Internet Engineering Task Force (IETF)
Request for Comments: 6611
Category: Standards Track
ISSN: 2070-1721

K. Chowdhury, Ed.
Radio Mobile Access, Inc.
A. Yegin
Samsung

May 2012

Mobile IPv6 (MIPv6) Bootstrapping for the Integrated Scenario

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 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.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6611.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction and Scope 2
2. Terminology 3
3. Assumptions and Conformance 4
4. Solution Overview 5
   4.1. Logical View of the Integrated Scenario 5
   4.2. Bootstrapping Message Sequence 6
        4.2.1. Home Agent Allocation in the MSP 7
        4.2.2. Home Agent Allocation in the ASP 9
   4.3. Bootstrapping Message Sequence: Fallback Case 10
   4.4. HoA and IKEv2 SA Bootstrapping in the Integrated Scenario 10
5. Security Considerations 10
6. Acknowledgements 11
7. Contributors 11
8. References 11
   8.1. Normative References 11
   8.2. Informative References 12

1. Introduction and Scope

The Mobile IPv6 protocol [RFC6275] requires the mobile node to have the following information:

- the Home Address (HoA),

- the home agent address, and

- the cryptographic materials for establishing an IPsec security association with the home agent.

The cryptographic materials need to be established prior to initiating the registration process. The mechanism via which the mobile node obtains this 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 the 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, ASA) and the entity that authenticates and authorizes the mobile node for mobility service (i.e., the Mobility Service Authorizer, MSA). The scenario in which the Access Service Authorizer is not the Mobility Service Authorizer is called the "split" scenario. The bootstrapping solution for the split scenario is defined in [RFC5026]. 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.

[RFC5026] identifies four different components of the bootstrapping problem: home agent address discovery, HoA assignment, IPsec Security Association [RFC4301] 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 [RFC5026].

In the integrated scenario, the bootstrapping of the home agent information can be achieved via DHCPv6. This document defines the MIPv6 bootstrapping procedures for the integrated scenario. It enables home agent assignment in the integrated scenario by utilizing DHCP and Authentication, Authorization, and Accounting (AAA) protocols. The specification utilizes DHCP and AAA options and attribute-value pairs (AVPs) that are defined in [RFC6610] and [RFC5447]. This document specifies the interworking among Mobile Node (MN), Network Access Server (NAS), DHCP, and AAA entities for the 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 [RFC2119].

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. An MSP is called a "home MSP" when MSP == MSA. In this document, the term MSP means a Mobility Service Provider that has a 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 and Conformance

The following assumptions are made in this document:

(a) MSA == ASA.

(b) MSA and MSP have a roaming relationship.

(c) DHCP relay and NAS are either co-located or there is a mechanism to transfer received AAA information from the NAS to the DHCP relay.

> Note: If assignment of a home agent in the home MSP is not required by a deployment, co-location 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 [RFC6610] should suffice.

(d) The NAS shall support MIPv6-specific AAA attributes as specified in [RFC5447].

(e) The AAA server in the home domain (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 is required only in the ASP 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 [RFC6610]. However, if home agent assignment in the MSP is required by the deployment, an implementation conforming to this specification SHALL be able to transfer the information received from the AAA server to the NAS, and from the NAS to the DHCP relay function. This can be achieved either by co-locating the NAS and the DHCP relay functions or via an interface between these functions. The details of this interface are out of the scope of this specification.

4. Solution Overview

4.1. Logical View of the Integrated Scenario

In the integrated scenario, the mobile node utilizes the 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 MIP6-specific AAA attributes and a co-located DHCP relay agent.

Figure 1 shows the AAA infrastructure with a AAA client (NAS), a AAA proxy in the visited network (AAAV), and a AAA server in the home network (AAAH).

```
                                      |
                  ASP(/MSP)           |   ASA/MSA(/MSP)
                                      |
                                      |
                  +-------+           |        +-------+
                  |       |           |        |       |
                  |AAAV   |-----------|--------|AAAH   |
                  |       |           |        |       |
                  +-------+           |        +-------+
                      |               |
                      |               |
                      |               |
                      |               |
                  +-----+    +------+ |
      +----+      | NAS/|    |DHCP  | |
      | MN |------|DHCP |----|Server| |
      +----+      |Relay|    |      | |
                  +-----+    +------+ |
                                      |
                                      |
                  +--------+          |      +--------+
                  | HA     |          |      | HA     |
                  | in ASP |          |      |in MSP  |
                  +--------+          |      +--------+
```

Figure 1: Integrated Scenario, Network Diagram with DHCP Server

The user's home network authorizes the mobile node for network access and mobility services. Note that usage of a home agent with the mobile node might be selected in the access service provider's network or alternatively in the mobility service provider's network.

The MSP may be co-located with the ASP, or the ASA/MSA, or independent of the two.

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. 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.

Figure 2 shows the message sequence for home agent allocation in both scenarios -- HA in the ASP (which is co-located with the MSP), or HA in an MSP that is separate from ASP and possibly from the ASA/MSA as well.

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

Figure 2: Message Sequence for Home Agent Allocation

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) that is (are) not co-located with the ASP. 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 a AAA protocol, e.g., [RFC5447].

Figure 2 shows the message sequence for home agent allocation. In the scenario with HA in the MSP, the following details apply.

(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 the Mobile IPv6 service. The AAAH assigns a home agent in the home MSP, and it assigns one or more home agents in 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 following:

- the Option Code for the Visited Home Network Information option [RFC6610] in the OPTION_ORO.
- Client Home Network ID FQDN option identifying the MSP.
- 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 Relay-Supplied Options option [RFC6610]. 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 a DHCP request, the NAS/DHCP relay does not include the Relay-Supplied Options option in the Relay Forward message.

(4) The DHCP server:

- identifies the client by looking at the DHCP Unique Identifier (DUID) for the client in the OPTION_CLIENTID.
- determines that the mobile node is requesting home agent information in the MSP by looking at the Home Network ID FQDN option.
- determines that the home agent is allocated by the AAAH by looking at the Relay-Supplied Options option.

   - extracts the allocated home agent information from the Relay-Supplied Options option and includes it in the Identified Home Network Information option [RFC6610] in the Reply Message. If the requested information is not available in the DHCP server, it follows the behavior described in [RFC6610].

(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 home agent allocation in the ASP by setting the id-type field to zero in the Home Network Identifier Option [RFC6610] in the DHCPv6 request message. In this scenario, the ASP becomes the MSP for the duration of the network access authentication session.

Figure 2 shows the message sequence for home agent allocation. In the scenario with HA in the ASP, the following details apply.

(1) The mobile node executes the network access authentication procedure (e.g., IEEE 802.11i/802.1X) and 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 the Mobile IPv6 services. The AAAH assigns a home agent in the home MSP, and it assigns one or more home agents in other authorized MSPs 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 following:

   - the Option Code for the Home Network Identifier Option [RFC6610] in the OPTION_ORO.

   - the OPTION_CLIENTID to identify itself to the DHCP server.

(3) The relay agent (which is the NAS) intercepts the Information Request from the mobile node and forwards it to the DHCP server. The relay agent also includes the received AAA AVP from the AAAH in the Relay-Supplied Options option [RFC6610].

(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 Visited Home Network Information option. If configured to do so, the DHCP server allocates a home agent from its configured list of home agents and includes it in the Visited Home Network Information Option [RFC6610] in the Reply Message. Note that in this case, the DHCP server does not use the received information in the Relay-Supplied Options 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 [RFC5026]. 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 are 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 Association setup, and Authentication and Authorization with the MSA are bootstrapped via the same mechanism as described in the bootstrapping solution for the split scenario [RFC5026].

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 Diameter or other AAA protocol security mechanisms. No additional security considerations are imposed by the usage of this document. The security mechanisms provided by [RFC3588] are applicable for this purpose. This document does not introduce any new security issues to Mobile IPv6.

6. Acknowledgements

The authors would like to thank Kilian Weniger, Vidya Narayanan, and George Tsirtsis for their review and comments. Thanks to Alfred Hoenes for thorough review and valuable suggestions to improve the readability of the document.

7. Contributors

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

The design team members can be reached at the following email addresses:

Jari Arkko	jari.arkko@kolumbus.fi
Julien Bournelle	julien.bournelle@orange-ftgroup.com
Kuntal Chowdhury	kc@radiomobiles.com
Vijay Devarapalli	Vijay.Devarapalli@AzaireNet.com
Gopal Dommety	dommety@yahoo.com
Gerardo Giaretta	gerardog@qualcomm.com
Junghoon Jee	jhjee@etri.re.kr
James Kempf	kempf@docomolabs-usa.com
Alpesh Patel	alpesh@cisco.com
Basavaraj Patil	basavaraj.patil@nsn.com
Hannes Tschofenig	hannes.tschofenig@nsn.com
Alper Yegin	alper.yegin@yegin.org

8. References

8.1. Normative References

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

[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.

[RFC5026] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[RFC5447] Korhonen, J., Bournelle, J., Tschofenig, H., Perkins, C., and K. Chowdhury, "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction", RFC 5447, February 2009.

[RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC6610] Jang, H., Yegin, A., Chowdhury, K., Choi, J., and T. Lemon, "DHCP Option for Home Agent Discovery in Mobile IPv6 (MIPv6)", RFC 6610, May 2012.

8.2. Informative References

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

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

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

Authors' Addresses

Kuntal Chowdhury (editor)
Radio Mobile Access, Inc.
100 Ames Pond Dr.
Tewksbury MA 01876

EMail: kc@radiomobiles.com

Alper Yegin
Samsung
Istanbul
Turkey

EMail: alper.yegin@yegin.org