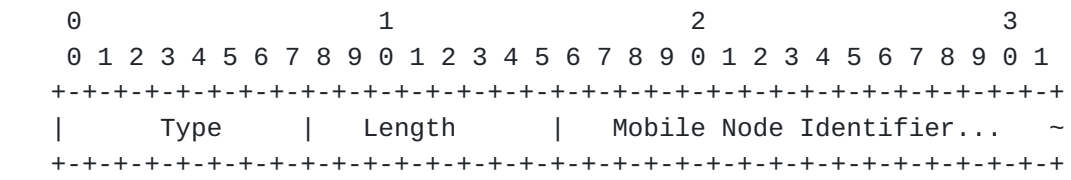
The MIP6-Feature-Vector attribute is also used on the LMA to the RADIUS AAA interface. This capability announcement attribute enables direct capability negotiation between the LMA and the AAA. The capabilities that are announced by both parties in the MIP6-Feature-Vector are known to be mutually supported. The LMA may use this mechanism during authorization of the received PBU against the AAA to check individual PMIPv6 feature permissions for a particular MN.

If the RADIUS Access-Accept contains contradicting combination of the capability flag bits such as both the PMIP6_SUPPORTED and the IP4_HOA_SUPPORTED flags are set, then the RADIUS client MUST treat the Access-Accept as an Access-Reject and SHOULD log the event. Similarly, if the RADIUS Access-Request contains contradicting combination of the capability flag bits, then the RADIUS server MUST reply with an Access-Reject message and SHOULD log the event.

4.2. Mobile-Node-Identifier

The Mobile-Node-Identifier attribute (Type value TBD1) is of type String and contains the mobile node identifier (MN-Identifier), see [RFC5213]), in a form of a Network Access Identifier (NAI) [RFC4282]. This identifier and the identifier used for access authentication may be different, however, there needs to be a mapping between the two identities as specified in Section 6.6 of [RFC5213]) This attribute is used on the interface between MAG and the AAA server. The Mobile-Node-Identifier attribute is designed for deployments where the identity used during Network Access Authentication and the identity used for mobility management is decoupled. It may also be the case where the MAG does not have means to find out the MN identity that could be used in subsequent PBU and Proxy Binding Acknowledgement (PBA) exchanges (e.g., due to identity hiding during the network access authentication) or when the HAAA wants to assign periodically changing identities to the MN.

The Mobile-Node-Identifier attribute MAY be returned by HAAA in the RADIUS Access-Accept message that completes a successful authentication and authorization exchange between the MAG and the HAAA. The MAG MUST use the received MN-Identifier.



Type:
Mobile-Node-Identifier TBD1.

Length:
In octets, including Type and Length fields (>= 3).

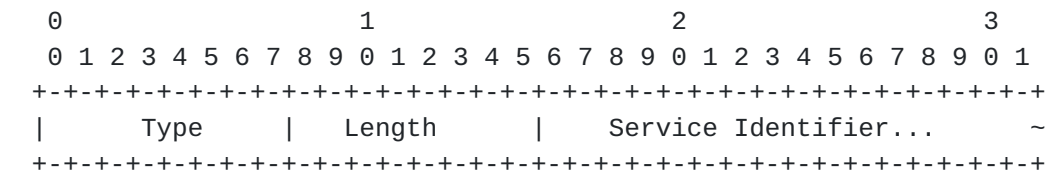
Mobile Node Identifier:
This field is of type String and contains the MN-Identifier of the MN to be used in the PBU/PBA exchange.

4.3. Service-Selection

The Service-Selection attribute (Type value TBD2) is of type UTF-8 text and contains the name of the service or the external network that the mobility service for the particular MN SHOULD be associated with [RFC5149]. The identifier MUST be unique within the PMIPv6 Domain when normalized using the selected normalization form [unicode] for the particular PMIPv6 Domain deployment. For instance, [RFC5149] uses the Normalization Form KC (NFKC).

The MAG MUST include the Service-Selection attribute in the Access-Request sent to the AAA if the information was acquired, e.g. by operator-specific configuration. The AAA MAY include the Service-Selection attribute in the Access-Accept response message to the MAG even if it was not included in the Access-Request as a means of indicating the MN's default service.

The service-selection mobility option defined in [RFC5149] can be used in PBU/PBA messages between the MAG and LMA. On the LMA-to-AAA interface, the LMA MAY populate the Service-Selection attribute in the Access-Request message using the service information found in the received PBU, if such mobility option was included. The Service-Selection identifier should be used to assist the PBU authorization, the assignment of the MN-HNP and the IPv4-MN-HoA as described in [RFC5149] and [RFC5779].



Type:
Service-Selection TBD2.

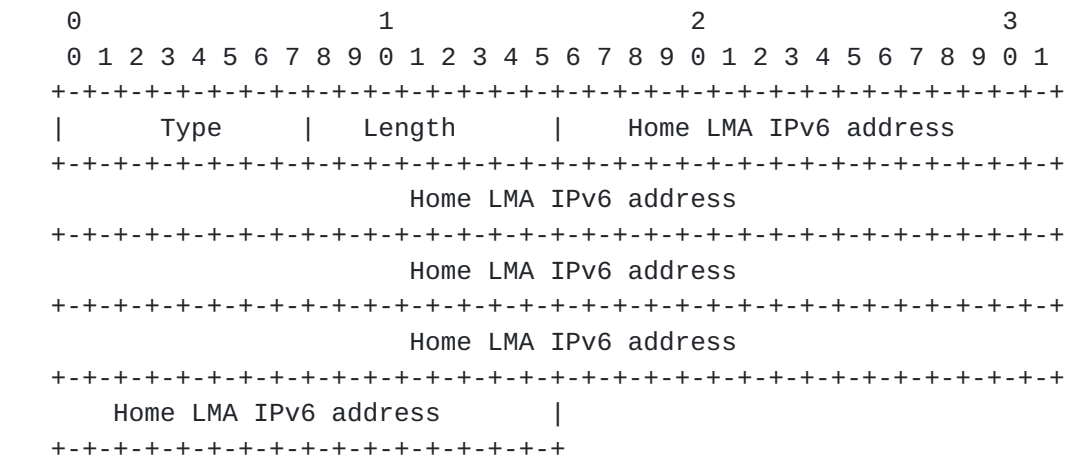
Length:
In octets, including Type and Length fields (>= 3).

Text:
This field is of type UTF-8 text and contains the Service Identifier the MN is associated with.

4.4. PMIP6-Home-LMA-IPv6-Address

The PMIP6-Home-LMA-IPv6-Address attribute (Type value TBD3) is of type IPv6 address and is used to deliver the IPv6 address of the LMA located in the Home network.
Before the MAG can initiate Proxy Mobile IPv6 signaling it must be aware of the LMA's IP address.

When the LMA is assigned to the MN from the home network, this attribute MAY be sent by the HAAA to the MAG in the RADIUS Access-Accept message.



Type:
PMIP6-Home-LMA-IPv6-Address TBD3.

Length:
= 18 octets

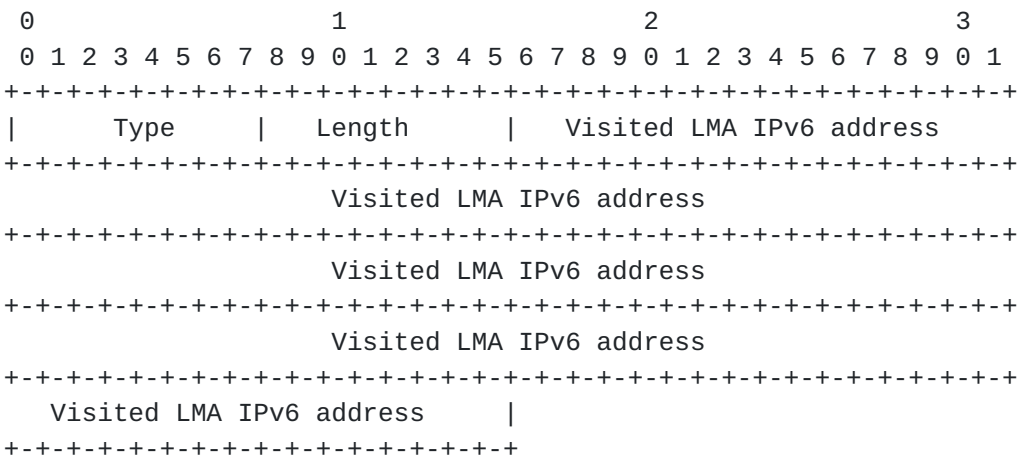
Home LMA IPv6 address:
128-bit IPv6 address of the assigned home LMA IPv6 address.

4.5. PMIP6-Visited-LMA-IPv6-Address

The PMIP6-Visited-LMA-IPv6-Address attribute (Type value TBD4) is of type IPv6 address and is used to propose a particular LMA in the Visited network, and to authorize the use of the LMA in the Visited network.

PMIP6-Visited-LMA-IPv6-Address attribute MAY be included by the MAG to the VAAA entity in the RADIUS Access-Request message. It enables the MAG to request an LMA in the visited network. The LMA in the visited network may be assigned by the visited AAA as the result of retrieved Policy Profile. If included by the VAAA in the RADIUS Access-Accept sent to the MAG, the use of the LMA in the visited network is authorized and the attribute SHALL carry the IPv6 address of the visited LMA assigned for the particular MN.

The attribute SHOULD NOT be included if the use of LMA in the Home Network is authorized (attribute PMIP6-Home-LMA-IPv6-Address is already present). However, if the VAAA local policy allows both home and visited LMA addresses to be delivered to the MAG, then the MAG has to select either visited or home network LMA based on its local policy.



Type:
PMIP6-Visited-LMA-IPv6-Address TBD4.

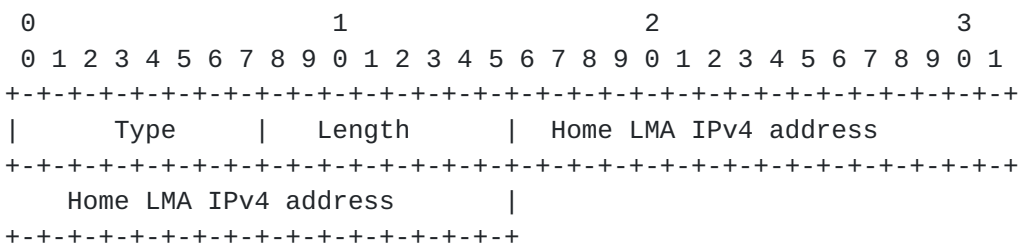
Length:
= 18 octets

Visited LMA IPv6 address:
128-bit IPv6 address of the assigned visited LMA IPv6 address.

4.6. PMIP6-Home-LMA-IPv4-Address

The PMIP6-Home-LMA-IPv4-Address attribute (Type value TBD5) is of type IPv4 address and contains the IPv4 address of the LMA assigned by the HAAA. The [RFC5844] supports Proxy Mobile IPv6 signaling exchange between MAG and LMA using the IPv4 transport.

When the LMA is located in the home network, this attribute MAY be sent by the HAAA to the MAG in the RADIUS Access-Accept message.



Type:
PMIP6-Home-LMA-IPv4-Address TBD5.

Length:
= 6 octets

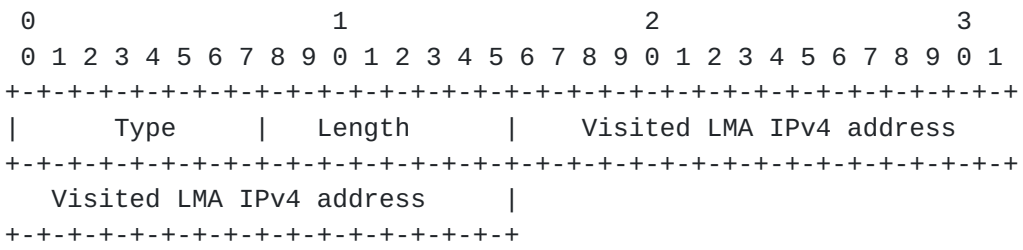
Home LMA IPv4 address:
32-bit IPv4 address of the assigned LMA.

4.7. PMIP6-Visited-LMA-IPv4-Address

The PMIP6-Visited-LMA-IPv4-Address attribute (Type value TBD6) is of type IPv4 address and is used to propose a particular LMA in the Visited network, and to authorize the use of the LMA in the Visited network.

PMIP6-Visited-LMA-IPv4-Address attribute MAY be included by the MAG to VAAA in the RADIUS Access-Request packet as a proposal to allocate the particular LMA to the MN. The LMA in the visited network may be assigned by the visited AAA as the result of retrieved Policy Profile. If included by VAAA in the RADIUS Access-Accept sent to the MAG, the use of the LMA in the visited network is authorized and the attribute SHALL carry the IPv4 address of the assigned visited LMA.

The attribute SHOULD NOT be included if the use of LMA in the Home Network is authorized (attribute PMIP6-Home-LMA-IPv4-Address is already present). However, if the VAAA local policy allows both home and visited LMA addresses to be delivered to the MAG, then the MAG has to select either visited or home network LMA based on its local policy.



Type:
PMIP6-Visited-LMA-IPv4-Address TBD6.

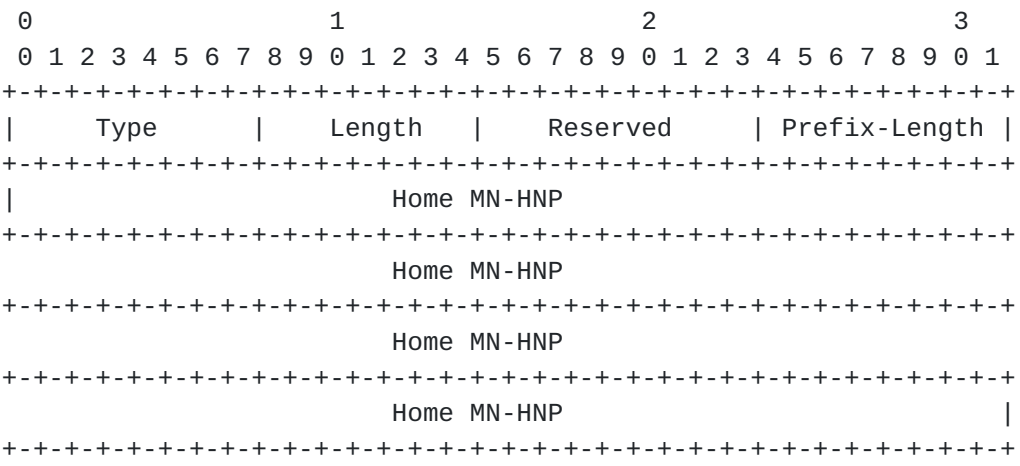
Length:
= 6 octets

IPv4 LMA address:
32-bit IPv4 address of the assigned LMA.

4.8. PMIP6-Home-HN-Prefix

The PMIP6-Home-HN-Prefix attribute (Type value TBD7) is of type IPv6 prefix. It contains Mobile Node's Home Network Prefix (MN-HNP) which is the IPv6 prefix assigned to the link between the MN and the MAG. The MN configures its IP interface from its home network prefix(es). When the LMA is located in the home network, PMIP6-Home-HN-Prefix attribute is used to deliver the MN-HNP from the HAAA to the MAG.

The PMIP6-Home-HN-Prefix attribute is also used on the LMA-to-HAAA interface containing the prefix assigned to the MN. If the LMA delegates the MN-HNP assignment to the HAAA, the attribute MUST contain all zeroes address (i.e., '::') in the Access-Request message. The attribute MUST be present in RADIUS Access-Accept message if the prior request already included one, and SHOULD carry the MN-HNP the HAAA assigned to the MN.



Type:
PMIP6-Home-HN-Prefix TBD7.

Length:
= at least 4 and no larger than 20.

Reserved:
Reserved for future use. The bits MUST be set to zero by the sender, and MUST be ignored by the receiver.

Prefix-Length:
The 8-bit unsigned integer indicating the prefix length of the Home Network Prefix (at least 0 and no larger than 128). If the Home Network Prefix contains all zeroes address (i.e., '::') then the Prefix-Length MUST be set to 128.

Home Network Prefix:
Home Network Prefix for the MN's IPv6 address configuration. The Prefix field is up to 16 octets in length. Bits outside of the Prefix-Length, if included, must be zero.

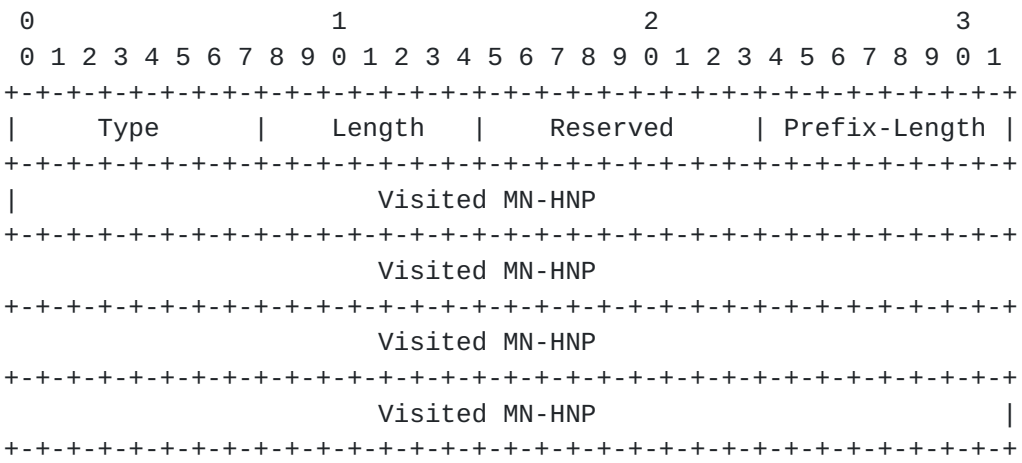
4.9. PMIP6-Visited-HN-Prefix

The PMIP6-Visited-HN-Prefix attribute (Type value TBD8) is of type IPv6 prefix. It contains Mobile Node's Home Network Prefix (MN-HNP) which is the IPv6 prefix assigned to the link between the MN and the MAG. The MN configures its IP interface from its home network prefix(es). When the LMA is located in the visited network, PMIP6-Visited-HN-Prefix attribute is used to deliver the MN-HNP from the VAAA to the MAG.

The PMIP6-Visited-HN-Prefix attribute is also used on the LMA to VAAA interface containing the IPv6 prefix assigned to the MN. If the LMA

delegates the assignment of the MN-HNP to the VAAA, the attribute MUST contain all zeroes address (i.e., '::') in the RADIUS Access-Request message. The attribute MUST be present in Access-Accept message if the prior request already included one, and SHOULD carry the MN-HNP the VAAA assigned to the MN.

The attribute SHOULD NOT be included if the use of LMA in the Home Network is authorized (attributes PMIP6-Home-HN-Prefix and/or PMIP6-Home-LMA-IPv6-Address are already present). However, if the VAAA local policy allows both home and visited LMA addresses to be delivered to the MAG, then this attribute MAY also be included.



Type:
PMIP6-Visited-HN-Prefix TBD8.

Length:
= at least 4 and no larger than 20.

Reserved:
Reserved for future use. The bits MUST be set to zero by the sender, and MUST be ignored by the receiver.

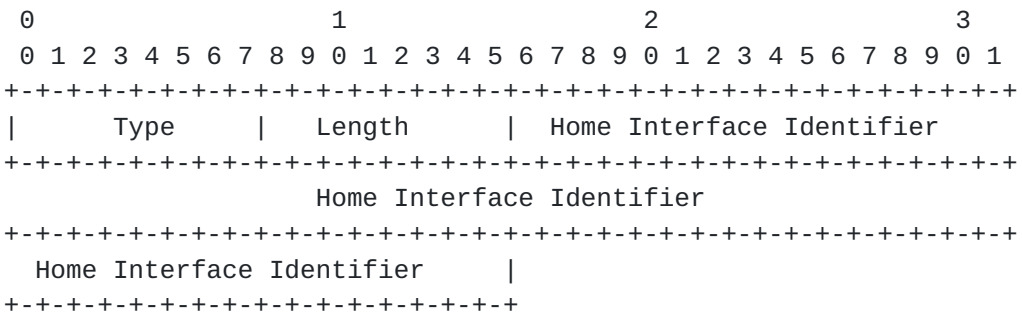
Prefix-Length:
The 8-bit unsigned integer indicating the prefix length of the Visited MN-HNP (at least 0 and no larger than 128). If the Visited Home Network Prefix contains all zeroes address (i.e., '::') then the Prefix-Length MUST be set to 128.

Visited Home Network Prefix:
Home Network Prefix for the MN's IPv6 address configuration. The Prefix field is up to 16 octets in length. Bits outside of the Prefix-Length, if included, must be zero.

4.10. PMIP6-Home-Interface-ID

The PMIP6-Home-Interface-ID attribute (Type value TBD9) is of type String and contains MN's interface identifier. The selection of the interface identifier SHOULD NOT allow tracking of individual MNs or users between PMIPv6 mobility session for privacy reasons. This attribute is applicable in network systems and link technologies, where the network explicitly delivers an interface identifier to the MN during the link setup. 3GPP and PPP link technologies are examples of such.

This attribute MAY be sent by the LMA or the MAG to the HAAA in the RADIUS Access-Request packet as a proposal. This attribute MAY be sent by HAAA to the LMA or to the MAG in an Access-Accept packet, however it MUST be present if the prior request already included one.



Type:
PMIP6-Home-Interface-ID TBD9.

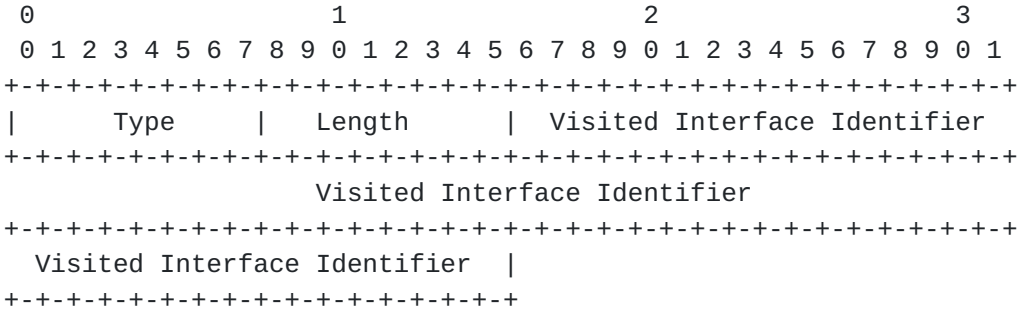
Length:
= 10 octets.

Home Interface Identifier:
The a 64 bit long interface identifier (8 octets).

4.11. PMIP6-Visited-Interface-ID

The PMIP6-Visited-Interface-ID attribute (Type value TBD10) is of type String and contains MN's interface identifier. The selection of the interface identifier SHOULD NOT allow tracking of individual MNs or users between PMIPv6 mobility session for privacy reasons. This attribute is applicable in network systems and link technologies, where the network explicitly delivers an interface identifier to the MN during the link setup. 3GPP and PPP link technologies are examples of such.

This attribute MAY be sent by the LMA or the MAG to the VAAA in the RADIUS Access-Request packet as a proposal. This attribute MAY be sent by VAAA to the LMA or to the MAG in an Access-Accept packet, however it MUST be present if the prior request already included one.



Type:
PMIP6-Visited-Interface-ID TBD10.

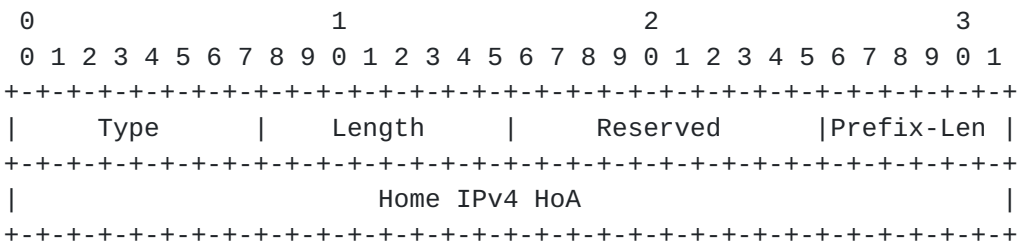
Length:
= 10 octets.

Visited Interface Identifier:
The a 64 bit long interface identifier (8 octets).

4.12. PMIP6-Home-IPv4-HoA

[RFC5844] specifies extensions to Proxy Mobile IPv6 protocol which enable IPv4 home address mobility support to the MN. The PMIP6-Home-IPv4-HoA attribute (Type value TBD11) is of type Address and contains the IPv4 Home Address of the MN. The primary use of this attribute is to deliver the assigned IPv4-HoA from HAAA to the MAG.

The PMIP6-Home-IPv4-HoA is also used on the LMA-to-HAAA interface. If the LMA in the home network delegates the assignment of the IPv4-HoA to the HAAA, the attribute MUST contain all zeroes address (i.e., 0.0.0.0) in the Access-Request message. The attribute MUST be included in by HAAA in the Access-Accept message if the previous request included it, and it contains the IPv4-HoA assigned to the MN.



Type:
PMIP6-Home-IPv4-HoA TBD11.

Length:
= 8 octets

Reserved
The 10-bit field reserved for future use. Value MUST be initialized to zero by sender, and MUST be ignored by the receiver.

Prefix-Len
The 6-bit unsigned integer indicating the prefix length of the IPv4 HoA. If the Home IPv4 HoA contains all zeroes address (i.e., '0.0.0.0') then the Prefix-Len MUST be set to 32.

Home IPv4 HoA:
This field is of type Address and contains the IPv4 home address of the MN in the home network.

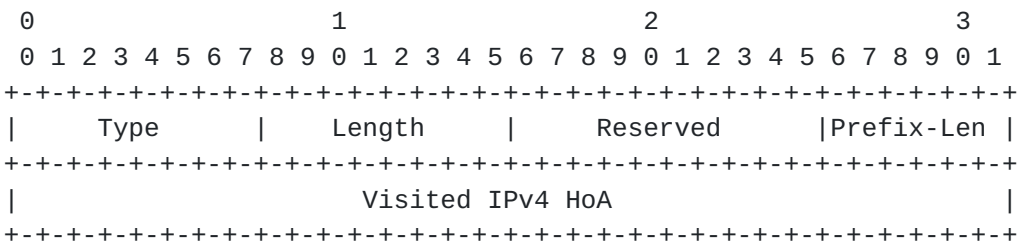
4.13. PMIP6-Visited-IPv4-HoA

When both MAG and the LMA are in the visited network, the PMIP6-Visited-IPv4-HoA attribute (Type value TBD12) is of type Address and is used to exchange information between the VAAA and the MAG on the assignment of the IPv4 Home Address to the MN being present in the Visited network.

The PMIP6-Visited-IPv4-HoA is also used on the LMA-to-VAAA interface. If the LMA delegates the assignment of the IPv4-HoA to the VAAA, the attribute MUST contain all zeroes address (i.e., 0.0.0.0) in the RADIUS Access-Request message. The Access-Accept message MUST have the attribute present if the prior request to the VAAA already included one.

The attribute SHOULD NOT be included if the use of LMA in the Home Network is authorized (attributes PMIP6-Home-IPv4-HoA and/or PMIP6-Home-LMA-IPv4-Address are already present). However, if the VAAA

local policy allows both home and visited LMA addresses to be delivered to the MAG, then this attribute MAY also be included.



Type:
PMIP6-Visited-IPv4-HoA TBD12.

Length:
= 8 octets

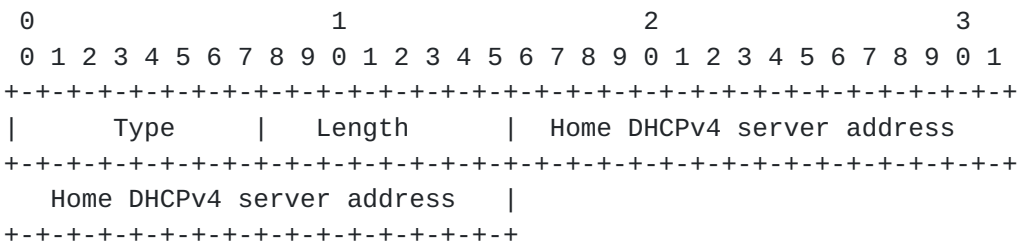
Reserved:
The 10-bit field reserved for future use. Value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Prefix-Len:
6-bit unsigned integer indicating the prefix length of the IPv4 HoA. If the Visited IPv4 HoA contains all zeroes address (i.e., '0.0.0.0') then the Prefix-Len MUST be set to 32.

Visited IPv4 HoA:
This field is of type Address and contains the IPv4 home address of the MN in the visited network.

4.14. PMIP6-Home-DHCP4-Server-Address

The PMIP6-Home-DHCP4-Server-Address (Type value TBD13) is of type Address and contains the IPv4 address of the DHCPv4 server in the home network. The particular DHCP server address is indicated to the MAG that serves the concerning MN. The HAAA MAY assign a DHCP server to the MAG in deployments where the MAG acts as a DHCP Relay, as defined in [RFC5844].



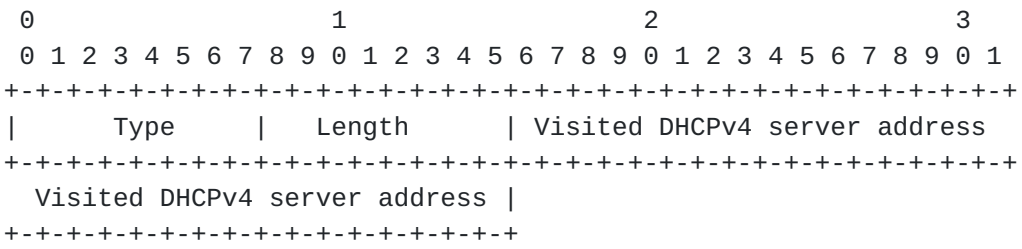
Type:
PMIP6-Home-DHCP4-Server-Address TBD13.

Length:
= 6 octets.

Home DHCPv4 server address:
This field is of type Address and contains a 4-octet IPv4 address of the DHCP server.

4.15. PMIP6-Visited-DHCP4-Server-Address

PMIP6-Visited-DHCP4-Server-Address attribute (Type value TBD14) of type Address and delivers the IPv4 address of the DHCPv4 server from the visited network to the MAG. When both MAG and the LMA are in the visited network, the VAAA MAY assign a DHCPv4 server to the MAG in deployments where the MAG acts as a DHCP Relay, as defined in [RFC5844].



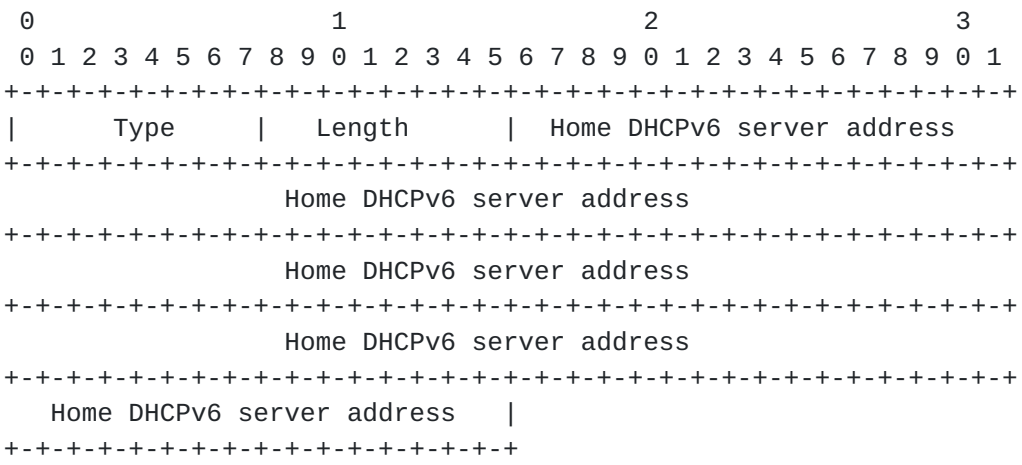
Type:
PMIP6-Visited-DHCP4-Server-Address TBD14.

Length:
= 6 octets

Visited DHCPv4 server address:
This field is of type Address and contains a 4-octet IPv4 address of the DHCPv4 server

4.16. PMIP6-Home-DHCP6-Server-Address

The PMIP6-Home-DHCP6-Server-Address (Type value TBD15) is of type IPv6 address and contains the IPv6 address of the DHCPv6 server in the home network indicated by the HAAA to the MAG that serves the MN. The HAAA MAY assign a DHCPv6 server to the MAG in deployments where the MAG acts as a DHCP Relay, as defined in [RFC5213].



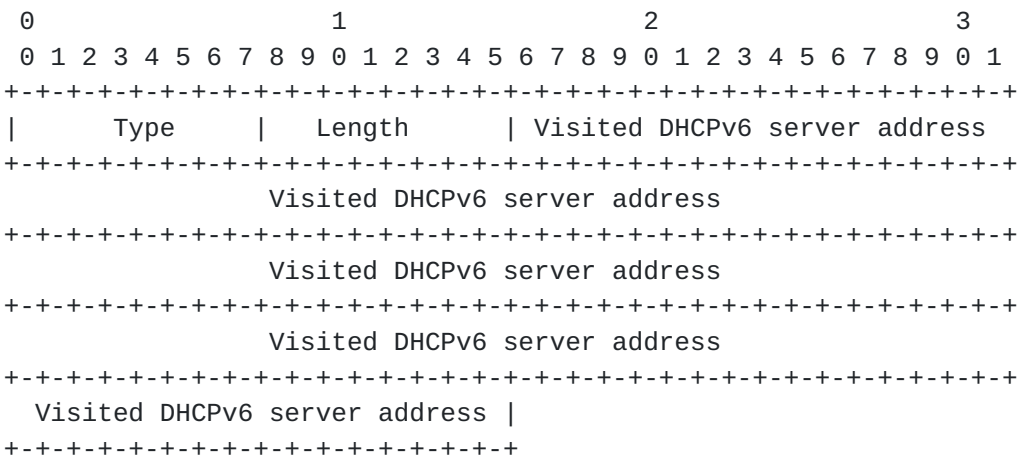
Type:
PMIP6-Home-DHCP6-Server-Address TBD15.

Length:
= 18 octets

Home DHCPv6 server address:
This field is of type Address and contains 16-octet IPv6 address of the DHCPv6 server.

4.17. PMIP6-Visited-DHCP6-Server-Address

The PMIP6-Visited-DHCP6-Server-Address attribute (Type value TBD16) is of type IPv6 address and contains the IPv6 address of the DHCPv6 server in the visited network indicated by the VAAA to the MAG that serves the MN. When both MAG and the LMA are located in the visited network, the VAAA MAY assign a DHCPv6 server to the MAG in deployments where the MAG acts as a DHCP Relay, as defined in [RFC5213].



Type:
PMIP6-Visited-DHCP6-Server-Address TBD16.

Length:
= 18 octets

Visited DHCPv6 server address:
This field is of type Address and contains the 16-octet IPv6 address of the DHCPv6 server.

4.18. Calling-Station-Id

The Calling-Station-Id attribute (Type value 31) is of type String [RFC2865]. When used within PMIPv6 deployments the attribute contains the link-layer identifier of the MN as defined in [RFC5213], Sections 2.2 and 8.6.

4.19. Chargeable-User-Identity

The Chargeable-User-Identity attribute or CUI (Type value 89) is an unique temporary handle used as means to, for example, correlate authentication, accounting and bill post-processing for a particular chargeable subscriber. The CUI format and use follows guidelines defined by [RFC4372].

In scope of this document, the CUI attribute MAY be present in the Access-Request. The CUI MAY also be present in the Access-Accept. The CUI Identity MUST be present in the Access-Accept if it was present in the Access-Request. If the use of the Chargeable User Identity is supported, then the MAG and/or the LMA commits to include the Chargeable User Identity in all subsequent RADIUS Accounting packets they send for the given user.

5. MAG to RADIUS AAA interface

5.1. Interface operations

The MAG to the AAA RADIUS server interface is used for retrieval of the Policy Profile when a MN tries to attach, authenticate and authorize to a PMIPv6 domain. Depending on the policies and network capabilities the MAG may retrieve different sets of PMIPv6-session related parameters:

- Configuration attributes for Home or Visited Network access scenario, depending on the location and attachment point of the MN,
- The IPv6 or IPv4 address of the designated LMA, depending on the access network's actual IP topology,
- The IPv6 or IPv4 configuration parameters for the MN, depending on the utilized IP configuration method and individual MN's service Policy,
- The DHCP Relay support attributes (IPv4 or IPv6) in case such functionality is supported in the network.

In addition to PMIPv6-specific attributes, other RADIUS attributes are to be used on the MAG-to-AAA interface.

The User-Name attribute MUST be present in the Access-Request. It MUST carry a correctly formed identifier that SHOULD correspond to a MN 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 RADIUS request messages towards the correct HAAA. The MN identity used on the MAG-to-HAAA interface and in the User-Name attribute MAY entirely be related to the network access authentication, and therefore not suitable to be used as the MN-Identifier mobility option value in the subsequent PBU/PBA messages. In this case the HAAA MUST provide the MN-Identifier for PBU/PBA messages using the Mobile-Node-Identifier attribute (see Section 4.2).

At least one of the NAS-IP-Address, NAS-IPv6-Address or NAS-Identifier attributes MUST be present in the Access-Request. The Service-Type attribute set to value 1 (Login) and the NAS-Port-Type attribute SHOULD be present in the Access-Request.

5.2. Table of Attributes

The following table provides a guide to attributes that may be found in authentication and authorization RADIUS messages between MAG and the AAA Server.

Request	Accept	Reject	Challenge	#	Attribute
1	0-1	0	0	1	User-Name
0-1	0	0	0	4	NAS-IP-Address
0-1	0-1	0	0	5	NAS-Port
0-1	0-1	0	0	6	Service-Type
0-1	0-1	0	0-1	24	State
0	0-1	0	0	25	Class
0	0-1	0	0-1	27	Session-Timeout
0-1	0	0	0	31	Calling-Station-Id
0-1	0	0	0	32	NAS-Identifier
0+	0+	0+	0+	33	Proxy-State
0-1	0	0	0	69	NAS-Port-Type
0+	0+	0+	0+	79	EAP-Message
1	1	1	1	80	Message-Authenticator
0-1	0-1	0	0	89	Chargeable-User-Identity
0-1	0	0	0	95	NAS-IPv6-Address
0-1	0-1	0	0	124	MIP6-Feature-Vector
0	1	0	0	TBD1	Mobile-Node-Identifier
0-1	0-1	0	0	TBD2	Service-Selection
0	0-1	0	0	TBD3	PMIP6-Home-LMA-IPv6-Address
0-1	0-1	0	0	TBD4	PMIP6-Visited-LMA-IPv6-Address
0	0-1	0	0	TBD5	PMIP6-Home-LMA-IPv4-Address
0-1	0-1	0	0	TBD6	PMIP6-Visited-LMA-IPv4-Address
0	0+	0	0	TBD7	PMIP6-Home-HN-Prefix
0	0+	0	0	TBD8	PMIP6-Visited-HN-Prefix
0	0-1	0	0	TBD9	PMIP6-Home-Interface-ID
0	0-1	0	0	TBD10	PMIP6-Visited-Interface-ID
0	0-1	0	0	TBD11	PMIP6-Home-IPv4-HoA
0	0-1	0	0	TBD12	PMIP6-Visited-IPv4-HoA
0	0-1	0	0	TBD13	PMIP6-Home-DHCP4-Server-Address
0	0-1	0	0	TBD14	PMIP6-Visited-DHCP4-Server-Address
0	0-1	0	0	TBD15	PMIP6-Home-DHCP6-Server-Address
0	0-1	0	0	TBD16	PMIP6-Visited-DHCP6-Server-Address

6. LMA to RADIUS AAA interface

6.1. Interface operations

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.

Whenever the LMA sends a Access-Request message to the HAAA, the User-Name attribute SHOULD contain the MN's identity. The LMA-provided identity in the User-Name attribute is strongly RECOMMENDED to be the same as the MN's identity information in the PBU MN-Identifier 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 attribute 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 attribute 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 Service-Type attribute MUST be set to the value 17 (Authorize Only). If the HAAA is not able to authorize the subscriber's mobility service session, then the Access-Reject message to the LMA MAY contain the Reply-Message attribute describing the reason for rejecting the authorization. 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).

In case of a dynamic LMA discovery and assignment [RFC6097], 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 PMIP6-*-LMA-*-Address attribute 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.

The LMA and the HAAA use the PMIP6-Home-HN-Prefix/ PMIP6-Visited-HN-Prefix attributes to exchange the MN-HNP when appropriate. Similarly, the LMA and the HAAA use the PMIP6-Home-IPv4-HoA/PMIP6-Visited-IPv4-HoA attributes to exchange the IPv4-MN-HoA when appropriate. 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 PMIP6-*-HN-Prefix/PMIP6-*-IPv4-HoA attributes are 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 in the Access-Request message sent from the LMA to the HAAA. The LMA expects to receive the HAAA assigned HNP/IPv4-MN-HoA in the corresponding Access-Accept message.

6.2. Table of Attributes

The following table provides a guide to which attributes may be found in authorization process between LMA and the AAA.

Request	Accept	Reject	Challenge	#	Attribute
1	0-1	0	0	1	User-Name
0-1	0-1	0	0	4	NAS-IP-Address
0-1	0-1	0	0	5	NAS-Port
1	0-1	0	0	6	Service-Type
0	0-1	0	0	25	Class
0	0-1	0	0-1	27	Session-Timeout
0-1	0	0	0	31	Calling-Station-Id
1	0	0	0	32	NAS-Identifier
0+	0+	0+	0+	33	Proxy-State
1	0	0	0	69	NAS-Port-Type
1	1	1	1	80	Message-Authenticator
0-1	0-1	0	0	89	Chargeable-User-Identity
0-1	0-1	0	0	95	NAS-IPv6-Address
0-1	0-1	0	0	124	MIP6-Feature-Vector
1	0	0	0	TBD1	Mobile-Node-Identifier
0-1	0-1	0	0	TBD2	Service-Selection
0-1	0	0	0	TBD3	PMIP6-Home-LMA-IPv6-Address
0-1	0	0	0	TBD4	PMIP6-Visited-LMA-IPv6-Address
0-1	0	0	0	TBD5	PMIP6-Home-LMA-IPv4-Address
0-1	0	0	0	TBD6	PMIP6-Visited-LMA-IPv4-Address
0+	0+	0	0	TBD7	PMIP6-Home-HN-Prefix
0+	0+	0	0	TBD8	PMIP6-Visited-HN-Prefix
0-1	0-1	0	0	TBD9	PMIP6-Home-Interface-ID
0-1	0-1	0	0	TBD10	PMIP6-Visited-Interface-ID
0-1	0-1	0	0	TBD11	PMIP6-Home-IPv4-HoA
0-1	0-1	0	0	TBD12	PMIP6-Visited-IPv4-HoA

7. Accounting

Radius based interfaces at the MAG and LMA with the AAA server enables metering of traffic associated with the MN, commonly called accounting. If accounting is turned on in the mobile node's Policy Profile, the local routing SHOULD NOT be enabled [RFC5213].

7.1. Accounting at LMA

The accounting at the LMA to AAA server interface is based on [RFC2865] and [RFC2866]. This interface MUST support the transfer of accounting records needed for service control and charging. These records should include (but may not be limited to): time of binding cache entry creation and deletion, number of the octets sent and received by the MN over the bi-directional tunnel, etc.

7.2. Accounting at MAG

The accounting at the MAG to AAA server interface is based on [RFC2865] and [RFC2866]. The interface MUST also support the transfer of accounting records which should include: time of binding cache entry creation and deletion, number of the octets sent and received by the MN over the bi-directional tunnel, etc.

If there is data traffic between a visiting MN and a correspondent node that is locally attached to an access link connected to the same MAG, the mobile access gateway MAY optimize on the delivery efforts by locally routing the packets instead of using reverse tunneling to the mobile node's LMA. In this case, the local data traffic too MUST be reported to AAA Accounting servers by means of RADIUS protocol.

7.3. Table of Attributes

The following table provides a list of attributes that may be included in the RADIUS Accounting messages. These attributes are to complement the set of accounting attributes already required by [RFC2866] and [RFC2869].

Request	Interim	Stop	#	Attribute
0-1	0-1	0-1	TBD1	Mobile-Node-Identifier
0-1	0	0-1	TBD2	Service-Selection
0-1	0	0-1	TBD3	PMIP6-Home-LMA-IPv6-Address
0-1	0	0-1	TBD4	PMIP6-Visited-LMA-IPv6-Address
0-1	0	0-1	TBD5	PMIP6-Home-LMA-IPv4-Address
0-1	0	0-1	TBD6	PMIP6-Visited-LMA-IPv4-Address
0+	0	0+	TBD7	PMIP6-Home-HN-Prefix
0+	0	0+	TBD8	PMIP6-Visited-HN-Prefix
0-1	0	0-1	TBD11	PMIP6-Home-IPv4-HoA
0-1	0	0-1	TBD12	PMIP6-Visited-IPv4-HoA
0-1	0	0-1	31	Calling-Station-Id
0-1	0-1	0-1	80	Message-Authenticator
0-1	0-1	0-1	89	Chargeable-User-Identity
0-1	0	0-1	124	MIP6-Feature-Vector

8. Security Considerations

The RADIUS messages may be transported between the MAG and/or the LMA to the RADIUS server via one or more AAA brokers or RADIUS proxies. In this case the LMA to the RADIUS AAA server communication relies on the security properties of the intermediate AAA brokers and RADIUS proxies.

Regarding the privacy threats associated with sending MN specific information between the MAG and AAA server and between the LMA and AAA server, considerations of the Radius Base protocol [RFC2865], [RFC2866], and the Radius EAP application [RFC3579] are applicable to this document. The MAG, LMA and AAA server SHOULD avoid including attributes containing personally identifying information such as an MN's Interface ID, link-layer address or NAI, except as needed, and SHOULD pay special attention if identity hiding is desired.

9. IANA consideration

9.1. Attribute Type Codes

This specification defines the following new RADIUS attribute type values:

Mobile-Node-Identifier	<TBD1>
Service-Selection	<TBD2>
PMIP6-Home-LMA-IPv6-Address	<TBD3>
PMIP6-Visited-LMA-IPv6-Address	<TBD4>
PMIP6-Home-LMA-IPv4-Address	<TBD5>
PMIP6-Visited-LMA-IPv4-Address	<TBD6>
PMIP6-Home-HN-Prefix	<TBD7>
PMIP6-Visited-HN-Prefix	<TBD8>
PMIP6-Home-Interface-ID	<TBD9>
PMIP6-Visited-Interface-ID	<TBD10>
PMIP6-Home-IPv4-HoA	<TBD11>
PMIP6-Visited-IPv4-HoA	<TBD12>
PMIP6-Home-DHCP4-Server-Address	<TBD13>
PMIP6-Visited-DHCP4-Server-Address	<TBD14>
PMIP6-Home-DHCP6-Server-Address	<TBD15>
PMIP6-Visited-DHCP6-Server-Address	<TBD16>

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
IP4_TRANSPORT_SUPPORTED	<TBD17>
IP4_HOA_ONLY_SUPPORTED	<TBD18>

10. Acknowledgements

First of all, the authors would like to acknowledge the standardization work and people of the WiMAX Forum that have set the foundation for this document.

The authors would like to thank Basavaraj Patil, Glen Zorn, Avi Lior, Alan DeKok and Pete McCann for reviewing the document and providing valuable input. The authors also thank Elwyn Davies, Pete Resnick, Bernard Aboba, Jari Arkko and Stephen Farrell for their reviews on the document during the IESG process.

The authors would also like to thank the authors of [RFC5779] as this document re-uses some procedural ideas of the aforementioned specification.

11. References

11.1. Normative References

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

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

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

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

[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.

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

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

[RFC5779] Korhonen, J., Bournelle, J., Chowdhury, K., Muhanna, A., and U. Meyer, "Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server", RFC 5779, February 2010.

[RFC4372] Adrangi, F., Lior, A., Korhonen, J., and J. Loughney, "Chargeable User Identity", RFC 4372, January 2006.

11.2. Informative references

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC2869] Rigney, C., Willats, W., and P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H.

Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

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

[RFC6097] Korhonen, J. and V. Devarapalli, "Local Mobility Anchor (LMA) Discovery for Proxy Mobile IPv6", RFC 6097, February 2011.

[unicode] Davis, M. and M. Duerst, "Unicode Standard Annex #15; Unicode Normalization Forms", Unicode 5.0.0, October 2006.

Authors' Addresses

Frank Xia
Huawei USA
1700 Alma Dr. Suite 500
Plano, TX 75075

Phone: +1 972-509-5599
Email: xiayangsong@huawei.com

Behcet Sarikaya
Huawei USA
1700 Alma Dr. Suite 500
Plano, TX 75075

Phone: +1 972-509-5599
Email: sarikaya@ieee.org

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

Email: jouni.nospam@gmail.com

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134

Email: sgundave@cisco.com

Damjan Damic
Siemens
Heinzelova 70a
Zagreb 10000
Croatia

Email: damjan.damic@siemens.com