Network Working Group
Internet-Draft
Expires: December 28, 2006

J. Bournelle (Ed.)
M. Laurent-Maknavicius
GET/INT
J-M. Combes
France Telecom R&D
June 26, 2006

Using PANA in the Mobile IPv6 Integrated Case
draft-bournelle-pana-mip6-01

Status of this Memo

Copyright Notice

Abstract

A Mobile IPv6 node needs a home address, a home agent address and a security association with its home agent. One of the current challenge is to dynamically provide these information to the Mobile Node. This problem is known as the Mobile IPv6 Bootstrapping problem. A solution for this is to rely on the AAA infrastructure to provide the Home Agent Information to the Network Access server

(NAS). Then the Mobile Node uses DHCPv6 to get this information. This document provides a way for the Mobile Node to get the Home Agent information by using the PANA protocol instead of DHCPv6.

Before the authentication phase, the PANA Authentication Agent (PAA) indicates to the PANA Client (PaC) that it can provide him with the Home Agent Information. According to the PANA client's response, after the authentication and authorization phase with the AAA infrastructure, the PAA will send this information to the PaC.

Table of Contents

1. Introduction

One of the major issue of Mobile IPv6 [1] is currently the bootstrapping problem. Indeed, a mobile node needs a home address, a home agent address and a security association with its home agent to register. The problem is to find a way for the mobile to get those information.

The document [5] describes various deployment scenarios. In particular, it makes a clear distinction between the Access Service Provider (ASP) and the Mobility Service Provider (MSP). Both can be integrated in a Integrated Access Service Provider (IASP).

In the integrated scenario [2], the home AAA server is in charge of allocating a Home Agent to the MN. This Home Agent information is carried in the AAA protocol from the AAA server to the NAS. Then the Mobile Node uses DHCPv6 to get the HA information.

In this document, we propose to use the Protocol for carrying Authentication Network Access (PANA) insted of DHCPv6. For this, we describe what should be added to the current PANA specification and the related operations. This solution suppose that we are in the IASP scenario.

2. Terminology and Definitions

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 [3].

The MIPv6 bootstrapping terminology is taken from [5].

This document also uses the following terms or abbreviations:
PANA Protocol for Carrying Network Authentication for Network Access.

PANA Client (PaC) A mobile node (MN) using a PANA protocol implementation to authenticate itself to the network.

PAA The PANA Authentication Agent (PAA) is the entity responsible to verify the credentials provided by the PANA client. It is also responsible of granting network access.

HA The home agent is a Mobile IPv6 device. It is a router in charge of delivering IPv6 packets addressed to the home address of the mobile node.

3. PANA overview

PANA [4]is a protocol that carries EAP over IP/UDP to authenticate users. The PAA (PANA Authentication Agent) is the endpoint of the PANA protocol at the access network. The PAA itself might not be able to authenticate the user by terminating the EAP protocol. Instead the PAA might forward the EAP payloads to the backend AAA infrastructure.

The Enforcement Point (EP) is an entity which enforces the result of the PANA protocol exchange. The EP might be co-located with the PAA or separated as a stand-alone device.

A successful EAP authentication exchange results in a PANA security association (PANA SA) if the EAP method was able to derive session keys. In this case, all further PANA messages between PaC and PAA will be authenticated, replay and integrity protected thanks to the MAC AVP.

4. The Mobile IPv6 Bootstrapping Integrated scenario

This section is extracted from [6].

In the integrated scenario [2], the assumption is that the IPv6 mobility service is authorized by the same authorizer than network access service. Basically Mobility Service Authorizer (MSA) and the Access Service Authorizer (ASA) are the same entity. The scenario considers two cases:

1. Mobile Node requests a home agent to its home domain (ASA/MSA).

2. Mobile Node requests a home agent to the Access Service Provider (ASP)

In the first case, Home Agent is allocated by user's home domain. In the second case it is allocated by user's visited domain. In both cases, it is assumed that the AAA server in the home domain (AAAH) authorizes both network access service and mobility service.

In this scenario, Mobile Node discovers the Home Agent Address using DHCPv6. During network access service authentication and authorization, AAAH also verifies if authenticating user is authorized to use mobility service. In affirmative case, AAAH sends to the Network Access Server (NAS) where the Mobile Node is attached, the information about the assigned home agent. Then NAS stores that information. To request home agent data, Mobile Node sends a DHCPv6 Information Request to the All_DHCP_Relay_Agents_and_Servers

multicast address. With this request, Mobile Node can specify if it wants a home agent provided by the visited domain (ASP) or by the home domain (ASA). In both cases, the NAS acts a DHCPv6 relay. When the NAS receives DHCPv6 Information Request then it attaches home agent information received from AAAH in a new DHC Relay Agent Option.

In case Mobile Node cannot acquire home agent information via DHCPv6, it can try the default mechanism based on DNS described in [7]. After the Mobile Node has acquired home agent information, the mechanism used to bootstrap the HoA, IPsec Security Association, and Authentication and Authorization with the MSA is the same described in the bootstrapping solution for split scenario [7].

5. Using PANA instead of DHCPv6

The goal of this document is to provide a way for the MN to acquire the Home Agent Information through PANA messages instead of relying on DHCPv6.

For this purpose, the PAA indicates to the PaC/MN that it can provide him with a Home Agent. This is realized during the PANA-Start

exchange. The PAA adds a Mobility-Capability AVP (To Be Allocated) in the PANA-Start-Request message which indicates what type of Mobility Agents it can provide. The PaC replies with a PSA message which will contain its answer to this proposal in the Mobility-Capability AVP. If the PaC requires a Home Agent, the PAA adds the Home Agent information in the PANA-Bind exchange. This Home-Agent information is received by the PAA from the AAA infrastructure (cf. [8] and [9]). After this negotiation, the MN/PaC falls back in the split scenario case [7].

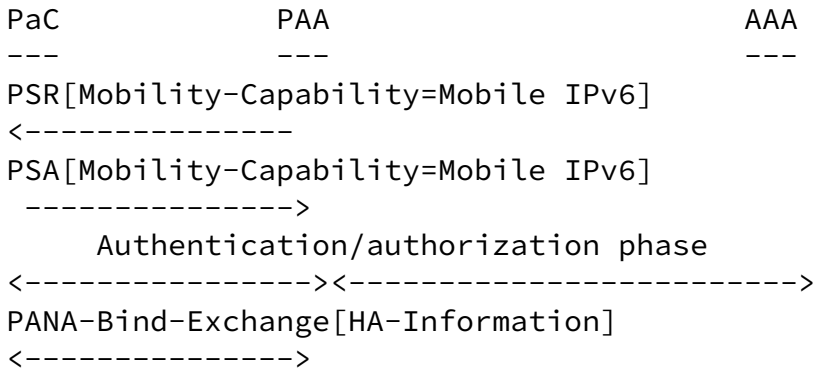

Figure 1: PANA for Mobile IPv6 bootstrapping

If the PaC/MN does not support this specification or does not need a Home Agent, it simply ignore the Mobility-Capability AVP. In this

case, the PAA should not provide the Home Agent Information in the PANA-Bind-Exchange.

6. Advantages of using PANA instead of DHCPv6

One of the advantage of this proposal is that in a PANA-Based network access, this proposal avoids to use DHCPv6 to get the HA information.

The other advantage is that the HA-Information is naturally Integrity protected thanks to the AUTH AVP.

7. New AVPs

7.1. Mobility-Capability AVP

The Mobility-Capability AVP (AVP Code TBD) is of type Unsigned 32 and contains the type of Mobility Agent that the PAA can provide to the PaC/MN. This AVP is also used by the PaC/MN to indicates its need. Below is a list of valid data values and associated Mobility Agent:

1. IPv6 Home Agent

The support of this AVP is not required. For this reason, the 'M' bit MUST NOT be set.

[Editor's Note: it is left for further study if other mobility agents could be provided by this proposal (e.g. IPv4 HA, HIP rendez-vous server)]

7.2. Home Agent related AVPs

The two AVPs presented below are extracted from [8]. These AVPs can be reused by the PAA to provide HA information to the PaC. These AVPs must be included in the PANA-Bind-Request message.

7.2.1. MIP6-Home-Agent-Address AVP

The MIP6-Home-Agent-Address AVP (AVP Code TBD) is of type OctetString and contains the Mobile IPv6 home agent address and the prefix length of the said address. The AVP is a discriminated union, representing IPv6 address in network byte order. The first two octets of this AVP represents the home link prefix length followed by 16 octets of the IPv6 address.

The Diameter server MAY decide to assign a MIPv6 home agent to the MN that is in close proximity to the point of attachment (e.g.

determined by the NAS-Identifier). There may be other reasons for dynamically assigning home agents to the MN, for example to share the traffic load. The AVP also contains the prefix length so that the MN can easily infer one of the possible Home Link prefixes from the home agent address.

7.2.2. MIP6-Home-Agent-FQDN AVP

The MIP6-Home-Agent-FQDN AVP (AVP Code TBD) is of type UTF8String and contains the FQDN of a Mobile IPv6 home agent.

8. Security Considerations

The Home Agent Information may be a sensitive information from an operator's perspective. This proposal permits to provide integrity to the Home Agent Information since the PANA-Bind exchange can be protected by the AUTH AVP.

9. IANA Considerations

This document defines a new AVP:

Mobility-Capability	is set to TBD

10. Acknowledgements

The authors would like to thanks Junghoon Jee, Sondes Larafa and Hannes Tschofenig for useful discussion on this topic.

The authors would also like to thanks France Telecom R&D for partly funding this work.

11. References

11.1. Normative References

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

[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] Bradner, S., "Key words for use in RFCs to Indicate Requirement

Levels", BCP 14, RFC 2119, March 1997.

[4] Forsberg, D., "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-11 (work in progress), March 2006.

11.2. Informative References

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

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

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

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

[9] Chowdhury, K., "RADIUS Mobile IPv6 Support", draft-chowdhury-mip6-radius-01 (work in progress), March 2006.

Authors' Addresses

Julien Bournelle
GET/INT
9 rue Charles Fourier
Evry 91011
France

Email: julien.bournelle@int-evry.fr

Maryline Laurent-Maknavicius
GET/INT
9 rue Charles Fourier
Evry 91011
France

Email: maryline.maknavicius@int-evry.fr

Jean-Michel Combes
France Telecom R&D
38/40 rue du General Leclerc
Issy-les-Moulineaux 92794
France

Email: jeanmichel.combes@orange-ft.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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