           Mobile IPv4 Extension for Carrying Network Access Identifiers

Status of this Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements. Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Abstract

   When a mobile node moves between two foreign networks, it has to be
   re-authenticated. If the home network has both multiple
   Authentication Authorization and Accounting (AAA) servers and Home
   Agents (HAs) in use, the Home AAA server may not have sufficient
   information to process the re-authentication correctly (i.e., to
   ensure that the same HA continues to be used). This document defines
   a Mobile IP extension that carries identities for the Home AAA and HA
   servers in the form of Network Access Identifiers (NAIs). The
   extension allows a Home Agent to pass its identity (and that of the
   Home AAA server) to the mobile node, which can then pass it on to the
   local AAA server when changing its point of attachment. This
   extension may also be used in other situations requiring
   communication of a NAI between Mobile IP nodes.

Table of Contents

1. Introduction

   When building networks one would like to be able to have redundancy.
   In order to achieve this, one might place multiple AAA servers in one
   domain. When a mobile node registers via a visited network, the
   authentication will be handled by one of the AAA servers in the home
   domain. At a later point, when the mobile node moves to another
   visited domain it again has to be authenticated. However, due to the
   redundancy offered by the AAA protocol, it can not be guaranteed that
   the authentication will be handled by the same AAAH server as the
   previous one, which can result in the new AAAH not knowing to which
   HA the session was assigned. This document defines a Mobile IP
   extension which can be used to distribute the information needed to
   resolve this.

   Furthermore, the only information that is normally available about
   the home agent in the registration request is the IP address as
   defined in RFC 3344 [5]. Unfortunately this may not be enough since
   some AAA infrastructures (such as Diameter [6]) use realm based
   routing; such a AAA infrastructure needs to know the FQDN identity of
   the home agent to be able to correctly handle the assignment of the
   home agent. A reverse DNS lookup would only disclose the identity of
   the Mobile IP interface for that HA IP address, which may or may not
   have a one-to-one correspondence with the home agent FQDN identity.
   This is a reason for the HA to also include its own identity in the
   registration reply. The MIP v4 extension defined in this document
   also has a subtype defined by which this may be done. The HA
   identity can then be included by the mobile node in later
   registration requests when changing the point of attachment.

2. Requirements 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 BCP 14, RFC 2119 [1].

   The Mobile IP related terminology described in RFC 3344 [5] is used
   in this document. In addition, the following terms are used:

   AAAH
      One of several possible AAA Servers in the Home Network

   FQDN
      Fully Qualified Domain Name.

   Identity
      The identity of a node is equal to its FQDN.

   NAI
      Network Access Identifier [2].

3. NAI Carrying Extension

   This section defines the NAI Carrying Extension which may be used in
   Mobile IP Registration Request and Reply messages, and also in Mobile
   IP Agent Advertisements [5]. The extension may be used by any node
   that wants to send identity information in the form of a NAI [4].
   This document also defines some subtype numbers which identify the
   specific type of NAI carried in Sections 4 and 5. It is expected
   that other types of NAI will be defined by other documents in the
   future.

```
    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 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |    Length     |   Sub-Type    |   NAI ...
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Type   136 (skippable) [5].

   Length   8-bit unsigned integer. Length of the extension, in
      octets, excluding the extension Type and the extension Length
      fields. This field MUST be set to 1 plus the total length of the
      NAI field.

   Sub-Type This field describes the particular type NAI which is
      carried in the NAI field.

   NAI   Contains the NAI [2] in a string format.

3.1. Processing of the NAI Carrying Extension

   When a mobile node or home agent adds a NAI Carrying Extension to a
   registration message, the extension MUST appear prior to any
   authentication extensions.

In the event the foreign agent adds a NAI Carrying Extension to a
registration message, the extension MUST appear prior to any
authentication extensions added by the FA.

If an HA has appended a NAI Carrying Extension to a Registration
Reply to an MN, and does not receive the NAI extension in subsequent
Registration Request messages from the MN, the HA can assume that the
MN does not understand this NAI extension. In this case, the HA
SHOULD NOT append this NAI extension to further Registration Reply
messages to the MN.

4.   HA Identity subtype

   The HA identity uses subtype 1 of the NAI Carrying Extension. It
   contains the NAI of the HA in the form hostname@realm. Together the
   hostname and realm form the complete FQDN (hostname.realm) of the HA.

   A Home Agent using this extension MUST provide it in the first
   Registration Reply sent to a Mobile Node which is not currently
   registered. The extension only need to be included in subsequent
   Registration Replies if the same extension is included in
   Registration Requests received from the same Mobile Node.

   A mobile node using this extension MUST, if it receives it in a
   registration reply message, provide it in every subsequent
   registration request when re-authentication is needed. Failure to
   re-authenticate, for instance because no AAAH can be reached, will
   result in termination of the Mobile-IP session. Upon initiation of a
   new session a new HA Identity NAI may be provided to the Mobile node,
   and the requirement above will apply to the newly received NAI.

   If the mobile node requires a specific home agent and it has the NAI
   available it MUST provide this extension in its initial registration
   request.

   A foreign agent which receives the Home Agent NAI by this extension
   in a registration request SHOULD include the Home Agent NAI when
   requesting Mobile Node authentication through the AAA infrastructure
   if the AAA protocol used can carry the information.

5.   AAAH Identity subtype

   The AAAH identity uses subtype 2 of the NAI Carrying Extension. It
   contains the NAI of the home AAA server in the form hostname@realm.
   Together the hostname and realm form the complete FQDN
   (hostname.realm) of the home AAA server.

If several AAA servers exist in the Home Network, a Home Agent
providing AAAH selection support according to this document MUST
provide the AAAH identity in the first Registration Reply sent to the
Mobile Node. The extension only needs to be included in subsequent
Registration Replies if the same extension is included in
Registration Requests received from the same Mobile Node.

A mobile node SHOULD save the latest AAAH Identity received in a
registration reply message and SHOULD provide the AAAH Identity in
every registration request sent when re-authenticating, for
efficiency reasons. Failure to reach the indicated AAAH during re-
authentication will result in a new AAAH Identity NAI being returned
(which should then be saved and provided in subsequent registration
requests). Similarly, failure to re-authenticate, for instance
because no AAAH can be reached, will result in termination of the
Mobile-IP session; on initiation of a new session, a new AAAH
Identity NAI may be provided to the Mobile Node for re-use during
later re-registrations.

A foreign agent which receives the AAAH NAI by this extension in a
registration request SHOULD include the AAAH NAI provided when
requesting Mobile Node authentication through the AAA infrastructure
if the AAA protocol used can carry the information.

6. Security Considerations

   This specification introduces new Mobile IP extensions that are used
   to carry mobility agent and AAA server identities, in the form of
   Network Access Identifiers. The Mobile IP messages that carry this
   extension MUST be authenticated as described in [4], unless other
   authentication methods have been agreed upon. Therefore, this
   specification does not lessen the security of Mobile IP messages.

   It should be noted that the identities sent in the extensions
   specified herein MAY be sent in the clear over the network. However,
   the authors do not envision that this information would create
   security issues.

7. IANA Considerations

   This document defines one new mobile IP extension, and one new Mobile
   IP extension sub-type numbering space to be managed by IANA.

   Section 3 defines a new Mobile IP extension, the Mobile IP NAI
   Carrying Extension. The type number for this extension is 136. This
   extension introduces a new sub-type numbering space where the values

1 and 2 have been assigned in this document. Approval of new Mobile
IP NAI Carrying Extension sub-type numbers is subject to Expert
Review, and a specification is required [3].

The content and format for this extension is not specific to AAA
NAIs, so if in the future new NAIs are defined which do not strictly
fall within the category of AAA NAIs, they may nevertheless be
accommodated within the subtype numbering space defined for the NAI
Carrying Extension defined in this document.

The NAI Carrying Extension should be assigned a type value from both
the IANA number space for Mobile IPv4 skippable extensions and from
the IANA number space for Mobile IPv4 advertisement extensions.
Ideally, the numbers assigned from these two numbering spaces should
have the same value.

8. Acknowledgements

Thanks to the original authors of the GNAIE document, Mohamed M
Khalil, Emad Qaddoura, Haseeb Akhtar, and Pat R. Calhoun. The
original document was removed from the MIP WG charter when no use was
seen for the extension. The original ideas have been reused in this
document. Also thanks to Henrik Levkowetz and Kevin Purser for
valuable feedback and help when writing this document.

9. Normative References

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

[2]   Aboba, B. and M. Beadles, "The Network Access Identifier", RFC
      2486, January 1999.

[3]   Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA
      Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[4]   Calhoun, P. and C. Perkins, "Mobile IP Network Access Identifier
      Extension for IPv4", RFC 2794, March 2000.

[5]   Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August
      2002.

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

10. Authors' Addresses

   Fredrik Johansson
   ipUnplugged AB
   Arenavagen 23
   Stockholm S-121 28
   SWEDEN

   Phone: +46 8 725 5916
   EMail: fredrik@ipunplugged.com

   Tony Johansson
   Bytemobile Inc
   2029 Stierlin Court
   Mountain View, CA 94043
   USA

   Phone: +1 650 862 0523
   EMail: tony.johansson@bytemobile.com

11. Full Copyright Statement

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.

Acknowledgement