Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 21, 2008

A. Lior
Bridgewater Systems
K. Chowdhury
Starent Networks
H. Tschofenig
Siemens

November 18, 2007

RADIUS Mobile IPv6 Support
draft-ietf-mip6-radius-03.txt

Status of this Memo

Copyright Notice

Abstract

A Mobile IPv6 node requires a home agent(HA) address, a home address(HOA), and IPsec security association with its HA before it can start utilizing Mobile IPv6 service. RFC 3775 requires that some or all of these parameters are statically configured. Ongoing work aims to make this information dynamically available to the mobile node. An important aspect of the Mobile IPv6 bootstrapping solution is to support interworking with existing authentication, authorization and accounting (AAA) infrastructure. This document defines new attributes to facilitate Mobile IPv6 bootstrapping via a RADIUS infrastructure. This information exchange may take place as part of the initial network access authentication procedure or as part of a separate protocol exchange between the mobile node, the HA and the AAA infrastructure.

Table of Contents

1. Introduction

Mobile IPv6 specification [6] requires a Mobile Node (MN) to perform registration with an HA with information about its current point of attachment (Care-of Address). The HA creates and maintains binding between the MN's HOA and the MN's Care-of Address.

In order to register with a HA, the MN needs to know some information such as, the Home Link prefix, the HA Address, the HOA, the Home Link prefix Length and security related information in order to secure the Binding Update.

The aforementioned set of information may be statically provisioned in the MN. However, static provisioning of this information has its drawbacks. It increases provisioning and network maintenance burden for the operator. Moreover, static provisioning does not allow load balancing, failover, opportunistic home link assignment etc. For example, the user may be accessing the network from a location that may be geographically far away from the preconfigured home link; the administrative burden to configure the MN's with the respective addresses is large and the ability to react on environmental changes is minimal. In these situations static provisioning may not be desirable.

Dynamic assignment of Mobile IPv6 home registration information is a desirable feature for ease of deployment and network maintenance. For this purpose, the RADIUS infrastructure, which is used for access authentication, can be leveraged to assign some or all of the necessary parameters. The RADIUS server in the Access Service

Provider (ASP) or in the Mobility Service Provider's (MSP) network may return these parameters to the AAA client. The AAA client might either be the NAS, in case of the integrated scenario, or the HA, in case of the split scenario. The terms integrated and split are described in the terminology section and were introduced in [7].

2. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [1].

General mobility terminology can be found in [8]. The following additional terms, as defined in [7], are used in this document:

Access Service Authorizer (ASA):

> A network operator that authenticates a mobile node and establishes the mobile node's authorization to receive Internet service.

Access Service Provider (ASP):

> A network operator that provides direct IP packet forwarding to and from the end host.

Mobility Service Authorizer (MSA):

A service provider that authorizes Mobile IPv6 service.

Mobility Service Provider (MSP):

A service provider that provides Mobile IPv6 service. In order to obtain such service, the MN must be authenticated and authorized to obtain the Mobile IPv6 service.

Split Scenario:

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

Integrated Scenario:

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

3. Solution Overview

This document addresses the authentication, authorization and accounting functionality required by MIPv6 bootstrapping as outlined in the MIPv6 bootstrapping problem statement document (see [7]). As such, the AAA functionality for the integrated and the split scenario needs to be defined. This requires the ability to offer support for the HA to AAA server and the network access server(NAS) to AAA server communication.

To highlight the main use cases, we briefly describe the integrated and the split scenarios in Section 3.1 and Section 3.2, respectively.

3.1. Integrated Scenario

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

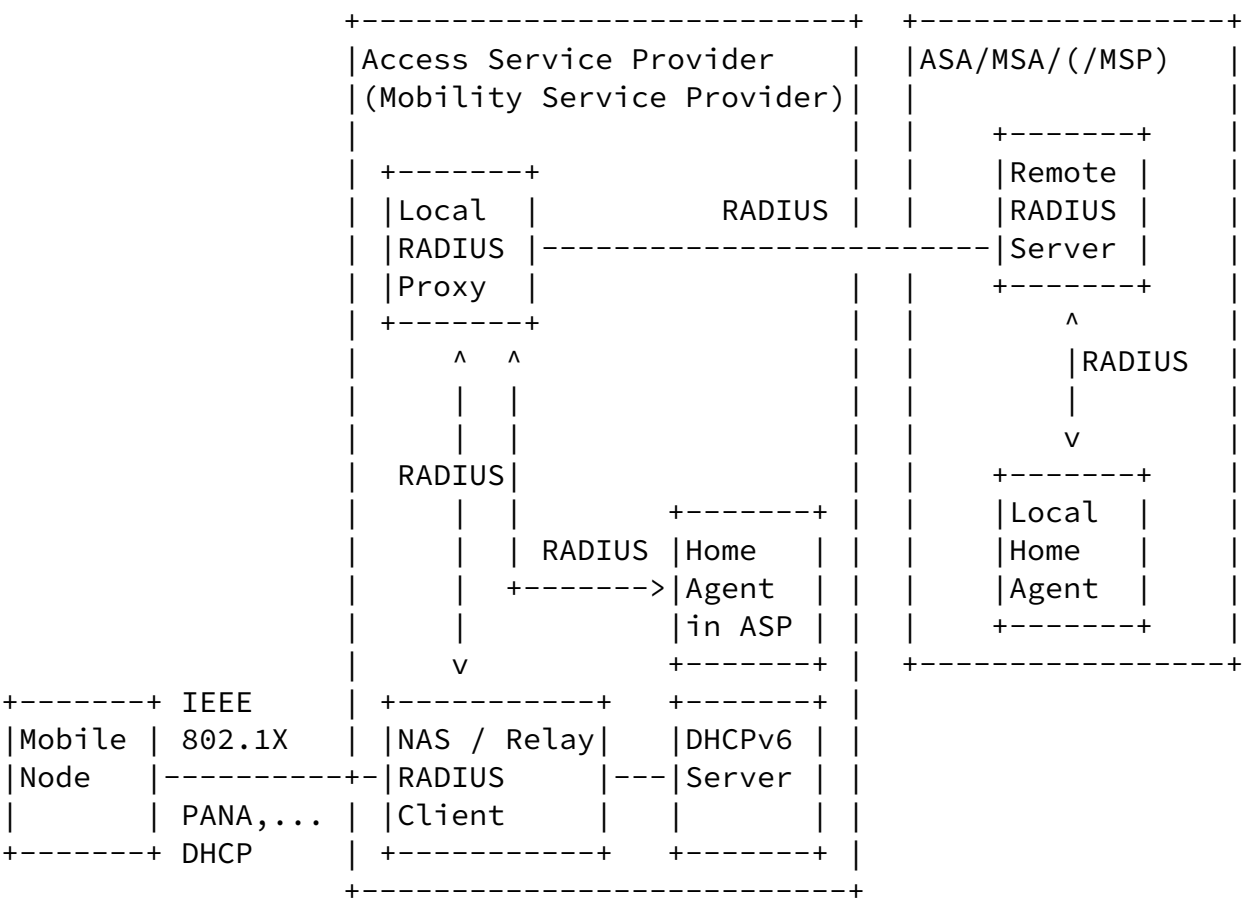


Figure 1: Mobile IPv6 Service Access in the Integrated Scenario

In the typical Mobile IPv6 access scenario as shown above, the MN attaches in the ASP's network. During this network attachment

procedure, the NAS/RADIUS client interacts with the MN. As shown in Figure 1, the authentication and authorization happens via a RADIUS infrastructure.

At the time of authorizing the user for IPv6 access, the RADIUS server in the MSA detects that the user is authorized for Mobile IPv6 access. Based on the MSA's policy, the RADIUS server may allocate several parameters to the MN for use during the subsequent Mobile

IPv6 protocol interaction with the HA.

Depending on the details of the solution interaction with the DHCPv6 server may be required, as described in [2].

3.2. Split Scenario

In the split scenario, Mobile IPv6 bootstrapping is not provided as part of the network access authentication procedure. The Mobile IPv6 bootstrapping procedure is executed with the Mobility Service Provider when desired by the MN. Two variations can be considered:

1. the MSA and the MSP are the same entity.

2. the MSA and the MSP are different entities.

Since scenario (2) is the more generic scenario we show it in Figure 2.

+----------------------+

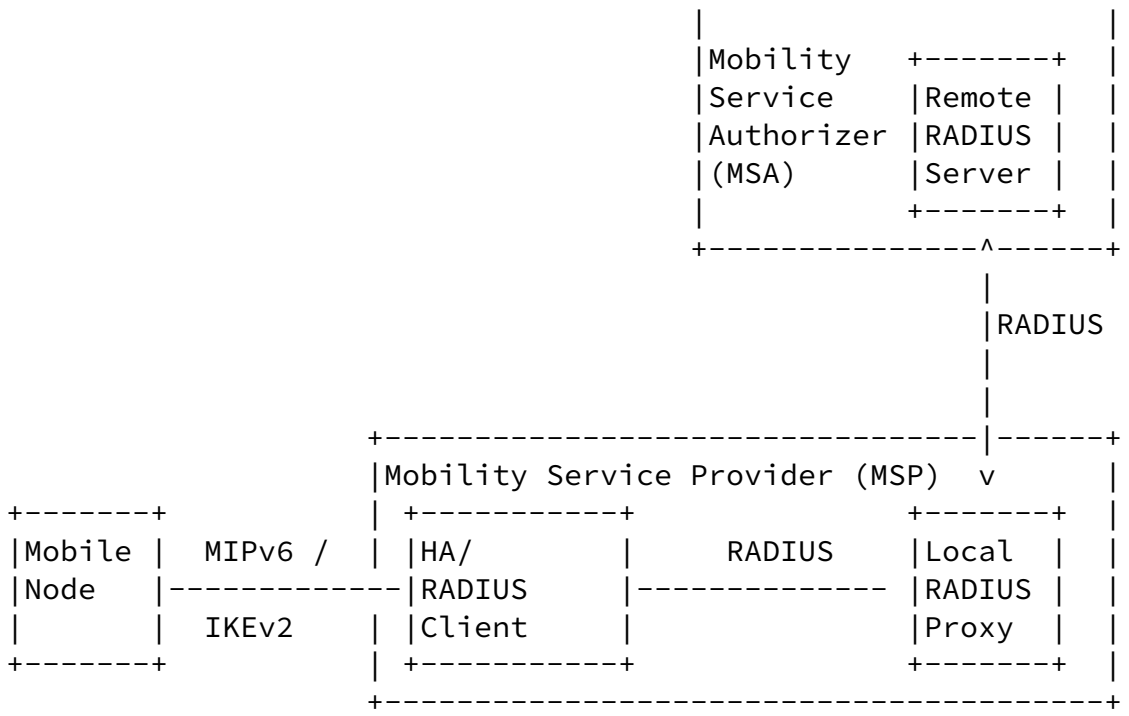


Figure 2: Mobile IPv6 service access in the split scenario (MSA != MSP)

As shown in Figure 2 the interaction between the RADIUS client and the RADIUS server is triggered by the protocol interaction between the MN and the HA/RADIUS client using IKEv2 (see [3] and [9]). The HA / RADIUS Client interacts with the RADIUS infrastructure to perform authentication, authorization, accounting and parameter bootstrapping. The exchange is triggered by the HA and an interaction with the RADIUS infrastructure is initiated. When the protocol exchange is completed then the HA needs to possess the Mobile IPv6 specific parameters (see [7]).

Additionally, the MN might instruct the RADIUS server (via the HA) to perform a dynamic DNS update.

4. RADIUS Attribute Overview

4.1. MIP6-Feature-Vector

The MIP6-Feature-Vector when included in an Access-Request packet is used by the NAS to indicate supported MIP6 features. For example, the NAS uses this attribute to indicate whether it can provide a local home agent.

When included in an Access-Accept packet, the MIP6-Feature-Vector is used by the RADIUS Server to indicate supported MIP6 features and to select advetized feature by the NAS. For example, if the NAS indicated support for local home agent assignment, the RADIUS server authorizes the NAS to support local home agent assignment by echoing the setting the same flag in the Access-Accept packet.

4.2. MIP6-HA Attribute

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

4.3. MIP6-HA-FQDN Attribute

The RADIUS server may assign an FQDN of the HA to the MN. The mobile node can perform DNS query with the FQDN to derive the HA address.

4.4. MIP6-HL-Prefix Attribute

For the same reason as the HA assignment, the RADIUS server may assign a Home Link that is in close proximity to the point of attachment (NAS-ID). The MN can perform [6] specific procedures to discover other information for Mobile IPv6 registration.

4.5. MIP6-HOA Attribute

The RADIUS server may assign a HOA to the MN. This allows the network operator to support mobile devices that are not configured with static addresses. The attribute also contains the prefix length so that the MN can easily infer the Home Link prefix from the HA address.

4.6. MIP6-DNS-MO Attribute

By using this payload the RADIUS client instructs the RADIUS server to perform a dynamic DNS update. When this payload is included in the reverse direction, i.e., from the RADIUS server to the RADIUS client, it informs about the status of the dynamic DNS update. When the payload is sent from the RADIUS client to the RADIUS server then the response MUST include the MIP6-DNS-MO attribute.

4.7. Use of existing RADIUS Attributes

4.7.1. User-Name

If authentication via IKEv2 is used then the User-Name attribute SHALL be set to the IDi payload received in the IKE_AUTH exchange.

4.7.2. Service-Type

If the HA uses Service-Type(6) is SHALL set its value to "Framed"(2).

4.7.3. NAS-Port-Type

In order for the AAA to distingiues the source of the Access-Request NAS-Port-Type(61) is used as follows:

In the split scenario when the Access-Request originates from an MIP6 HA, NAS-Port-Type MUST be included and its value set to HA6(IANA-TBD1).

4.7.4. Calling-Station-Id

In the split-scenario, the HA SHOULD use the Calling-Station-Id(31) to send the MN's COA to the AAA. If used, the string value of the Calling-Station-Id(31) should be set to the 128-bit MN IPv6 COA.

4.7.5. Use of MS-MPPE-Recv-Key and MS-MPPE-Send-Key

To transport the MSK from the RADIUS to the HA, RADIUS SHALL utilize the MS-MPPE-Recv-Key and the MS-MPPE-Send-Key as defined in [4]. The

first up to 32 octets of the MSK is stored into the MS-MPPE-Recv-Key, and the next up to 32 octets are stored into the MS-MPPE-Send-Key. The encryption of these attributes is described in [4].

5. RADIUS attributes

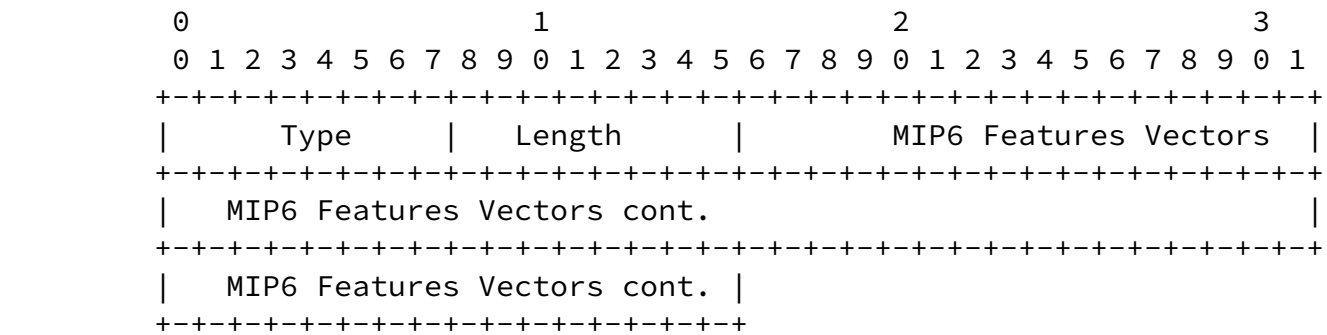
This section defines format and syntax for the attribute that carries the Mobile IPv6 parameters that are described in the previous section.

The attributes MAY be present in Access-Request, Access-Accept, and Accounting-Request packets.

5.1. MIP6-Feature-Vector Attribute

Exactly one of this attribute MUST be sent by the NAS in an Access-Request packet to inidcate support for MIP6.

Exactly one of this attribute MUST be sent by the RADIUS server in an Access-Accept packet to indicate support for MIP6 and to select features advetized by the NAS.



Type:

MIP6-FV-TYPE to be defined by IANA.

Length:

= 10 octets

Feature Flags:

This field is of type String. Supporting the following values:

MIP6_INTEGRATED (0x0000000000000001)

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

LOCAL_HOME_AGENT_ASSIGNMENT (0x0000000000000002)

When this flag is set by the NAS then a local home agent can be assigned to the MN. When this flag is set by the Diameter server then the assignment of location HAs is authorized by the Diameter server.

5.2. MIP6-HA Attribute

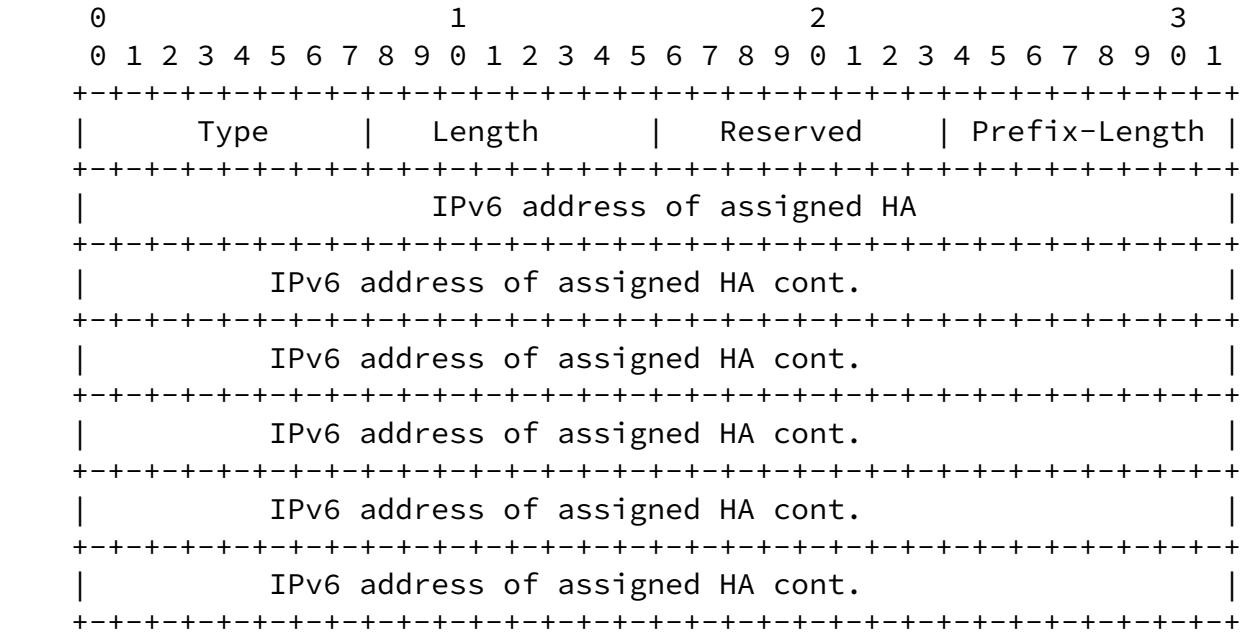
One or more of this attribute MAY be sent by the NAS to the RADIUS server in an Access-Request packet as a proposal by the NAS to allocate a local HA to the MN.

One or more of this attribute MAY be sent by the RADIUS server to the NAS in an Access-Accept packet. The attribute carries the HA address that may be assigned to the MN.

[EDITOR: WHAT IS THIS ABOUT?] This attribute MAY be MIP6-DNS-MO Attribute sent by the NAS to the RADIUS server in an Access-Request packet as a hint to suggest a dynamic HA that may be assigned to the MN. The RADIUS server MAY use this value or may ignore this suggestion.

If available at the NAS, at least MIP6-HA attribute and/or MIP6-HA-FQDN SHOULD appear in accounting packets to indicate the identity of

the serving HA for this session.



Type:

MIP6-HA-TYPE to be defined by IANA.

Length:

= 21 octets

Reserved:

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

Prefix-Length:

This field indicates the prefix length of the Home Link.

IPv6 address of assigned HA:

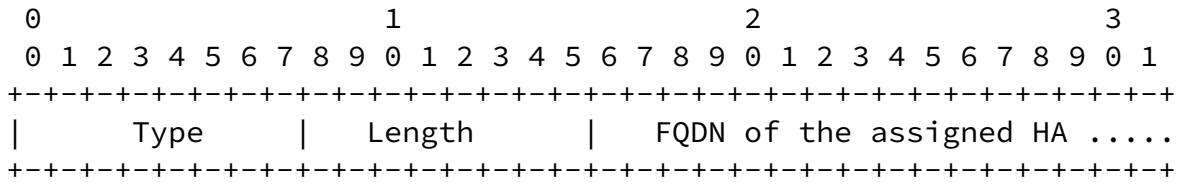
128-bit IPv6 address of the assigned HA.

5.3. MIP6-HA-FQDN Attribute

One or more instance of this attribute MAY be sent by the NAS to the RADIUS server in an Access-Request packet as a hint to suggest a dynamic HA that may be assigned to the MN. The RADIUS server MAY use this value or may ignore this suggestion.

One or more of this attribute is sent by the RADIUS server to the NAS in an Access-Accept packet. The attribute carries the FQDN of the assigned HA.

If available at the NAS, at least MIP6-HA-FQDN attribute and/or MIP6-HA SHOULD appear in accounting packets to indicate the identity of the serving HA for this session.



Type:

ASSIGNED-HA-FQDN-TYPE to be defined by IANA.

Length:

Variable length.

FQDN of the assigned HA:

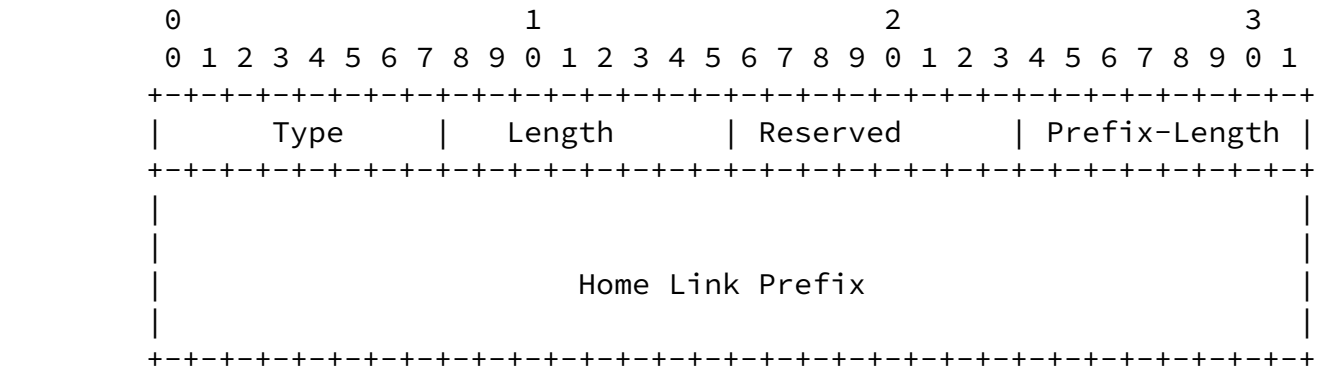
The data field MUST contain a FQDN as described in [10].

5.4. MIP6-HL-Prefix Attribute

This attribute is sent by the RADIUS-MIP server to the NAS in an

Access-Accept packet. The attribute carries the assigned Home Link prefix.

This attribute MAY be sent by the NAS to the RADIUS server in an Access-Request packet along with the MIP6-HA and/or MIP6-HA-FQDN attribute as a hint to suggest a Home Link prefix that may be assigned to the MN. The RADIUS server MUST use this value if it accepts the NAS's HA suggestion.



Type:

ASSIGNED-HL-TYPE to be defined by IANA.

Length:

>= 4 octets + the minimum length of a prefix.

Reserved:

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

Prefix-Length:

This field indicates the prefix length of the Home Link.

Home Link Prefix:

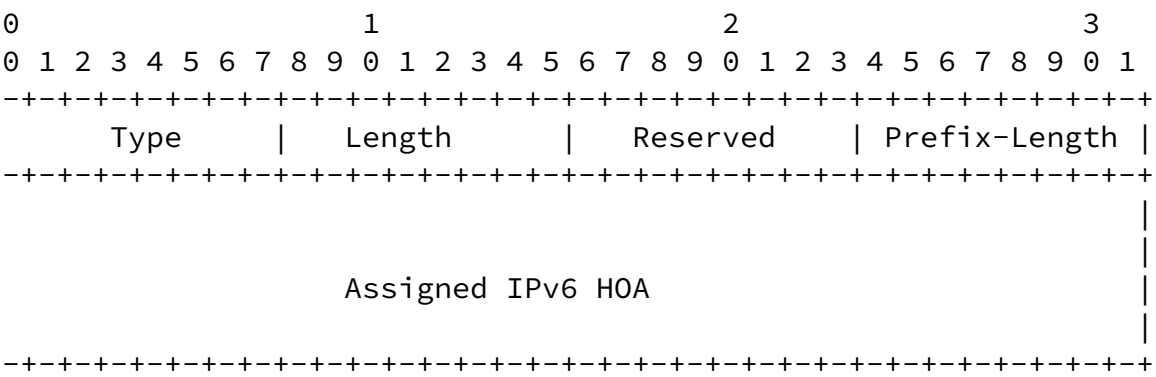
Home Link prefix (upper order bits) of the assigned Home Link where the MN should send binding update.

5.5. MIP6-HOA Attribute

This attribute is sent by the RADIUS server to the NAS in an Access-Accept packet. The attribute carries the assigned Home IPv6 Address for the MN.

This attribute MAY be sent by the NAS to the RADIUS server in an Access-Request packet along with the MIP6-HA and/or MIP6-HA-FQDN attribute as a hint to suggest a Home Address that may be assigned to the MN. The RADIUS server MUST use this value if it accepts the NAS's HA suggestion.

If available at the NAS, this attribute SHOULD appear in the accounting packets so that the IPv6 addressed used for this session is known in the accounting stream.



Type:

ASSIGNED-HOA-TYPE to be defined by IANA.

Length:

= 20 octets.

Reserved:

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

Prefix-Length:

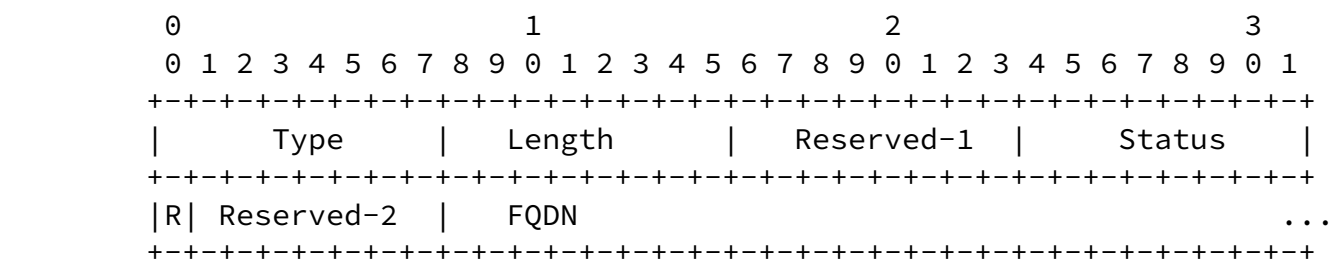
This field indicates the prefix length of the Home Link.

Assigned IPv6 HOA:

IPv6 HOA that is assigned to the MN.

5.6. MIP6-DNS-MO Attribute

The MIP6-DNS-MO attribute is used for triggering a DNS update by the RADIUS server and to return the result to the RADIUS client. The request MUST carry the MN's FQDN but the attribute carried in response to the request MAY not carry a FQDN value.



Type:

DNS-UPDATE-TYPE to be defined by IANA.

Length:

Variable length.

Reserved-1:

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

Status:

This 8 bit unsigned integer field indicates the result of the dynamic DNS update procedure as defined in [3]. This field MUST be set to 0 and ignored by the RADIUS server when the MIP6-DNS-MO is sent from the RADIUS client to the RADIUS server. When the MIP6-DNS-MO is provided in the response, values of the Status field less than 128 indicate that the dynamic DNS update was performed successfully by the RADIUS server. Values greater than or equal to 128 indicate that the dynamic DNS update was not successfully completed. The following values for the Status field are currently defined:

0 DNS update performed

128 Reason unspecified

129 Administratively prohibited

130 DNS Update Failed

R flag:

If this bit for the R flag is set then the RADIUS client requests the RADIUS server to remove the DNS entry identified by the FQDN included in this attribute. If not set, the RADIUS client is requesting the RADIUS server to create or update a DNS entry with the FQDN specified in this attribute and the Home Address carried in another attribute specified in this document.

Reserved-2:

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

FQDN of the MN:

In an Access-Request packet the data field MUST contain a FQDN. In an Access-Accept packet the data field MAY contain an FQDN. FQDN is described in [10].

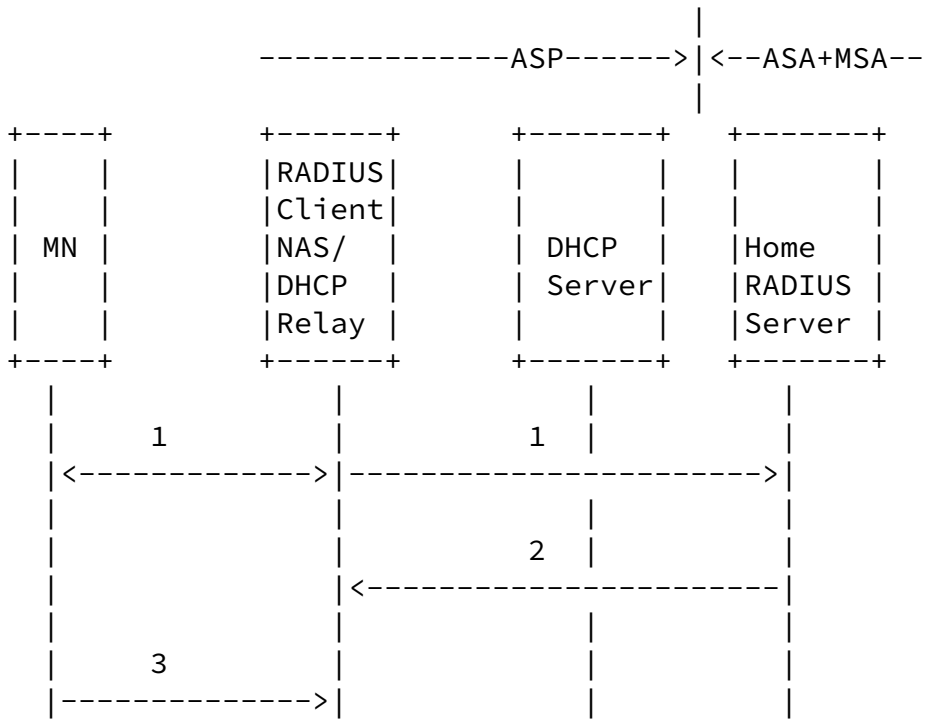
6. Message Flows

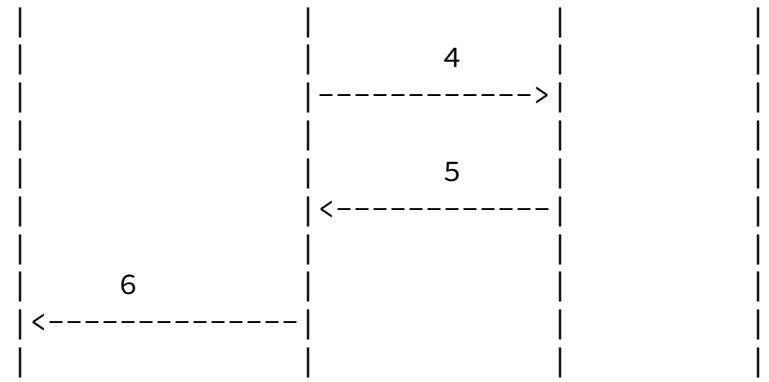
6.1. Integrated Scenario (MSA=ASA)

This section is based on [2] and uses the previously defined RADIUS attributes.

6.1.1. HA allocation in the MSP

RADIUS is used to authenticate the MN, to authorize it for the mobility service and to send information about the assigned HA to the NAS.





HA allocation in the MSP

In step (1), the MN executes the normal network access authentication procedure (e.g., IEEE 802.11i/802.1x, PANA) with the NAS. The NAS

acts as an authenticator in "pass-through" mode, i.e., the endpoint of the authentication dialogue is the MN's home RADIUS server. This is the typical scenario in case the messages involved in the authentication protocol are transported in EAP.

As per [11], the NAS encapsulates/decapsulates EAP packets into/from RADIUS packets until an Access-Response (either an Access-Accept or an Access/Reject packet is received by the NAS). This concludes the network access authentication phase.

If the NAS has the ability to support MIP6 Bootstrapping it includes the MIP6-Feature-Vector in the first Access-Request message and indicates whether it supports MIP6 bootstrapping and/or local home agent assignment by setting the appropriate flags therein.

If the NAS indicates support for Local home agent assignment, then it may also include the MIP6-HA Attribute(s) and/or MIP6-HA-FQDN Attribute(s) as a proposal to the RADIUS server of the HA to assign in the ASP.

In step (2), the RADIUS server sends an Access-Accept packet with the MIP6-Feature-Vector with the Local Home Agent Assignment flag set or cleared. If the flag is cleared then the RADIUS server needs to provide one or more Home Agent(s) to be assigned to the MN. If the flag is set, then it indicates to the NAS that it can assign HA to the MN; the RADIUS server may also include one or mroe HA addresses

thus indicating that the NAS can either allocate a local HA or one specified by the RADIUS server.

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

In step (4) the DHCP relay agent forwards this request to the DHCP server. The OPTION_MIP6-RELAY-Option is included in this forwarded message. This option carries the RADIUS MIP6-HA Attribute from the Access-Accept packet. If the NAS recieved the MIP6-HA-FQDN in the Access-Accept it peforms a DNS lookup to resolve the MIP6-HA address.

In step (5), the DHCP server identifies the client (by DUID) and finds out that it requests HA information in the MSP (by the Home Network Identifier Option = 1). The DHCP server extracts the HA address from OPTION_MIP6-RELAY-Option and places it into Home Network

Information Option in the Reply message.

In step (6), the Relay Agent forwards the Reply Message to the MN. On reception of this message, the HA address or the FQDN of the HA is available at the MN.

6.1.2. HA allocation in the ASP (visited network)

This scenario is similar to the one described in Section 6.1.1. The difference is in step (4), where the type-id field in the Home Network Identifier Option is set to zero, indicating that a HA is requested in the ASP instead of in the MSP. Thus, the information received by the home RADIUS server, via the DHCP relay, in the OPTION_MIP6-RELAY-Option (Information Request) is ignored. The DHCP server allocates a HA from its list of possible HAs and returns it in the Reply message (Home Network Information Option).

6.2. Split Scenario (MSA!=ASA)

6.2.1. Mobile Service Provider and Mobile Service Authorizer are the same entity.

The assumption in this scenario is that the MN has the domain name of the MSP preconfigured.

In this scenario there is no relationship between the network access authentication procedure and the MIPv6 bootstrapping procedure.

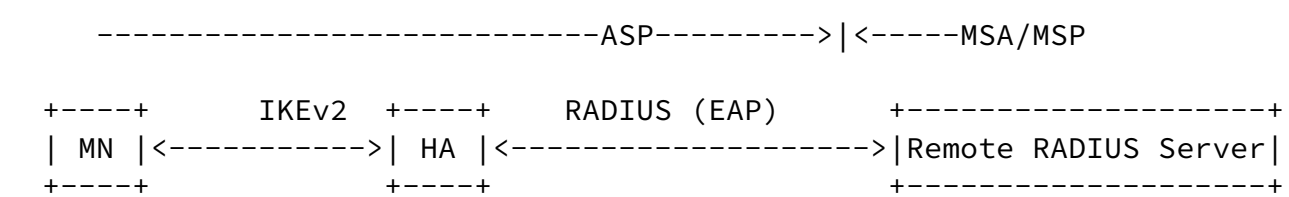
In order to learn the IP address of the HA, the MN either performs a DNS lookup of the HA Name or a DNS lookup by service name. In the first case, the MN is preconfigured with the FQDN of the HA, and thus sends a DNS request, where QNAME = name of HA, QTYPE='AAAA' (request for IPv6 address of HA). A DNS reply message is returned by the DNS server with the HA address.

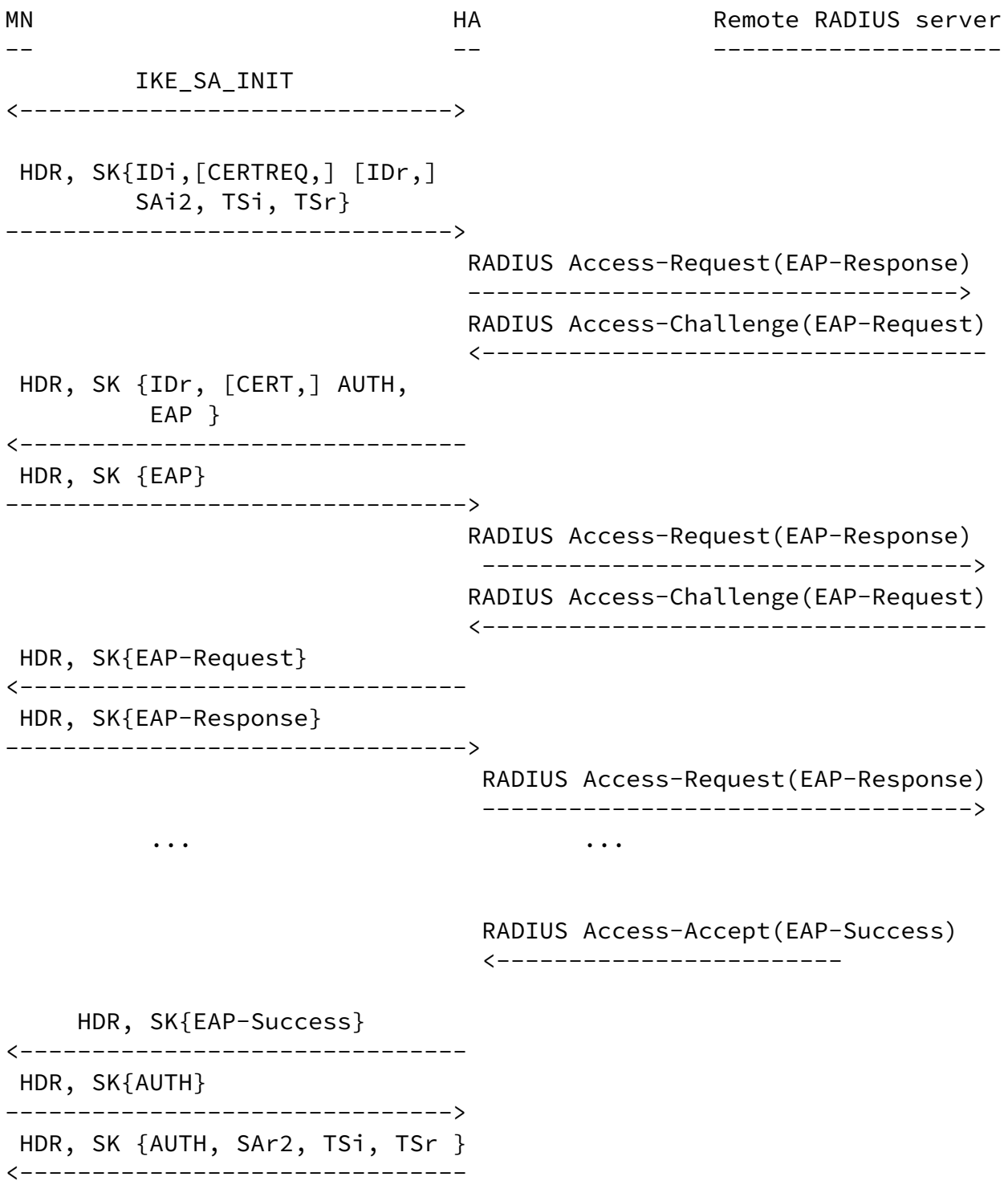
The MN then runs IKEv2 [12] with the HA in order to set up IPsec SAs (MN-HA). As part of this,the MN authenticates itself to the RADIUS server in the MSA domain, and obtains authorization for mobility service (including the Home Address).

The MN shares credentials with the RADIUS server in the MSA domain. The RADIUS communication between the HA and the this RADIUS server is also secured by RADIUS-specific mechanisms (e.g., IPsec). Using EAP within IKEv2 [12], the MN is authenticated and authorized for the IPv6 mobility service and is also assigned a HOA.

The setup of SAs and mutual authentication between MN and AAAH using RADIUS (and EAP) is similar to the one described for Diameter

protocol in [13]. The described mechanism ensureas that common keying material will be available at the MN and HA after successful completion.


ASP
MSA/MSP
IKEv2
RADIUS (EAP)
MN
HA
Remote RADIUS Server

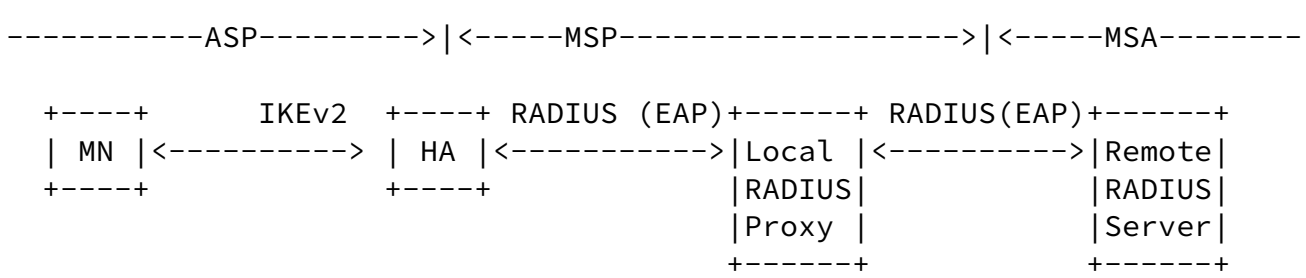


Split Scenario Exchange

MN and HA start with an IKE_SA_INIT to setup the IKE SA (messages defined in the IKEv2 specification [12], negotiating crypto algorithms and running DH key exchange). IKEv2 supports integration with EAP. The MN indicates its desire to use EAP by not including the AUTH payload in the third message. However, it indicates its identity (NAI) by using the IDi field. If the HA supports EAP for authentication, as per [11] it forwards the identity to the Remote RADIUS server by sending a RADIUS Access-Request packet containing the identity in the EAP-Payload AVP and in the RADIUS User-Name attribute. Based on this identity, the Remote RADIUS server chooses authentication method and sends the first EAP-Request in the RADIUS Access-Challenge packet. During the EAP authentication phase, the HA relays EAP packets between the MN and the Remote RADIUS server. If the authentication succeeds and if the MN is authorized to use Mobile IPv6 service, the Remote RADIUS server sends a RADIUS Access-Accept packet containing the EAP-Success and the AAA-Key derived from the EAP authentication method. EAP authentication methods that do not derive keys are not recommended. This key is used by both MN and HA to generate the AUTH payload. In subsequent messages, MN and HA setup IPsec SAs for Mobile IPv6.

6.2.2. Mobile Service Provider and Mobile Service Authorizer are different entities.

The HA address discovery is performed as described in Section 6.2.1.



MSP#MSA Exchange

The scenario is similar to previously described scenarios with the difference of utilizing AAA roaming agreements between the MSP and the MSA.

7. Goals for the HA-AAA Interface

Here, we follow the classification and labels listed in the MIPv6-AAA-Goals document [14].

7.1. General Goals

G1.1-G1.4 Security

These are standard requirements for a AAA protocol - mutual authentication, integrity, replay protection, confidentiality. IPsec can be used to achieve the goals. Goal G1.5 regarding inactive peer detection needs further investigations since heartbeat messages do not exist (like in the Diameter case, Watch-Dog-Request/Answer).

7.2. Service Authorization

G2.1. The AAA-HA interface should allow the use of Network Access Identifier (NAI) to identify the MN. The User-Name attribute can be used for the purpose to carry the NAI.

G2.2 The HA should be able to query the AAAH server to verify Mobile IPv6 service authorization for the MN. Any node implementing RADIUS functionality[5] can possibly initiate a request message. In combination with the ability of the RADIUS protocol to carry EAP messages [11] , our solution will enable an HA to query a RADIUS server and verify MIPv6 authorization for the MN.

G2.3 The AAAH server should be able to enforce explicit operational limitations and authorization restrictions on the HA (e.g., packet filters, QoS parameters). Work in progress in the area, including NAS-Filter-Rule, RADIUS quality of service support, prepaid extensions etc. is performed. The relevant attributes may be reused for providing required functionality over the AAAH-HA interface.

G2.4 - G2.6. Issues addressing the maintenance of a Mobile IPv6 session by the AAAH server, e.g., authorization lifetime, extension of the authorization lifetime and explicit session termination by the AAAH server side.

The attribute Session-Timeout may be sent in Access-Challenge or Access-Accept packet by the RADIUS server, thus limiting the

authorization session duration. In order to reauthenticate/ reauthorize the user, the Termination-Action attribute can be included, with value 1, meaning the NAS should send a new RADIUS-Request packet. Additional AVPs for dealing with pre-paid sessions (e.g,. volume, resource used--VolumeQuota AVP, ResourceQuota AVP) are specified in RADIUS prepaid extension. Exchanging of application

specific authorization request/answer messages provides extension of the authorization session (e.g., Authorize Only Access-Request sent by the HA (NAS) to the RADIUS server). Initiation of the re-authorization by both sides could be supported. Both sides could initiate session termination - the RADIUS server by sending Disconnect message [15].

7.3. Accounting

G3.1 The AAA-HA interface must support the transfer of accounting records needed for service control and charging. These include (but may not be limited to): time of binding cache entry creation and deletion, octets sent and received by the MN in bi-directional tunneling, etc.

The requirements for accounting over the AAAH-HA interface does not require enhancements to the existing accounting functionality.

7.4. MN Authentication

G4.1 The AAA-HA interface MUST support pass-through EAP authentication with the HA working as EAP authenticator operating in pass-through mode and the AAAH server working as back-end authentication server.

These issues require the functionality of AAAH server working as a back-end authentication server and HA working as NAS and EAP authenticator in pass-through mode for providing a MN authentication. This document suggests this mode of operation in the context of the relevant scenarios.

7.5. Provisioning of Configuration Parameters

G5.1 The HA should be able to communicate to the AAAH server the HOA allocated to the MN (e.g. for allowing the AAAH server to perform DNS

update on behalf of the MN).

This document describes needed AVPs for this purpose, see section "DNS Update Mobility Option Attribute"

8. Table of Attributes

The following tables provides a guide to which attributes may be found in RADIUS packet and in what number.

The following defines the meaning of the notation used in the following tables:

0	An instance of this attribute MUST NOT be present.
1	Exactly one instance of this attribute MUST be present
0-1	Zero or one instance of this attribute MAY be present.
0+	Zero or more instance of this attriubte MAY be present

Request	Accept	Reject	Challenge	Type	Attribute
1	1	0	0	MIP6-FV-TYPE	MIP6-Feature-Vector
0+[ac]	0+[a]	0	0	MIP6-HA-TYPE	MIP6-HA
0+[ac]	0+[a]	0	0	MIP6-HA-FQDN-TYPE	MIP6-HA-FQDN
0-1[b]	0-1	0	0	MIP6-HL-PREFIX-TYPE	MIP6-HL-Prefix
0-1[b]	0-1	0	0	MIP6-HOA-TYPE	MIP6-HOA
0-1	0-1	0	0	MIP6-DNS-MO-TYPE	MIP6-DNS-MO

Notes:

[a] Either MIP6-HA or MIP6-HA-FQDN MAY appear in a RADIUS packet.

[b] If MIP6-HA or MIP6-HA-FQDN are present in the Access-Request

then these attributes MUST also be present in the Access-Request. If the RADIUS server accepts the NAS suggestion for the HA, then the RADIUS server MUST also include the values received for these attributes in the Access-Accept.

[c] If these attributes are present in an Access-Request, then LOCAL_HOME_AGENT_ASSIGNMENT flag of the MIP6-Feature-Vector MUST be set. Otherwise these attributes are ignored.

As used in accounting packets:

Request	Interim	Stop	Type	Attribute
0-1	0-1	0-1	MIP6-HA-TYPE	MIP6-HA Attribute
0-1	0-1	0-1	MIP6-HA-FQDN-TYPE	MIP6-HA-FQDN Attribute
0	0	0	MIP6-HL-PREFIX-TYPE	MIP6-HL-Prefix Attribute
0-1	0-1	0-1	MIP6-HOA-TYPE	MIP6-HOA Attribute
0	0	0	MIP6-DNS-MO-TYPE	MIP6-DNS-MO Attribute

9. Diameter Considerations

When used in Diameter, the attributes defined in this specification can be used as Diameter AVPs from the Code space 1-255 (RADIUS attribute compatibility space). No additional Diameter Code values are therefore allocated. The data types and flag rules for the attributes are as follows:

		AVP Flag rules				
Attribute Name	Value Type	MUST	MAY	SHLD NOT	MUST NOT	Encr
MIP6-HA	Address	M	P		V	Y
MIP6-HA-FQDN	UTF8String	M	P		V	Y
MIP6-HL-Prefix	OctetString	M	P		V	Y
MIP6-HOA	Address	M	P		V	Y
MIP6-DNS-MO	OctetString	M	P		V	Y

```
------------------------------|----+-----+----+-----|----|
```

Other than MIP6-HA and HOA-IPv6, the attributes in this specification have no special translation requirements for Diameter to RADIUS or RADIUS to Diameter gateways; they are copied as is, except for changes relating to headers, alignment, and padding. See also [16] Section 4.1 and [17] Section 9. MIP6-HA and HOA-IPv6 must be translated between their RADIUS representation of String to a Diameter Address format which requires that the AddressType field be set to 2 for IP6 (IP version 6)

What this specification says about the applicability of the attributes for RADIUS Access-Request packets applies in Diameter to AA-Request [17] or Diameter-EAP-Request [18]. What is said about Access-Challenge applies in Diameter to AA-Answer [17] or Diameter-EAP-Answer [18] with Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH.

What is said about Access-Accept applies in Diameter to AA-Answer or Diameter-EAP-Answer messages that indicate success. Similarly, what is said about RADIUS Access-Reject packets applies in Diameter to AA-Answer or Diameter-EAP-Answer messages that indicate failure.

What is said about Accounting-Request applies to Diameter Accounting-Request [17] as well.

10. Security Considerations

Assignment of these values to a user should be based on successful authentication of the user at the NAS and/or at the HA. The RADIUS server should only assign these values to a user who is authorized for Mobile IPv6 service (this check could be performed with the user's subscription profile in the Home Network).

The NAS and the HA to the RADIUS server transactions must be adequately secured. Otherwise there is a possibility that the user may receive fraudulent values from a rogue RADIUS server potentially hijacking the user's Mobile IPv6 session.

These new attributes do not introduce additional security

considerations besides the ones identified in [5].

11. IANA Considerations

11.1. Registration of new AVPs

This specification defines the following new RADIUS attributes:

MIP6-Feature-Vector is set to MIP6-FV-TYPE

MIP6-HA is set to MIP6-HA-TYPE

MIP6-HA-FQDN is set to MIP6-HA-FQDN-TYPE

MIP6-HL-Prefix is set to MIP6-HL-PREFIX-TYPE

MIP6-HOA is set to MIP6-HOsA-TYPE

MIP6-DNS-MO is set to MIP6-DNS-MO-TYPE

11.2. New Registry: Mobility Capability

For MIP6-FV-TYPE flag values must be generated:

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

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

Following the policies outlined in [1] new values with a description of their semantic for usage with the MIP6-Feature-Vector AVP together with a Token will be assigned after Expert Review initiated by the O&M Area Directors in consultation with the DIME working group chairs or the working group chairs of a designated successor working group. Updates can be provided based on expert approval only. A designated expert will be appointed by the O&M Area Directors. No mechanism to mark entries as "deprecated" is envisioned. Based on expert approval it is possible to delete entries from the registry.

11.3. Addition of existing values

A new value HA6(IANA-TBD1) MUST be assigned to NAS-Port-Type(61)

12. Acknowledgements

We would like to thank the following individuals for their review and constructive comments during the development of this document:

Florian Kohlmayer, Mark Watson, Jayshree Bharatia, Dimiter Milushev, Andreas Pashalidis, Rafa Marin Lopez and Pasi Eronen.

13. References

13.1. Normative References

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

[2] Chowdhury, K. and A. Yegin, "MIP6-bootstrapping for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-05 (work in progress), July 2007.

[3] Giaretta, G., "Mobile IPv6 bootstrapping in split scenario", draft-ietf-mip6-bootstrapping-split-07 (work in progress), July 2007.

[4] Zorn, G., "Microsoft Vendor-specific RADIUS Attributes", RFC 2548, March 1999.

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

13.2. Informative References

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

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

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

[9] Dupont, F. and V. Devarapalli, "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture", draft-ietf-mip6-ikev2-ipsec-08 (work in progress), December 2006.

[10] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[11] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial

In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

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

[13] Tschofenig, H., "Mobile IPv6 Bootstrapping using Diameter", draft-tschofenig-mip6-aaa-ha-diameter-01 (work in progress), October 2005.

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

[15] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.

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

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

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

[19] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[20] Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[21] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

Authors' Addresses

Avi Lior
Bridgewater Systems
303 Terry Fox Drive, Suite 100
Ottawa, Ontario
Canada K2K 3J1

Phone: +1 613-591-6655
Email: avi@bridgewatersystems.com

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury, MA 01876
US

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

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Hannes.Tschofenig@siemens.com

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in

this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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