

DHC Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: June 21, 2007

L. Morand  
France Telecom R&D  
A. Yegin  
Samsung  
S. Kumar  
Tech Mahindra Ltd  
S. Madanapalli  
Samsung  
December 18, 2006

**DHCP options for PANA Authentication Agents**  
**draft-ietf-dhc-paa-option-05**

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

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 June 21, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2006).

Abstract

This document defines new DHCPv4 and DHCPv6 options that contain a list of IP addresses to locate one or more of PANA Authentication Agents (PAA). This is one of the methods that a PANA Client (PaC)

can use to locate PANA Authentication Agents (PAA).

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Specification of Requirements . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Terminology . . . . .	<a href="#">3</a>
<a href="#">4.</a>	PANA Authentication Agent DHCPv4 Option . . . . .	<a href="#">4</a>
<a href="#">5.</a>	PANA Authentication Agent DHCPv6 Option . . . . .	<a href="#">5</a>
<a href="#">6.</a>	IANA Considerations . . . . .	<a href="#">6</a>
<a href="#">7.</a>	Security Considerations . . . . .	<a href="#">6</a>
<a href="#">8.</a>	Acknowledgements . . . . .	<a href="#">7</a>
<a href="#">9.</a>	References . . . . .	<a href="#">7</a>
<a href="#">9.1.</a>	Normative References . . . . .	<a href="#">7</a>
<a href="#">9.2.</a>	Informative References . . . . .	<a href="#">7</a>
	Authors' Addresses . . . . .	<a href="#">7</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">9</a>



## 1. Introduction

The Protocol for carrying Authentication for Network Access (PANA) [[I-D.ietf-pana-pana](#)] defines a new Extensible Authentication Protocol (EAP) [[RFC3748](#)] lower layer that uses IP between the protocol endpoints.

The PANA protocol is run between a PANA Client (PaC) and a PANA Authentication Agent (PAA) in order to perform authentication and authorization for the network access service.

This document specifies DHCPv4 [[RFC2131](#)] and DHCPv6 [[RFC3315](#)] options that allow PANA client (PaC) to discover PANA Authentication Agents (PAA). This is one of the methods for locating PAAs.

The DHCP options defined in this document are used only as a PAA discovery mechanism. These DHCP options MUST NOT be used to perform any negotiation on the use of PANA between the PaC and a PAA.

## 2. Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. 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](#)].

## 3. Terminology

This document uses the DHCP terminology defined in [[RFC2131](#)], [[RFC2132](#)] and [[RFC3315](#)].

This document uses the PANA terminology defined in [[I-D.ietf-pana-pana](#)]. In particular, the following terms are defined:

PANA Client (PaC):

The client side of the protocol that resides in the access device (e.g., laptop, PDA, etc.). It is responsible for providing the credentials in order to prove its identity (authentication) for network access authorization.



PANA Authentication Agent (PAA):

The protocol entity in the access network whose responsibility is to verify the credentials provided by a PANA client (PaC) and authorize network access to the device associated with the client and identified by a Device Identifier (DI).

#### 4. PANA Authentication Agent DHCPv4 Option

This section defines a DHCPv4 option that carries a list of 32-bit (binary) IPv4 addresses indicating one or more PANA Authentication Agents (PAA) available to the PANA client.

The DHCPv4 option for PANA Authentication Agent has the format shown in Fig. 1.

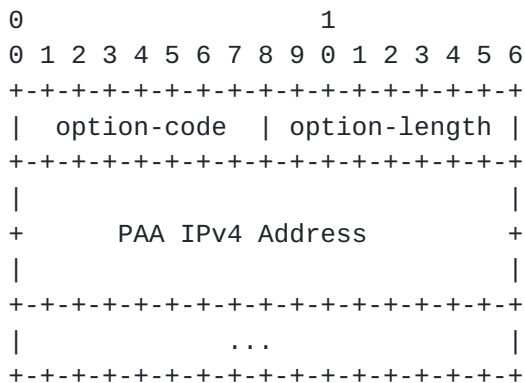


Figure 1: PAA DHCPv4 option

option-code:           OPTION\_PANA\_AGENT (TBD)

option-length:       Length of the 'options' field in octets;  
                      MUST be a multiple of four (4)

PAA IPv4 Address:    IPv4 address of a PAA for the client to use.  
                      The PAAs are listed in the order of preference  
                      for use by the client.

A PaC (DHCPv4 client) SHOULD request the PAA DHCPv4 Option in a Parameter Request List as described in [\[RFC2131\]](#) and [\[RFC2132\]](#).

If configured with a (list of) PAA address(es), a DHCPv4 server SHOULD send a client with the PAA DHCPv4 option, even if this option is not explicitly requested by the client.



A PaC (DHCPv4 client) receiving the PAA DHCPv4 option SHOULD use the (list of) IP address(es) to locate PAA.

The PaC (DHCPv4 client) MUST try the records in the order listed in the PAA DHCPv4 option received from the DHCPv4 server.

## 5. PANA Authentication Agent DHCPv6 Option

This section defines a DHCPv6 option that carries a list of 128-bit (binary) IPv6 addresses indicating one or more PANA Authentication Agents (PAA) available to the PANA client.

The DHCPv6 option for PANA Authentication Agent has the format shown in Fig. 2.

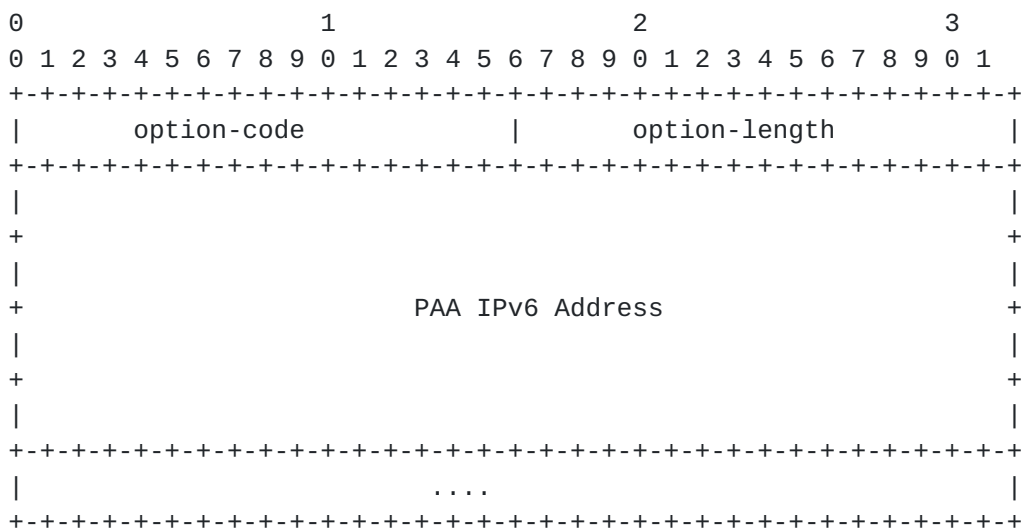


Figure 2: PAA DHCPv6 option

option-code:           OPTION\_PANA\_AGENT (TBD)

option-length:       Length of the 'options' field in octets;  
                      MUST be a multiple of sixteen (16)

PAA IPv6 Address:     IPv6 address of a PAA for the client to use.  
                      The PAAs are listed in the order of preference  
                      for use by the client.

A PaC DHCPv6 client SHOULD request the PAA DHCPv6 option in an Options Request Option (ORO) as described in the DHCPv6 specification [[RFC3315](#)].

If configured with a (list of) PAA address(es), a DHCPv6 server





SHOULD send a client with the PAA DHCPv6 option, even if this option is not explicitly requested by the client.

A PaC (DHCPv6 client) receiving the PAA DHCPv6 option SHOULD use the (list of) IP address(es) to locate PAA.

The PaC (DHCPv6 client) MUST try the records in the order listed in the PAA DHCPv6 option received from the DHCPv6 server.

## 6. IANA Considerations

The following DHCPv4 option code for PANA Authentication Agent option MUST be assigned by IANA:

Option	Name	Value	Described in
-----			
OPTION_PANA_AGENT		TBD	<a href="#">Section 4</a>

The following DHCPv6 option code for PANA Authentication Agent options MUST be assigned by IANA:

Option	Name	Value	Described in
-----			
OPTION_PAA_AGENT		TBD	<a href="#">Section 5</a>

## 7. Security Considerations

The security considerations in [\[RFC2131\]](#), [\[RFC2132\]](#) and [\[RFC3315\]](#) apply. If an adversary manages to modify the response from a DHCP server or insert its own response, a PANA Client could be led to contact a rogue PANA Authentication Agent, possibly one that then intercepts call requests or denies service.

In most of the networks, the DHCP exchange that delivers the options prior to network access authentication is neither integrity protected nor origin authenticated. Therefore, the options defined in this document MUST NOT be used to perform any negotiation on the use of PANA between the PANA Client and a PANA Authentication Agent. Using the presence (or absence) of these DHCP options as an indication of network mandating PANA authentication (or not) is an example such a negotiation mechanism. This negotiation would allow bidding down attacks by making the clients choose to use a lower-grade security mechanism (or even no security at all).



## **8. Acknowledgements**

We would like to thank to Ralph Droms, Stig Venaas, Ted Lemon, Andre Kostur and Bernie Volz for their valuable comments. We would like to thank also Jari Arkko, Thomas Norten, Bernard Aboba that provided several draft reviews, as well as all members of the PANA and DHC working groups that contribute to improve this document.

## **9. References**

### **9.1. Normative References**

- [I-D.ietf-pana-pana]  
Forsberg, D., "Protocol for Carrying Authentication for Network Access (PANA)", [draft-ietf-pana-pana-13](#) (work in progress), December 2006.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.
- [RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", [RFC 2132](#), 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.

### **9.2. Informative References**

- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowitz, "Extensible Authentication Protocol (EAP)", [RFC 3748](#), June 2004.

## Authors' Addresses

Lionel Morand  
France Telecom R&D

Email: [lionel.morand@orange-ft.com](mailto:lionel.morand@orange-ft.com)



Alper E. Yegin  
Samsung

Email: alper01.yegin@partner.samsung.com

Suraj Kumar  
Tech Mahindra Ltd

Email: surajk@techmahindra.com

Syam Madanapalli  
Samsung

Email: syam@samsung.com

## Full Copyright Statement

Copyright (C) The IETF Trust (2006).

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.

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, THE IETF TRUST 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.

## 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](mailto:ietf-ipr@ietf.org).

## Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).

