Network Working Group   K. Chowdhury, Editor
Internet-Draft   Starent Networks
Intended status: Standards Track   A. Yegin
Expires: December 22, 2007   Samsung AIT
                                                   June 20, 2007

            MIP6-bootstrapping for the Integrated Scenario
            draft-ietf-mip6-bootstrapping-integrated-05.txt

Status of this Memo

Copyright Notice

Abstract

   Mobile IPv6 bootstrapping can be categorized into two primary
   scenarios, the split scenario and the integrated scenario. In the
   split scenario, the mobile node's mobility service is authorized by a
   different service authorizer than the network access authorizer. In
   the the integrated scenario, the mobile node's mobility service is
   authorized by the same service authorizer as the network access
   service authorizer. This document defines a method for home agent
   information discovery for the integrated scenario.

Table of Contents

1. Introduction and Scope

   The Mobile IPv6 protocol [RFC3775] requires the mobile node to have
   information of its Home Address, the home agent address and the
   cryptographic materials for establishing an IPsec security
   association with the home agent prior to initiating the registration
   process. The mechanism via which the mobile node obtains these
   information is called Mobile IPv6 bootstrapping. In order to allow a
   flexible deployment model for Mobile IPv6, it is desirable to define
   a bootstrapping mechanism for the mobile node to acquire these
   parameters dynamically. [RFC4640] describes the problem statement
   for Mobile IPv6 bootstrapping. It also defines two bootstrapping
   scenarios based on the relationship between the entity that
   authenticates and authorizes the mobile node for network access
   (i.e., the Access Service Authorizer) and the entity that
   authenticates and authorizes the mobile node for mobility service
   (i.e., the Mobility Service Authorizer). The scenario in which the
   Access Service Authorizer is not the Mobility Service Authorizer is
   called the "Split" scenario. The bootstrapping solution for split
   scenario is defined in [BOOT-SPLIT]. The scenario in which the
   Access Service Authorizer is also the Mobility Service Authorizer is
   called the "Integrated" scenario. This document defines a
   bootstrapping solution for the Integrated scenario.

   [BOOT-SPLIT] identifies four different components of the
   bootstrapping problem: home agent address discovery, HoA assignment,
   IPsec Security Association setup and Authentication and Authorization
   with the MSA. This document defines a mechanism for home agent
   address discovery. The other components of bootstrapping are as per
   [BOOT-SPLIT].

   In the integrated scenario, the bootstrapping of the home agent
   information can be achieved via DHCPv6. This document defines the
   mip6 bootstrapping procedures for the integrated scenario. It
   enables Home Agent assignment in the integrated scenario by utilizing
   DHCP and AAA protocols. The specification utilizes DHCP and AAA
   options and AVPs that are defined in [HIOPT], [MIP6-Dime], and
   [MIP6-RADIUS]. This document specifies the interworking among MN,
   NAS, DHCP, and AAA entities for bootstrapping procedure in the
   integrated scenario.

2. **Terminology**

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in RFC 2119.

   General mobility terminology can be found in [RFC3753]. The
   following additional terms, as defined in [RFC4640], 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. A MSP is called home MSP when MSP == MSA. In
   this document the term MSP means a Mobility Service Provider that has
   roaming relationship with the MSA but it is not the MSA.

   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. Assumptions & Conformance

The following assumptions are made in this document:

a.   MSA == ASA.

b.   MSA and MSP roaming relationship is assumed but not required.

c.   DHCP relay and NAS are collocated or there is a mechanism to
transfer received AAA information from the NAS to the DHCP relay.

Note: if assignment of home agent in the home MSP is not required by
a deployment, collocation of the NAS and the DHCP relay functions or
a mechanism to transfer received AAA information from the NAS to the
DHCP relay won't be necessary. In such a case, only the
implementation of the options and procedures defined in [HIOPT]
should suffice.

d. the NAS shall support MIPv6 specific AAA attributes as specified
in [MIP6-RADIUS] and [MIP6-Dime].

e.   The AAAH used for network access authentication (ASA) has access
to the same database as the AAAH used for the mobility service
authentication (MSA).

If home agent assignment only in the ASP is required by the
deployment, a minimal implementation of this specification MAY only
support the delivery of information from the DHCP server to the DHCP
client through [HIOPT]. However, if home agent assignment in the MSP
is required by the deployment, the implementation conforming to this
specification SHALL be able to transfer received information (from
the AAA server) from the NAS to the DHCP relay function. This can be
achieved either by collocating the NAS and the DHCP relay functions
or via an interface between these functions. The detail of this
interface is out of scope of this specification.

4. Solution Overview

4.1. Logical View of the Integrated Scenario

   In the integrated scenario the mobile node utilizes network access
   authentication process to bootstrap Mobile IPv6. It is assumed that
   the access service authorizer is mobility service aware. This allows
   for Mobile IPv6 bootstrapping at the time of access authentication
   and authorization. Also, the mechanism defined in this document
   requires the NAS to support Mobile IPv6 specific AAA attributes and a
   collocated DHCP relay agent.

   The following diagram shows the network elements and layout in the
   integrated scenario:

```
                                     |
              ASP(/MSP)              |     ASA/MSA(/MSP)
                                     |
                                     |
              +-------+              |          +-------+
              |       |              |          |       |
              |AAAV   |--------------|--------|AAAH    |
              |       |              |          |       |
              |       |              |          |       |
              +-------+              |          +-------+
                  |                  |
                  |                  |
                  |                  |
                  |                  |
                  |                  |
                  |                  |
                  |                  |
              +-----+    +------+ |
      +----+      |     |    |DHCP  | |
      | MN |------| NAS/|----|Server| |
      +----+      |Relay|    |      | |
              +-----+    +------+ |
                                     |
                                     |
              +--------+             |     +--------+
              | HA     |             |     | HA     |
              | in ASP |             |     |in MSP  |
              +--------+             |     +--------+
```
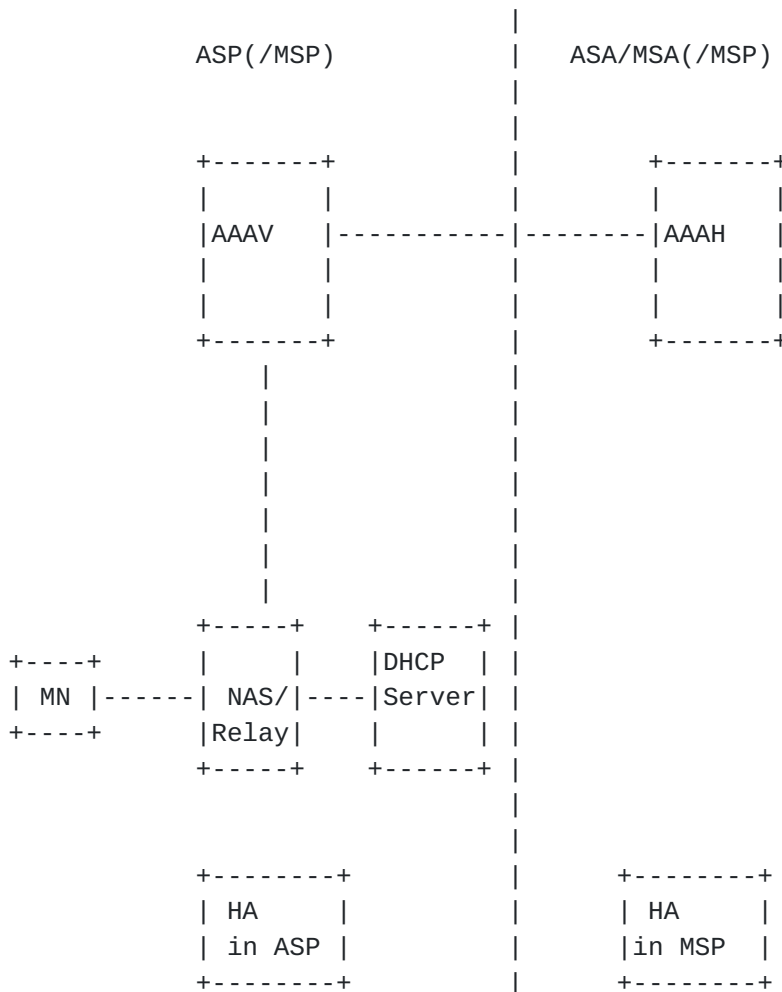
Integrated Scenario, Network Diagram with DHCP Server

Figure 1. Integrated Scenario, Network Diagram with DHCP

Figure 1 shows the AAA infrastructure with a AAA client (NAS), a AAA
proxy in the visited network and a AAA server in the home network.
The user's home network authorizes the mobile node for network access
and also for mobility services. Note that a home agent for usage
with the mobile node might be selected in the access service
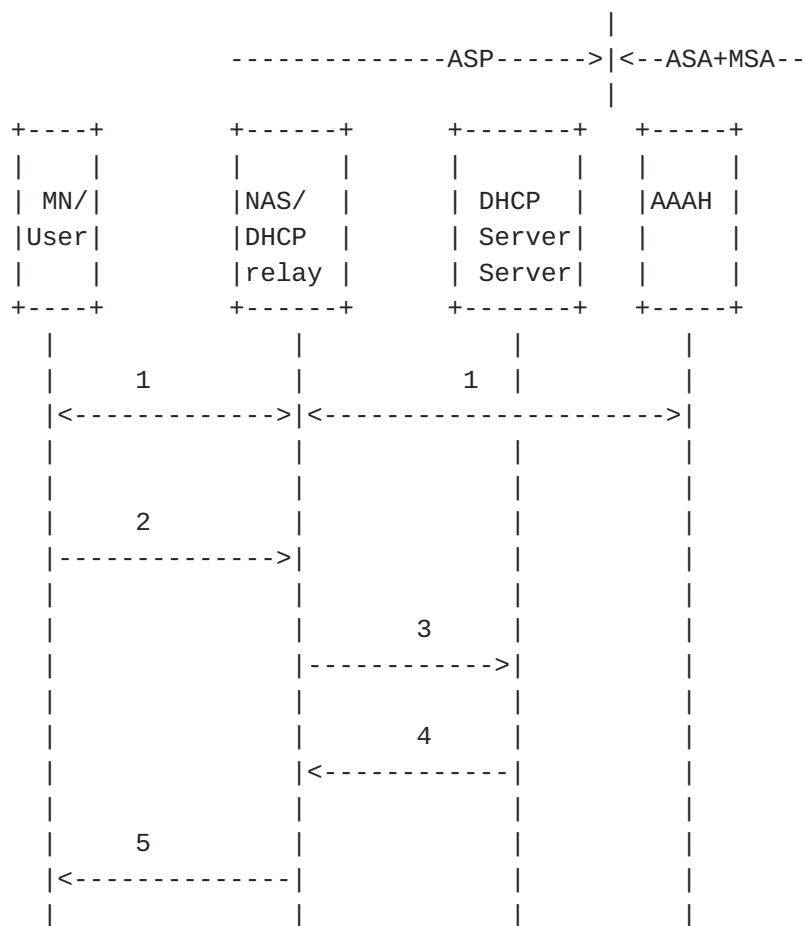provider's network or alternatively in the mobility service
provider's network.

The mobile node interacts with the DHCP Server via the Relay Agent
after the network access authentication as part of the mobile node
configuration procedure.

4.2. Bootstrapping Message Sequence

In this case, the mobile node is able to acquire the home agent
address via a DHCPv6 query. The message flows for home agent
allocation in the ASP and the MSP are illustrated below. In the
integrated scenario, the ASA and the MSA are the same, it can be
safely assumed that the AAAH used for network access authentication
(ASA) has access to the same database as the AAAH used for the
mobility service authentication (MSA). Hence, the same AAAH can
authorize the mobile node for network access and mobility service at
the same time. When the MN performs Mobile IPv6 registration, the
AAAH ensures that the MN is accessing the assigned Home Agent for
that MSP.

4.2.1. Home Agent allocation in the MSP

This section describes a scenario where the home agent is allocated
in the mobile node's MSP network(s). in order to provide the mobile
node with information about the assigned home agent the AAAH conveys
the assigned home agent's information to the NAS via AAA protocol
[MIP6-RADIUS] or [MIP6-Dime].

```
                                |
                 --------------ASP------>|<--ASA+MSA--
                                |
   +----+         +------+        +-------+   +-----+
   |    |         |      |        |       |   |     |
   | MN/|         |NAS/  |        | DHCP  |   |AAAH |
   |User|         |DHCP  |        | Server|   |     |
   |    |         |relay |        | Server|   |     |
   +----+         +------+        +-------+   +-----+
     |               |               |           |
     |       1       |          1    |           |
     |<------------->|<---------------------->|
     |               |               |           |
     |               |               |           |
     |       2       |               |           |
     |-------------->|               |           |
     |               |               |           |
     |               |       3       |           |
     |               |------------>|           |
     |               |               |           |
     |               |       4       |           |
     |               |<------------|           |
     |               |               |           |
     |       5       |               |           |
     |<--------------|               |           |
     |               |               |           |
```

                      Home Agent in the MSP

    Figure 2. The home agent allocation in the MSP

    Figure 2 shows the message sequence for home agent allocation in the
    MSP.

    (1) The mobile node executes the network access authentication
    procedure (e.g., IEEE 802.11i/802.1X) and it interacts with the NAS.
    The NAS is in the ASP and it interacts with the AAAH, which is in the
    ASA/MSA, to authenticate the mobile node. In the process of
    authorizing the mobile node the AAAH verifies in the AAA profile that
    the mobile node is allowed to use Mobile IPv6 service. The AAAH
    assigns home agent in the home MSP and other authorized MSPs and
    returns this information to the NAS. The NAS may keep the received
    information for a configurable duration or it may keep the
    information for as long as the MN is connected to the NAS.

    (2) The mobile node sends a DHCPv6 Information Request message
    [RFC3315] to the All_DHCP_Relay_Agents_and_Servers multicast address.

In this message the mobile node (DHCP client) SHALL include the
Option Code for Home Network Identifier Option [HIOPT] in the
OPTION_ORO, Home Network Identifier Option with id-type set to 1 and
the Home Network Identifier field set to the network realm of the
home MSP [HIOPT]. The mobile node SHALL also include the
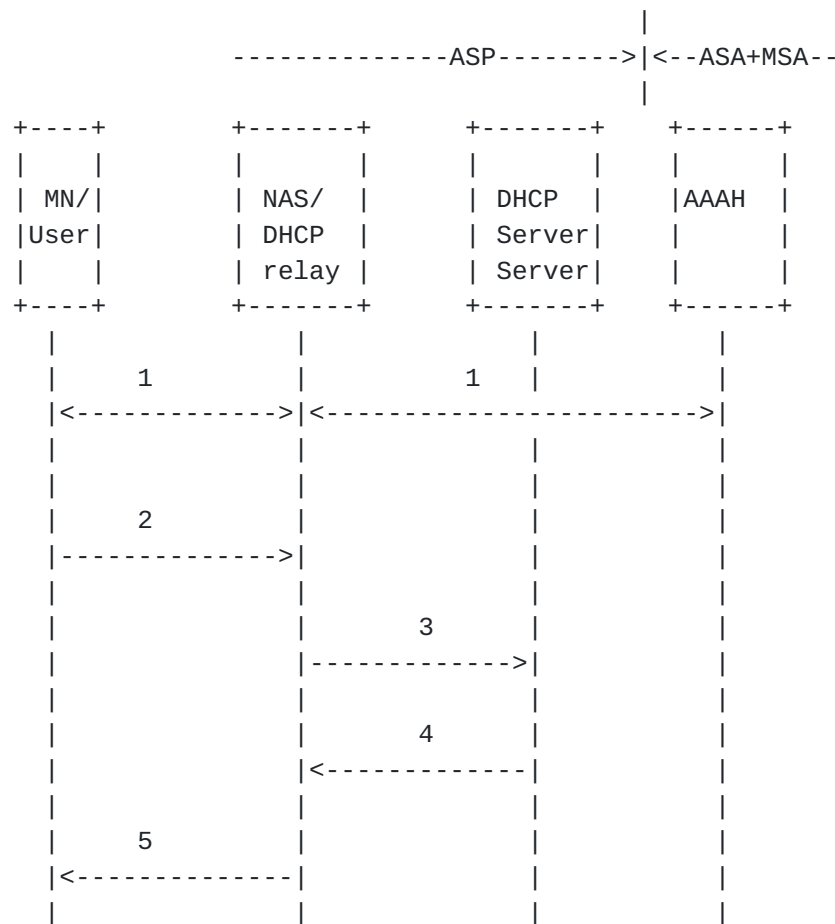OPTION_CLIENTID to identify itself to the DHCP server.

(3) The Relay Agent intercepts the Information Request from the
mobile node and forwards it to the DHCP server. The Relay Agent also
includes the received home agent information from the AAAH in the
OPTION_MIP6-RELAY-Option [HIOPT]. If a NAS implementation does not
store the received information as long as the MN's session remains in
the ASP, and if the MN delays sending DHCP request, the NAS/DHCP
relay does not include the OPTION_MIP6-RELAY-Option in the Relay
Forward message.

(4) The DHCP server identifies the client by looking at the DUID for
the client in the OPTION_CLIENTID. The DHCP server also determines
that the mobile node is requesting home agent information in the MSP
by looking at the Home Network Identifier Option (id-type 1). The
DHCP server determines that the home agent is allocated by the AAAH
by looking at the MIP6 home agent sub-option in the OPTION_MIP6-
RELAY-Option. The DHCP server extracts the allocated home agent
information from the OPTION_MIP6-RELAY-Option and includes it in the
Home Network Information Option [HIOPT] in the Reply Message. If the
requested information is not available in the DHCP server, it follows
the behavior described in [HIOPT].

(5) The Relay Agent relays the Reply Message from the DHCP server to
the mobile node. At this point, the mobile node has the home agent
information that it requested.

4.2.2. Home Agent allocation in the ASP

This section describes a scenario where the mobile node requests for
home agent allocation in the ASP by setting the id-type field to zero
in the Home Network Identifier Option [HIOPT] in the DHCPv6 request
message. In this scenario, the ASP becomes the MSP for the duration
of the network access authentication session.

```
                                   |
                  --------------ASP-------->|<--ASA+MSA--
                                   |
     +----+          +-------+        +-------+      +------+
     |    |          |       |        |       |      |      |
     | MN/|          | NAS/  |        | DHCP  |      |AAAH  |
     |User|          | DHCP  |        | Server|      |      |
     |    |          | relay |        | Server|      |      |
     +----+          +-------+        +-------+      +------+
       |                 |                |             |
       |       1         |                1  |          |
       |<------------->|<------------------------------>|
       |                 |                |             |
       |                 |                |             |
       |       2         |                |             |
       |-------------->|                |             |
       |                 |                |             |
       |                 |        3       |             |
       |                 |-------------->|             |
       |                 |                |             |
       |                 |        4       |             |
       |                 |<-------------|             |
       |                 |                |             |
       |       5         |                |             |
       |<-------------|                |             |
       |                 |                |             |
```

                    Home Agent in the ASP

   Figure 3. The home agent allocation in the ASP

   Figure 3 shows the message sequence for home agent allocation in the
   ASP.

   (1) The mobile node executes the network access authentication
   procedure (e.g., IEEE 802.11i/802.1X) and it interacts with the NAS.
   The NAS is in the ASP and it interacts with the AAAH, which is in the
   ASA/MSA, to authenticate the mobile node. In the process of
   authorizing the mobile node the AAAH verifies in the AAA profile that
   the mobile node is allowed to use Mobile IPv6 services. The AAAH
   assigns a home agent in the home MSP and returns this information to
   the NAS. Note that the AAAH is not aware of the fact that the mobile
   node prefers a home agent allocation in the ASP. Therefore the
   assigned home agent may not be used by the mobile node. This leaves
   the location of the mobility anchor point decision to the mobile
   node.

(2) The mobile node sends a DHCPv6 Information Request message
[RFC3315] to the All_DHCP_Relay_Agents_and_Servers multicast address.
In this message the mobile node (DHCP client) SHALL include the
Option Code for Home Network Identifier Option [HIOPT] in the
OPTION_ORO, Home Network Identifier Option with id-type set to 0.
The mobile node SHALL also include the OPTION_CLIENTID to identify
itself to the DHCP server.

(3) The Relay Agent intercepts the Information Request from the
mobile node and forwards it to the DHCP server. The Relay Agent
(which is the NAS) also includes the received AAA AVP from the AAAH
in the OPTION_MIP6-RELAY-Option [HIOPT].

(4) The DHCP server identifies the client by looking at the DUID for
the client in the OPTION_CLIENTID. The DHCP server also determines
that the mobile node is requesting home agent information in the ASP
by looking at the Home Network Identifier Option (id-type 0). If
configured to do so, the DHCP server allocates an home agent from its
configured list of home agents and includes it in the Home Network
Information Option [HIOPT] in the Reply Message. Note that in this
case, the DHCP server does not use the received information in the
OPTION_MIP6-RELAY-Option.

(5) The Relay Agent relays the Reply Message from the DHCP server to
the mobile node. At this point, the mobile node has the home agent
information that it requested.

4.3. Bootstrapping Message Sequence: Fallback case

In the fallback case, the mobile node is not able to acquire the home
agent information via DHCPv6. The mobile node MAY perform DNS
queries to discover the home agent address as defined in
[BOOT-SPLIT]. To perform DNS based home agent discovery, the mobile
node needs to know the DNS server address. The details of how the MN
is configured with the DNS server address is outside the scope of
this document.

4.4. HoA and IKEv2 SA Bootstrapping in the Integrated Scenario

In the integrated scenario, the HoA, IPsec Security Associations
setup, and Authentication and Authorization with the MSA are
bootstrapped via the same mechanism as described in the bootstrapping
solution for split scenario [BOOT-SPLIT].

5. Security Considerations

   The transport of the assigned home agent information via the AAA
   infrastructure (i.e., from the AAA server to the AAA client) to the
   NAS may only be integrity protected as per standard RADIUS and
   Diameter security mechanisms. No additional security considerations
   are imposed by the usage of this document. The security mechanisms
   provided by [RFC2865] and [RFC3588] are applicable for this purpose.
   This document does not introduce any new security issues to Mobile
   IPv6.

6. IANA Considerations

   None

[7](). Acknowledgements

   The authors would like to thank Kilian Weniger, Vidya Narayanan, and
   George Tsirtsis for their review and comments.

[8](#). Contributors

This contribution is a joint effort of the bootstrapping solution
design team of the MIP6 WG. The contributors include Gerardo
Giaretta, Basavaraj Patil, Alpesh Patel, Jari Arkko, James Kempf,
Gopal Dommety, Alper Yegin, Junghoon Jee, Vijay Devarapalli, Kuntal
Chowdhury, Julien Bournelle, and Hannes Tschofenig.

The design team members can be reached at:

Gerardo Giaretta gerardog@qualcomm.com

Basavaraj Patil basavaraj.patil@nsn.com

Alpesh Patel alpesh@cisco.com

Jari Arkko jari.arkko@kolumbus.fi

James Kempf kempf@docomolabs-usa.com

Gopal Dommety gdommety@cisco.com

Alper Yegin a.yegin@partner.samsung.com

Junghoon Jee jhjee@etri.re.kr

Vijay Devarapalli Vijay.Devarapalli@AzaireNet.com

Kuntal Chowdhury kchowdhury@starentnetworks.com

Julien Bournelle julien.bournelle@orange-ftgroup.com

Hannes Tschofenig hannes.tschofenig@nsn.com

9. References

9.1. Normative References

   [BOOT-SPLIT]
               Giaretta et. al., A., "Mobile IPv6 bootstrapping in split
               scenario.", draft-ietf-mip6-bootstrapping-split-05.txt
               (work in progress), May 2007.

   [HIOPT]   Hee Jang et. al., A., "DHCP Option for Home Agent
               Discovery in MIPv6.", draft-ietf-mip6-hiopt-03.txt (work
               in progress), May 2007.

   [MIP6-Dime]
               Korhonen et. al., J., "Diameter Mobile IPv6: NAS - HAAA
               Support.", draft-ietf-dime-mip6-integrated-04.txt (work in
               progress), May 2007.

   [MIP6-RADIUS]
               Chowdhury et. al., K., "RADIUS Mobile IPv6 Support.",
               draft-ietf-mip6-radius-02.txt (work in progress),
               March 2007.

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

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

   [RFC3315]   Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C.,
               and M. Carney, "Dynamic Host Configuration Protocol for
               IPv6 (DHCPv6)", RFC 3315, July 2003.

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

   [RFC3775]   Johnson, D., Perkins, C., and J. Arkko, "Mobility Support
               in IPv6", RFC 3775, June 2004.

9.2. Informative References

   [RFC3753]   Manner, J. and M. Kojo, "Mobility Related Terminology",
               RFC 3753, June 2004.

   [RFC4640]   Patel, A. and G. Giaretta, "Problem Statement for
               bootstrapping Mobile IPv6 (MIPv6)", RFC 4640,
               September 2006.

Authors' Addresses

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

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

    Alper Yegin
    Samsung AIT
    Istanbul,
    Turkey

    Phone:
    Email: a.yegin@partner.samsung.com

Full Copyright Statement

Intellectual Property

Acknowledgment