RADIUS Attributes for Mobile IPv6 bootstrapping
draft-chowdhury-mip6-bootstrap-radius-01.txt

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on April 26, 2005.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document defines new attributes to facilitate Mobile IPv6 bootstrapping via a RADIUS infrastructure. In an access network where the user attaches to get IPv6 access, there may be a Network Access Server (NAS) or an Access Gateway that will require authentication and authorization. In some cases, this type of access authentication takes place via RADIUS infrastructure. As part of the authentication setup the NAS may receive useful configuration information from the home RADIUS server of the user. In case of
Mobile IPv6 access, the Home RADIUS server may assign various information relevant to the user’s device for bootstrapping.

Table of Contents

1. Motivation .................................................. 3
2. Overview .................................................. 4
   2.1 Home Agent .............................................. 4
   2.2 Home Link Prefix ........................................ 5
   2.3 Home Address ............................................. 5
   2.4 Authenticity payload ..................................... 5
3. Terminology .................................................. 6
4. RADIUS attributes to carry Mobile IPv6 parameters .......... 7
   4.1 Home Agent Attribute .................................... 7
   4.2 Home Link Prefix Attribute ............................. 8
   4.3 Home Address ............................................ 8
   4.4 MIP6 Parameter Authenticity Attribute .................. 9
5. Table of Attributes .......................................... 11
6. MN Considerations ........................................... 12
7. Security Considerations ..................................... 13
8. IANA Considerations ......................................... 14
9. Acknowledgements ........................................... 15
10. Normative References ........................................ 15
    Authors’ Addresses ......................................... 15
    Intellectual Property and Copyright Statements ............ 16
1. Motivation

Mobile IPv6 specification [RFC3775] 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 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 information such as, the Home Link prefix, the Home Agent Address, the Home Address, the Home Link prefix Length etc.

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; or the cost of the link between the NAS and the Home Link is too great. 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 Serving or Home Mobility Service Provider’s network (RADIUS-MIP) may return these parameters to the NAS.

The NAS may convey the received information to the MN using various techniques. One such technique may utilize the role of the NAS as a relay agent for Dynamic Host Configuration Protocol. In this case, upon receiving the information from the RADIUS-MIP server, the NAS forwards the set of parameters to the DHCP Client along with REPLY or ADVERTISE messages [MIP6-DHC-AGENTOP].
2. Overview

In the typical Mobile IPv6 access scenario as shown above, the MN attaches in a Access Service Provider’s network. During this attach procedure, the NAS or the Access Router authenticates and authorizes the MN for IPv6 access service. In the scenario shown, the authentication and authorization happens via a RADIUS infrastructure.

At the time of authorizing the user for IPv6 access, the RADIUS server in the Home or Serving Mobility Service Provider’s (MSP) network (RADIUS-MIP) detects that the user is authorized for Mobile IPv6 access. Based on the MSP’s policy, the RADIUS-MIP server may allocate several parameters to the MN for use during the subsequent Mobile IPv6 registration. A list of such parameters is described in the following sub sections.

2.1 Home Agent

The Home or the Serving MSP 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 assigning Home Agents to the MN, e.g. load sharing in the network. The
attribute also contains the prefix length so that the MN can easily infer the Home Link prefix from the Home Agent address.

2.2 Home Link Prefix

For the same reason as the HA assignment, the Home or the Serving MSP may assign a Home Link that is in close proximity to the point of attachment (NAS-ID). The MN can perform [RFC3775] specific procedures to discover other information for Mobile IPv6 registration.

2.3 Home Address

The RADIUS-MIP 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.

2.4 Authenticity payload

The RADIUS-MIP server includes a secure hash of all the MIP6 related assigned parameters. The secure hash is computed with the shared secret that the RADIUS-MIP has with the MN. This helps maintain the integrity of the assigned values while the Access Service Provider and the Mobility Service Provider do not a share trust relationship.
3. 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 RFC 2119.
4. RADIUS attributes to carry Mobile IPv6 parameters

This section defines format and syntax for the attribute that carries the Mobile IPv6 parameters described in section 2.

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

4.1 Home Agent Attribute

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

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |   Length      |    Reserved   | Prefix-Length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                                                               |
|                                                               |
|              IPv6 address of assigned Home Agent              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

ASSIGNED-HA-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.
4.2 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.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type | Length | Reserved |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| HOME_LINK_PREFIX |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

ASSIGNED-HL-TYPE to be defined by IANA.

Length:

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

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.

4.3 Home Address

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.
4.4 MIP6 Parameter Authenticity Attribute

This attribute is sent by the RADIUS-MIP server to the NAS in an Access-Accept message. The attribute carries a authenticator to validate the integrity of the MIP6 parameters that are assigned by the RADIUS-MIP server. The authenticator is calculated by taking HMAC-SHA-1 of all the MIP6-related assigned parameter values and a shared secret that the RADIUS-MIP server has for the MN.
Type:  
MIP6-PARM-AUTH-TYPE to be defined by IANA.

Length:  
= 20 octets.

Reserved:  
Reserved for future use. All bits set to 0.

Authenticator:  
HMAC-SHA-1 (shared secret between the MN and the RADIUS-MIP, assigned MIP6 values).
5. Table of Attributes

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

<table>
<thead>
<tr>
<th>Request</th>
<th>Accept</th>
<th>Reject</th>
<th>Challenge</th>
<th>#</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>TBD</td>
<td>Home Agent</td>
</tr>
<tr>
<td>0</td>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>TBD</td>
<td>Home Link Prefix</td>
</tr>
<tr>
<td>0</td>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>TBD</td>
<td>Home Address</td>
</tr>
<tr>
<td>0</td>
<td>0-1</td>
<td>0</td>
<td>0</td>
<td>TBD</td>
<td>MIP6 Parameter Authenticity</td>
</tr>
</tbody>
</table>

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.
6. MN Considerations

Upon receiving the MIP6 parameters from the network via mechanisms such as [MIP6-DHC-AGENTOP] the MN MUST check whether the parameter set contains the MIP6 Parameter Authenticity value. If yes, the MN MUST compute a secure hash as following:

HMAC-SHA-1 (shared secret between the MN and the RADIUS-MIP, received MIP6 values)

The MN matches the output of the above hash with the MIP6 Parameter Authenticity value received from the network. If the values match the MN accept the received MIP6 parameters to be from a trusted source. If the comparison results in a mismatch, the MN MUST silently discard the received MIP6 parameters.

If the received MIP6 parameter set does not contain the MIP6 Parameter Authenticity value, the MN MAY accept the received MIP6 parameters.
7. Security Considerations

Assignment of these values to a user should be based on successful authentication of the user’s access at the NAS. The RADIUS-MIP server should only assign these values to an 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 to the Home 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.

If the RADIUS-MIP server has a shared secret with the MN, the RADIUS-MIP server MUST include the MIP6 Parameter Authenticity attribute while assigning other MIP6 bootstrap information to the MN. This enables the MN to verify that the received MIP6 bootstrap information is from a trusted source.

These new attributes do not involve additional security considerations besides the one identified in [RFC2865].
8. IANA Considerations

The RADIUS attribute types: ASSIGNED-HA-TYPE, ASSIGNED-HL-TYPE, ASSIGNED-HOA-TYPE, and MIP6-PARM-AUTH-TYPE MUST be assigned by IANA.
9. Acknowledgements

Thanks to the following individuals for their review and constructive comments during the development of this document:

Mark Watson, Jayshree Bharatia.

10 Normative References

[MIP6-DHC-AGENTOP]
Chowdhury et. al., K., "DHCP Relay Agent Option to Support Mobile IPv6 bootstrapping",
draft-chowdhury-dhc-mip6-agentop-00.txt (work in progress), October 2004.


Authors’ Addresses

Kuntal Chowdhury
Nortel Networks
2221 Lakeside Blvd.
Richardson, TX  75082
US

Phone: +1 972-685-7788
EMail: chowdury@nortelnetworks.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
Intellectual Property Statement

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.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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