MIP6
Internet-Draft
Expires: December 25, 2006

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

June 23, 2006

RADIUS Mobile IPv6 Support
draft-chowdhury-mip6-radius-02.txt

Status of this Memo

Copyright Notice

Abstract

A Mobile IPv6 node requires a home agent address, a home address, and an IPsec security association with its home agent 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 the existing authentication, authorization and accounting infrastructure. This document defines new attributes that 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 home agent and the AAA infrastructure.

Table of Contents

1. Introduction

The Mobile IPv6 specification [5] requires a Mobile Node (MN) to perform registration with a Home Agent with information about its current point of attachment (Care-of Address). The Home Agent creates and maintains a binding between the MN's Home Address and the MN's Care-of Address.

In order to register with a Home Agent, the MN needs to know some information such as the Home Link prefix, the Home Agent Address, the Home Address, 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 home agent, in case of the split scenario. The terms integrated and split are described in the terminology section and were introduced in [6].

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 [7]. The following additional terms, as defined in [6], 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 mobile node.

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 mobile node 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 the MIPv6 bootstrapping as outlined in the MIPv6 bootstrapping problem statement document (see [6]). 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 home agent to AAA server and the network access server 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 entities.

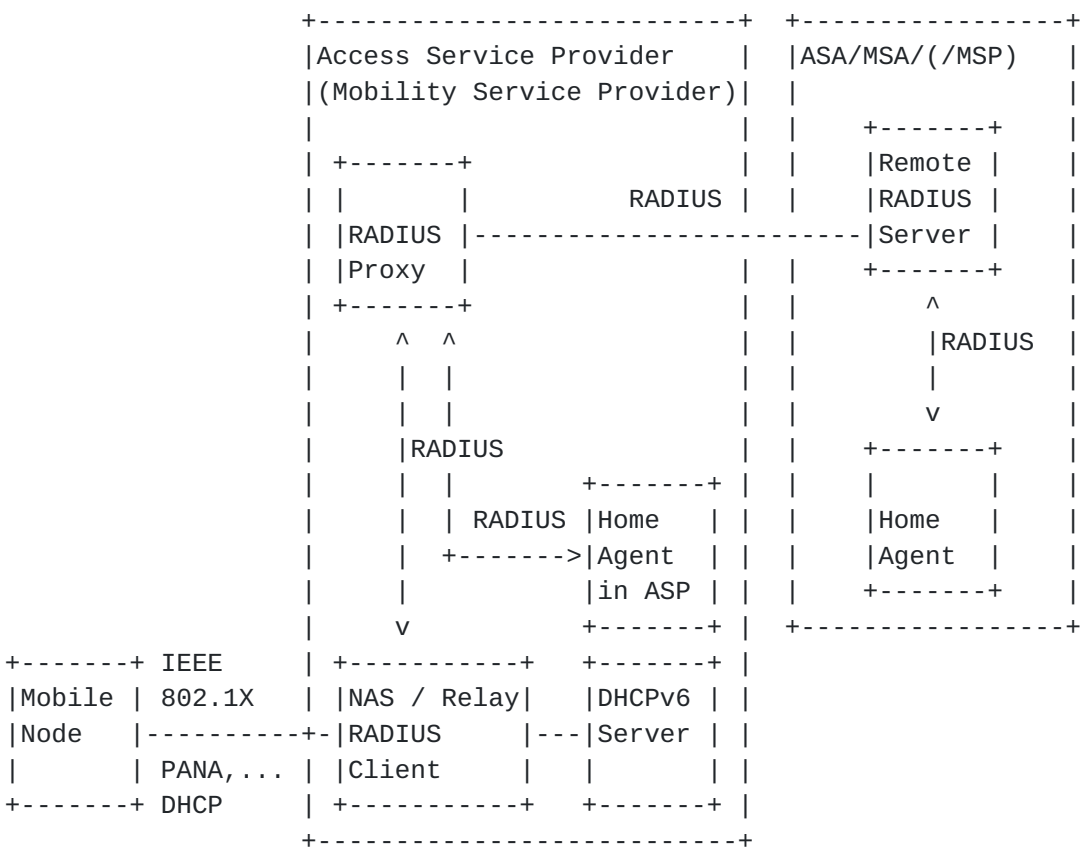


Figure 1: Mobile IPv6 Service Access in the Integrated Scenario

In the typical Mobile IPv6 access scenario as shown above, the MN attaches in a Access Service Provider's network. During this network

attachment procedure, the NAS/RADIUS client interacts with the mobile node. 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 to use the Mobile IPv6 service, too. 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 home agent.

Depending on the details of the solution, an 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 mobile node. 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.

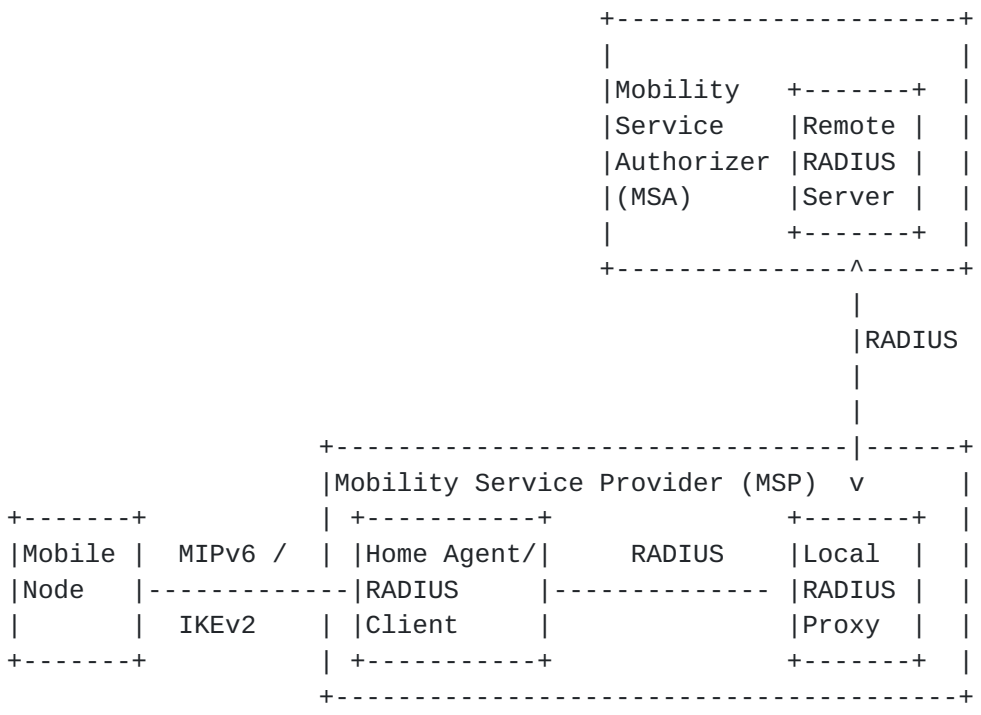


Figure 2: Mobile IPv6 service access in the split scenario (MSA != MSP)

As shown in Figure 2 the interaction between the RADIUS client and the RADIUS server is triggered by the protocol interaction between the mobile node and the home agent/RADIUS client using IKEv2 (see [3] and [8]). The home agent (i.e., RADIUS client) interacts with the RADIUS infrastructure in order to perform authentication, authorization, accounting and parameter bootstrapping. The AAA exchange is triggered by the home agent. When the protocol exchange is completed then the home agent possesses the Mobile IPv6 specific parameters (see [6]).

Additionally, the mobile node may instruct the RADIUS server (via the home agent) to perform a dynamic DNS update.

4. RADIUS Attribute Overview

4.1. Home Agent Address Attribute

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

4.2. Home Agent FQDN Attribute

The RADIUS server may assign an home agent address FQDN. The mobile node can perform a DNS query with the FQDN to derive the home agent address.

4.3. Home Link 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).

4.4. Home Address Attribute

The RADIUS server may assign a Home Address 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 Home Agent address.

4.5. DNS Update Mobility Option 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 DNS Update Mobility Option attribute.

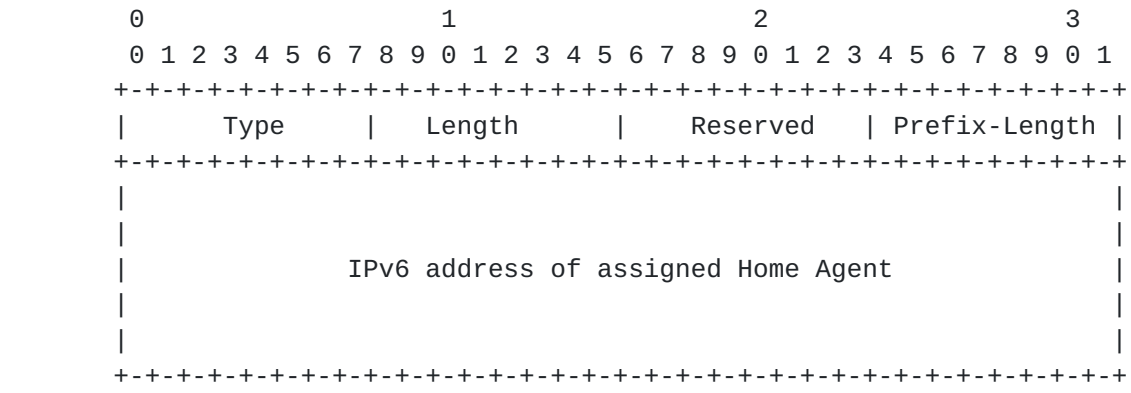
5. RADIUS attributes

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 the Access-Accept and the Accounting-Request.

5.1. Home Agent Address Attribute

This attribute is sent by the RADIUS server to the NAS in an Access-Accept message. The attribute carries the assigned Home Agent address.



Type:

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

Length:

= 20 octets

Reserved:

Reserved for future use. All bits set to 0.

Prefix-Length:

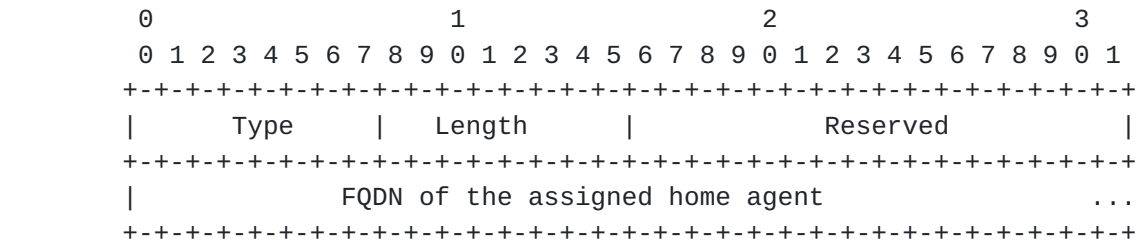
This field indicates the prefix length of the Home Link.

IPv6 address of assigned Home Agent:

128-bit IPv6 address of the assigned Home Agent.

5.2. Home Agent FQDN Attribute

This attribute is sent by the RADIUS server to the NAS in an Access-Accept message. The attribute carries the FQDN of the assigned home agent.



Type:

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

Length:

Variable.

Reserved:

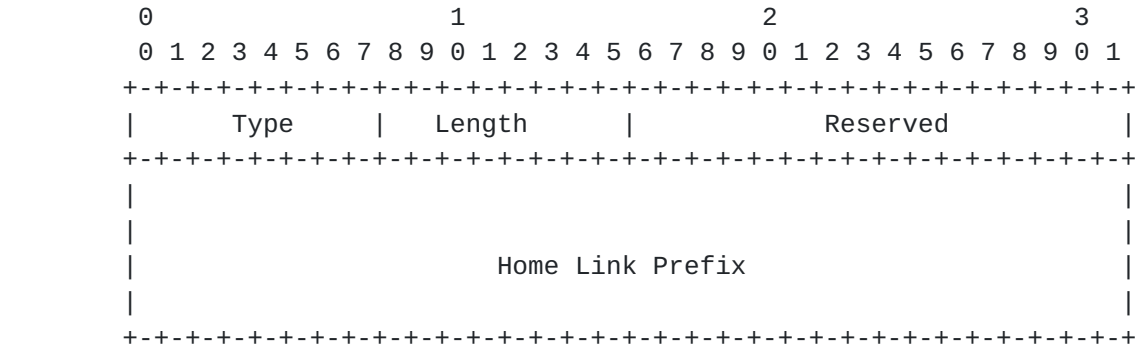
Reserved for future use. All bits set to 0.

FQDN of the assigned home agent:

The data field MUST contain a FQDN as described in [9].

5.3. Home Link Prefix Attribute

This attribute is sent by the RADIUS-MIP server to the NAS in an Access-Accept message. The attribute carries the assigned Home Link prefix.



Type:

ASSIGNED-HL-TYPE to be defined by IANA.

Length:

Variable

Reserved:

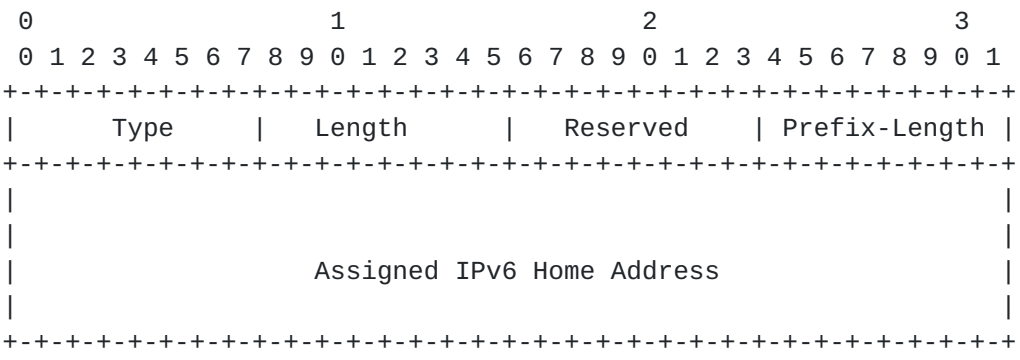
Reserved for future use. All bits set to 0.

Home Link Prefix:

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

5.4. Home Address Attribute

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



Type:

ASSIGNED-HOA-TYPE to be defined by IANA.

Length:

= 20 octets.

Reserved:

Reserved for future use. All bits set to 0.

Prefix-Length:

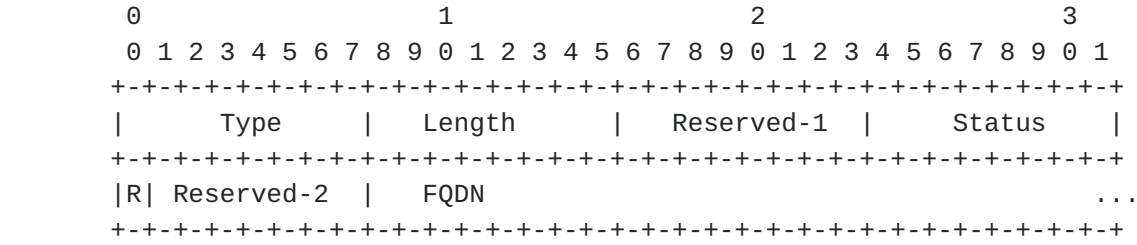
This field indicates the prefix length of the Home Link.

Assigned IPv6 Home Address:

IPv6 Home Address that is assigned to the MN.

5.5. DNS Update Mobility Option Attribute

The DNS Update Mobility Option 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 mobile node'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

Reserved-1:

Reserved for future use. All bits set to 0.

Status:

This 8 bit unsigned integer field indicates the result of the dynamic DNS update procedure. This field MUST be set to 0 and ignored by the RADIUS server when the DNS Update Mobility Option is sent from the RADIUS client to the RADIUS server. When the DNS Update Mobility Option 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. All bits set to 0.

FQDN of the mobile node:

The data field MUST contain a FQDN as described in [9].

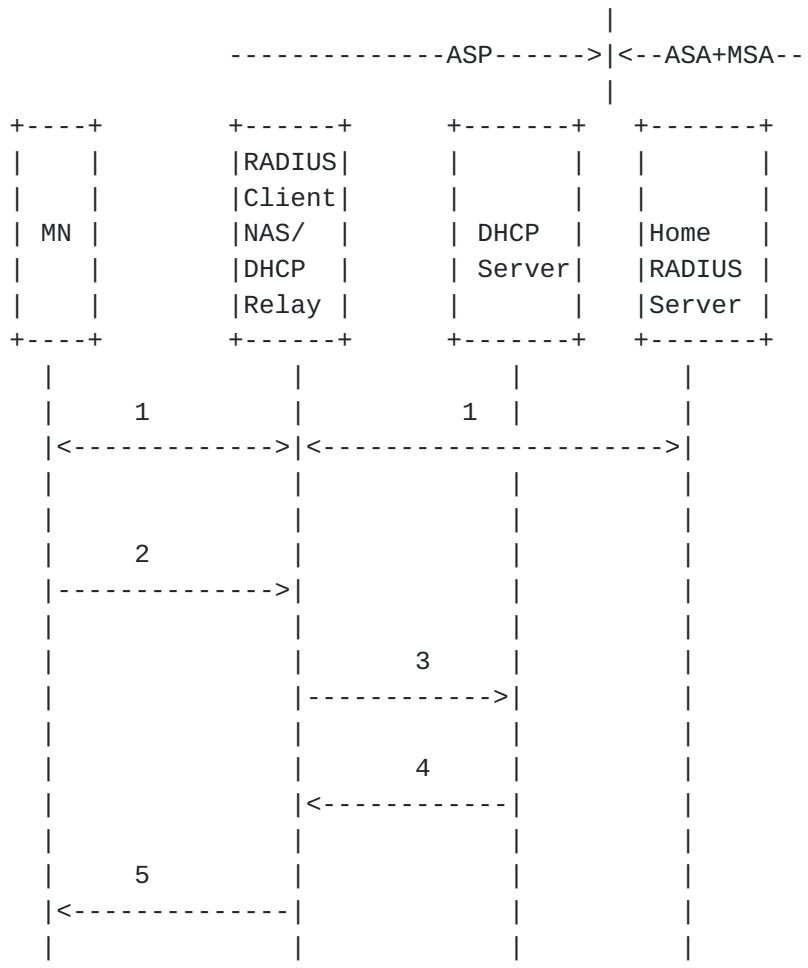
6. Message Flows

6.1. Integrated Scenario (MSA=ASA)

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

6.1.1. Home Agent allocation in the MSP

RADIUS is used to authenticate the mobile node, to authorize it for the mobility service and to send information about the assigned home agent to the NAS.



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.

The NAS encapsulates/decapsulates EAP packets into/from RADIUS messages 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.

Depending on the RADIUS server configuration, the Home Agent Address attribute or the Home Agent FQDN attribute may be appended to the Access-Accept message. In the latter case the MN needs to perform a DNS query in order to discover the Home Agent address.

The Home Agent Address or Home Agent FQDN attribute is appended to the access accept in case the home RADIUS server knows or has allocated a HA to the access request (this is assumed in this scenario).

In step (2) 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 (3) 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 Home Agent Address Attribute from the access accept message.

In step (4), the DHCP server identifies the client and finds out that it requests home agent information in the MSP (by the Home Network Identifier Option = 1). The DHCP server extracts the home agent address from OPTION_MIP6-RELAY-Option and places it into Home Network Information Option in the Reply message.

In step (5), the Relay Agent forwards the Reply Message to the Mobile Node. On reception of this message, the home agent address or the FQDN of the home agent is available at the MN.

6.1.2. Home Agent allocation in the ASP (visited network)

This scenario is similar to the one described in Section 6.1.1. The difference is in step (2), where the type-id field in the Home Network Identifier Option is set to zero, indicating that a Home Agent 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 home agent from its list of possible home

agents 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.

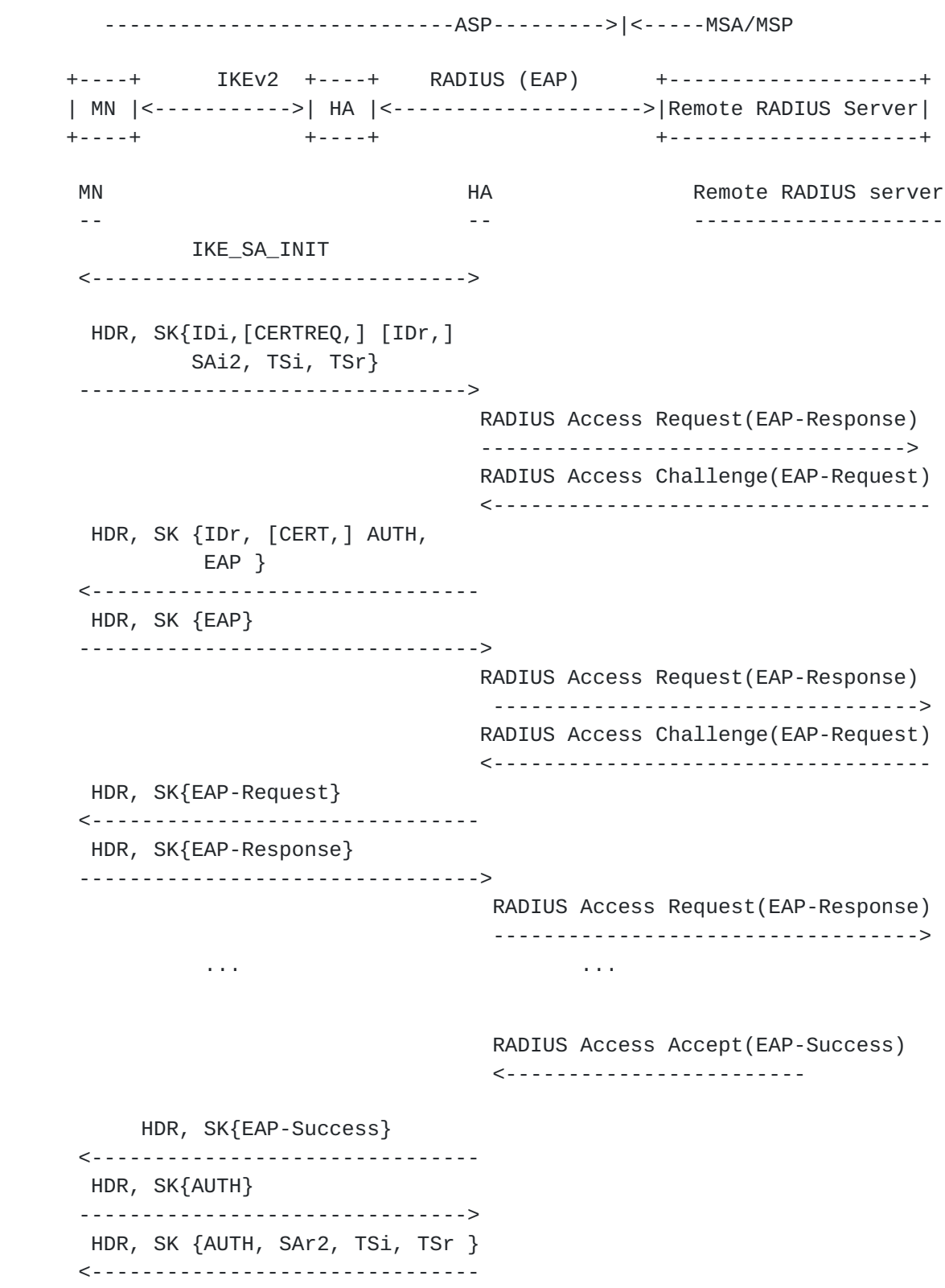
In this scenario there is no relationship between the network access authentication procedure and the MIPv6 bootstrapping procedure.

In order to learn the IP address of the home agent, the MN either performs a DNS lookup of the Home Agent 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 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, the MN is authenticated and authorized for the IPv6 mobility service and is also assigned a home address.

The setup of SAs and mutual authentication between MN and AAAH using RADIUS (and EAP) is similar to the one described for the Diameter protocol in [10]. The described mechanism ensures that common keying material will be available at the MN and the HA after successful completion.

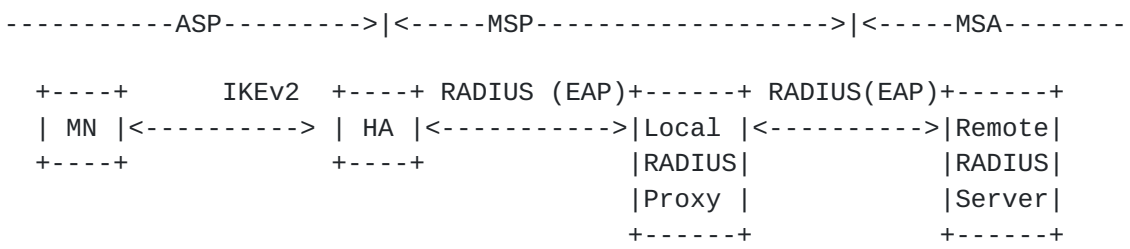


MN and HA start with an IKE_SA_INIT to setup the IKE SA (messages defined in the IKEv2 specification, negotiating crypto algorithms and

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, it forwards the identity to the Remote RADIUS server by sending a RADIUS Access-Request message 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 message. 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 message 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.



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 [11].

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 in RADIUS (like in the Diameter case, Watch-Dog-Request/ Answer).

7.2. Service Authorization

G2.1. The AAA-HA interface should allow the use of the Network Access Identifier (NAI) to identify the mobile node. 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 in order to verify Mobile IPv6 service authorization for the mobile node. Any node implementing RADIUS functionality can possibly initiate a request message. In combination with the ability of the RADIUS protocol to carry EAP messages, the mechanisms described in this document 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 message 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.

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 mobile node 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. Mobile Node 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 mobile node 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 Home Address 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 table provides a guide to which attributes may be found in RADIUS message and in what number.

Request	Accept	Reject	Challenge	Attribute
0-1	0-1	0	0	Home Agent Address Attribute
0-1	0-1	0	0	Home Agent FQDN Attribute
0-1	0-1	0	0	Home Link Prefix Attribute
0-1	0-1	0	0	Home Address Attribute
0-1	0-1	0	0	DNS Update Mobility Option Attribute

The following table defines the meaning of the above table entries.

0	This attribute MUST NOT be present.
0-1	Zero or one instance of this attribute MAY be present.

9. Security Considerations

Assignment of MIPv6 specific parameters has to be based on a protocol run between the participating parties with a successful outcome (i.e., successful authentication and authorization). The RADIUS server should only assign MIPv6 specific parameters to an end host that 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 home agent 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 [4].

10. IANA Considerations

The following RADIUS attribute Type values MUST be assigned by IANA.

- ASSIGNED-HA-ADDR-TYPE
- ASSIGNED-HA-FQDN-TYPE
- ASSIGNED-HL-TYPE
- ASSIGNED-HOA-TYPE
- DNS-UPDATE-TYPE

11. 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.

12. References

12.1. 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 via DHCPv6 for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-01 (work in progress), June 2006.

[3] Giaretta, G., "Mobile IPv6 bootstrapping in split scenario", draft-ietf-mip6-bootstrapping-split-02 (work in progress), March 2006.

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

12.2. Informative References

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

[6] Giaretta, G. and A. Patel, "Problem Statement for bootstrapping Mobile IPv6", draft-ietf-mip6-bootstrap-ps-05 (work in progress), May 2006.

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

[8] Dupont, F. and V. Devarapalli, "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture", draft-ietf-mip6-ikev2-ipsec-06 (work in progress), April 2006.

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

[10] Korhonen, J., "Diameter MIPv6 Bootstrapping for the Integrated Scenario", draft-ietf-dime-mip6-integrated-00 (work in progress), June 2006.

[11] Giaretta, G., "Goals for AAA-HA interface", draft-ietf-mip6-aaa-ha-goals-01 (work in progress), January 2006.

[12] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose,

"DNS Security Introduction and Requirements", RFC 4033, March 2005.

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

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

Authors' Addresses

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

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

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

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

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

Email: Hannes.Tschofenig@siemens.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.