Network Working Group
Internet-Draft
Expires: September 23, 2006

L. Morand (Ed.)
France Telecom R&D
S. Kumar
Samsung India Software Operations
A. Yegin
Samsung Advanced Institute of Technology
S. Madanapalli
Samsung India Software Operations
March 22, 2006

DHCP options for PANA Authentication Agents
draft-ietf-dhc-paa-option-02

Status of this Memo

Copyright Notice

Abstract

This document defines new DHCPv4 and DHCPv6 options that contain a list of domain names or IP addresses that can be mapped to one or

more of PANA Authentication Agents (PAA). This is one of the many methods that a PANA Client (PaC) can use to locate PANA Authentication Agents (PAA).

Requirements Language

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 [RFC2119].

Table of Contents

1. Introduction

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

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 many methods for locating PAAs: manual configuration is an example of another one.

2. Terminology

This document uses the PANA terminology defined in [I-D.ietf-pana-pana].

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

3. Requirements

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

4. DHCP Specification Dependency

This document describes new options for DHCPv4 and DHCPv6 for obtaining a list of domain names or IP addresses to locate a PANA

Authentication Agent.

This document should be read in conjunction with the DHCPv4 specifications [RFC2131], [RFC2132] and DHCPv6 specification [RFC3315].

Definitions for terms and acronyms not specifically defined in this document are defined in [RFC2131], [RFC2132] and [RFC3315].

5. PANA Authentication Agent DHCPv4 Option

This document defines a new DHCPv4 option that carries either a domain name list or a 32-bit (binary) IPv4 address list to be used by the PANA client to locate PANA authentication Agents.

5.1. PANA Authentication Agent Option

The PANA Authentication Agent Option is specified as a "container" option that conveys one or more "sub-options" providing information to locate PANA Authentication Agents. The format of the PANA Authentication Agent Option is shown in Fig. 1.

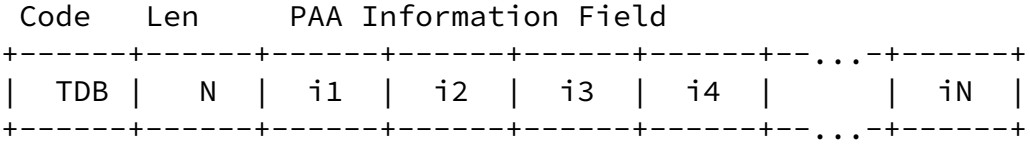

Figure 1: DHCPv4 option for PANA Authentication Agent

The length N gives the total number of octets in the PAA Information Field. The PAA Information field consists of a sequence of SubOpt/ Length/Value tuples for each sub-option, encoded as shown in the Fig. 2.

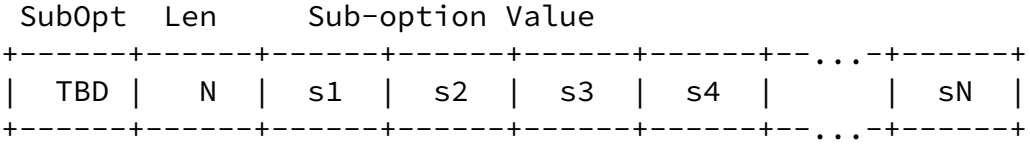

Figure 2: Encoding of of PAA Information field

No "pad" sub-option is defined, and the PAA Information field SHALL NOT be terminated with a 255 sub-option.

The length N of the PANA Authentication Agent Option SHALL include all octets of the sub-option code/length/value tuples.

Since at least one sub-option MUST be defined, the minimum PANA Authentication Agent Option length is two (2).

The length N of the sub-options SHALL be the number of octets in only that sub-option's value field. A sub-option length MAY be zero. The sub-options need not appear in sub-option code order.

The initial assignment of PANA Authentication Agent Sub-options is as follows:

PAA Sub-option Code	Sub-Option Description
1	PAA Domain Name List Sub-option
2	PAA IPv4 Address List Sub-option

An implementation implementing this specification MUST support both sub-options.

5.2. PANA Authentication Agent Domain Name List Sub-option

This sub-option carries a list of domain names indicating one or more PANA Authentication Agents available to the PANA client.

This sub-option MAY contain multiple domain names, but these SHOULD refer to different NAPTR records, rather than different A records. Domain names MUST be listed in order of preference.

Use of multiple domain names is not meant to replace NAPTR and SRV records, but rather to allow a single DHCPv4 server to indicate multiple PANA Authentication Agents available in the same access network.

The domain names are encoded according to Section 3.1 of [RFC1035]. Clients MUST support compression according to the encoding in Section 4.1.4 of [RFC1035].

If the length of the domain list exceeds the maximum permissible within a single option (254 octets), then the domain list MUST be represented in the DHCP message as specified in [RFC3396].

5.3. PANA Authentication Agent IPv4 Address List Sub-option

This sub-option carries a list of IPv4 addresses indicating one or more PANA Authentication Agents available to the PANA client.

PAAs MUST be listed in order of preference for use by the PaC.

The number of octets following the sub-option length field MUST be a multiple of four (4).

6. PANA Authentication Agent DHCPv6 Options

This section defines two DHCPv6 options that describe a PANA Authentication Agent: one carries a list of domain names, the other a list of 128-bit (binary) IPv6 addresses.

An implementation implementing this specification MUST support both options.

6.1. PANA Authentication Agent Domain Name List

This option carries a list of domain names indicating one or more PANA Authentication Agents available to the PANA client.

The option length is followed by a sequence of labels, encoded according to Section 3.1 of [RFC1035],quoted below:

> "Domain names in messages are expressed in terms of a sequence of labels. Each label is represented as a one octet length field followed by that number of octets. Since every domain name ends with the null label of the root, a domain name is terminated by a

length byte of zero. The high order two bits of every length octet must be zero, and the remaining six bits of the length field limit the label to 63 octets or less. To simplify implementations, the total length of a domain name (i.e., label octets and label length octets) is restricted to 255 octets or less."

[RFC1035] encoding was chosen to accommodate future internationalized domain name mechanisms.

The option MAY contain multiple domain names, but these SHOULD refer to different NAPTR records, rather than different A records. Domain names MUST be listed in order of preference. Use of multiple domain names is not meant to replace NAPTR or SRV records, but rather to allow a single DHCP server to indicate PANA Authentication Agents operated by multiple providers.

The DHCPv6 option for PANA Authentication Agent Domain Name List has the format shown in Fig. 3.

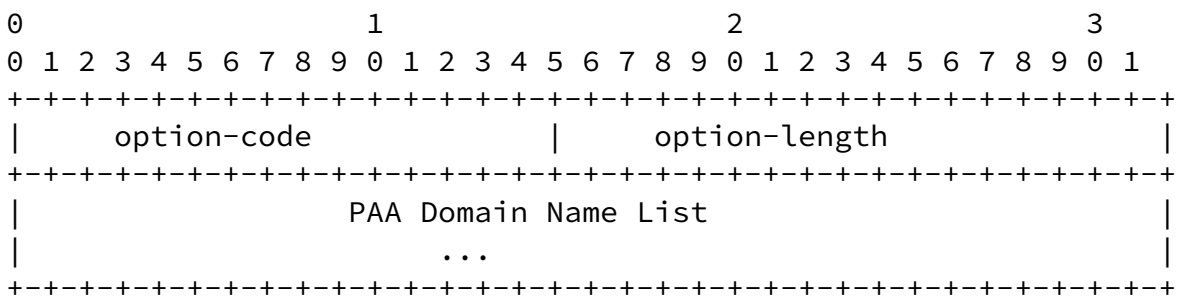

Figure 3: DHCPv6 option for PAA Domain Name List

option-code: OPTION_PANA_AGENT_D (TBD).

option-length: Length of the 'PAA Domain Name List' field in octets;

variable.

PAA Domain Name List: The domain names of the PANA Authentication Agents (PAA) for the client to use. The domain names are encoded as specified in Section 8 ("Representation and use of domain names") of the DHCPv6 specification [RFC3315].

6.2. PANA Authentication Agent IPv6 Address List

This option specifies a list of IPv6 addresses indicating PANA Authentication Agent available to the client.

PANA Authentication Agents MUST be listed in order of preference.

The DHCPv6 option for PAA IPv6 Address List has the format shown in Fig. 4.

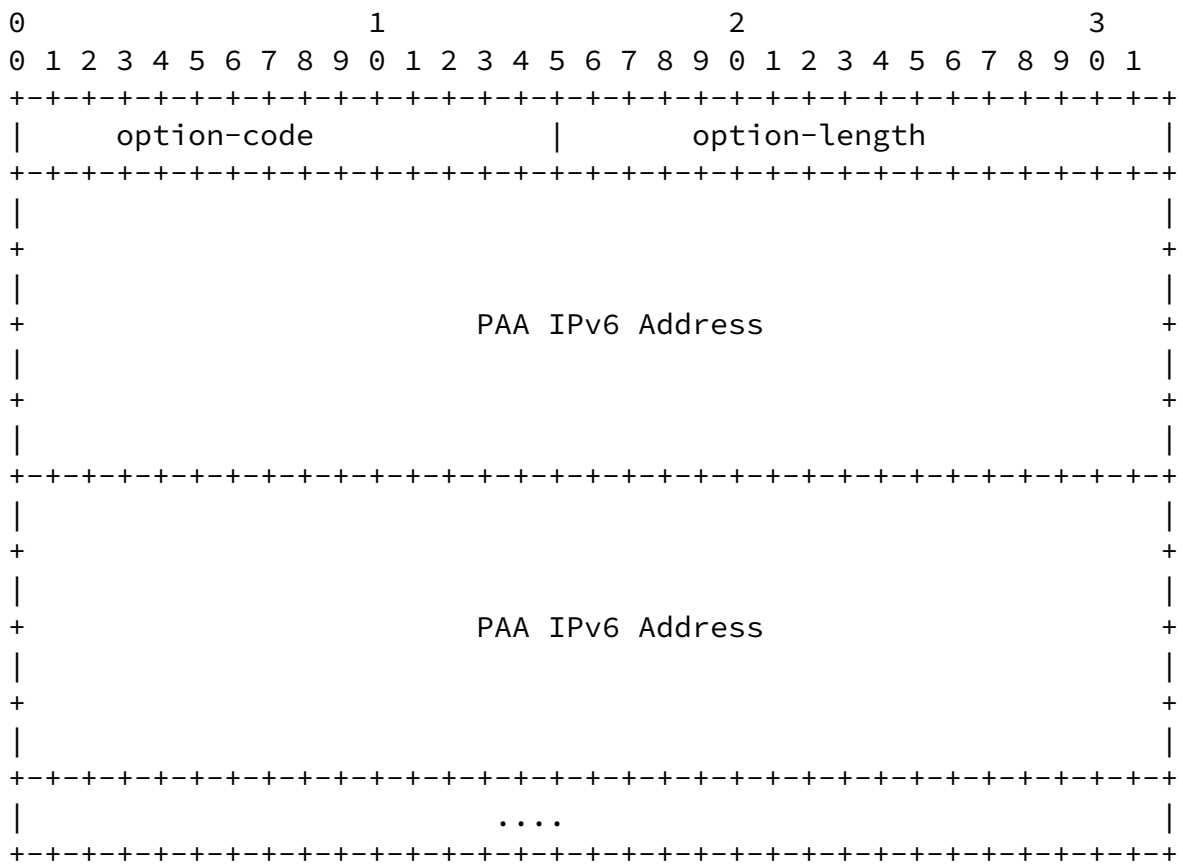

Figure 4: DHCPv6 option for PAA IPv6 Address List

option-code: OPTION_PANA_AGENT_A (TBD).

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

PANA IP 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.

7. Client Operation

7.1. DHCPv4 Client

The client requests PAA Option in a Parameter Request List as described in [RFC2131] and [RFC2132].

If a client receives in response a PAA Domain Name List Sub-option, the client MUST try the records in the order listed. The client only resolves the subsequent domain names if attempts to contact the first one failed or denote a domain administratively prohibited by client policy.

If a client receives in response a PAA IPv4 Address List Sub-option, the client MUST try the records in the order listed.

If a client receives both the PAA Domain Name List Sub-option and PAA IPv4 Address List Sub-options, it SHOULD use first the PAA Domain Name List Sub-option. The client MUST try the records in the order listed. The client only resolves the subsequent domain name if attempts to contact the first one failed or denote a domain administratively prohibited by client policy. Only if no PANA Authentication Agent in the Domain Name List can be resolved or reached, the client MAY use the PAA IPv4 Address List Sub-option.

7.2. DHCPv6 Client

A DHCPv6 client may request either or both PAA domain name list and PAA IPv6 address list options in an Options Request Option (ORO) as described in the DHCPv6 specification [RFC3315].

If a client receives in response a PAA Domain Name List Sub-option, the client MUST try the records in the order listed. The client only resolves the subsequent domain names if attempts to contact the first one failed or denote a domain administratively prohibited by client policy.

If a client receives in response a PAA IPv6 Address List Sub-option, the client MUST try the records in the order listed.

If a client receives both the PAA Domain Name List and PAA IPv6 Address List options, it SHOULD use first the PAA Domain Name List option. The client MUST try the records in the order listed. The client only resolves the subsequent domain names if attempts to contact the first one failed or denote a domain administratively

prohibited by client policy. Only if no PANA Authentication Agent in the Domain Name List can be resolved or reached, the client MAY use the PAA IPv6 Address List option.

8. DHCP Server Operation

8.1. DHCPv4 Server

If configured with both PAA domain name list and PAA IP address list, the DHCPv4 server SHOULD responds to the request with the domain name list to be used by the PANA client. However the DHCPv4 server MAY send a DHCPv4 client both of the PAA Domain Name List and PAA IPv4 Address List Sub-options.

8.2. DHCPv6 Server

If configured with both PAA domain name list and PAA IP address list, a DHCPv6 server MAY send a DHCPv6 client one or both of the PAA Domain Name List and PAA IPv6 Address List options.

If a DHCPv6 client requests both options in an ORO and the server is configured for both, the DHCPv6 server MAY send a DHCPv6 client only one of these options and that option SHOULD be the PAA Domain Name List.

If a DHCPv6 client requests only the PAA IPv6 Address List option and the DHCPv6 server is configured with both options, the server MUST send a DHCPv6 client the PAA IPv6 Address List option and MAY send a the PAA Domain Name List (see [RFC3315]).

The following table summarizes the DHCPv6 server's responses:

Client sends in ORO	Domain Name List	IPv6 Address List
Neither option	SHOULD	MAY
PAA Domain Name List	SHOULD	MAY
PAA IPv6 Address List	MAY	MUST
Both options	SHOULD	MAY

9. IANA Considerations

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

Option	Name	Value
PAA Option		TBD

IANA is required to maintain a new number space of "DHCP PAA Sub-options", located in the BOOTP-DHCP Parameters Registry. The initial sub-options are described in section 5 of this document with the following assignment:

PAA Sub-option Code	Sub-Option Description	Described in
1	PAA Domain Name List Sub-option	Section 5.1
2	PAA IPv4 Address List Sub-option	Section 5.2

IANA assigns future DHCP PAA Sub-options with a "IETF Consensus" policy as described in [RFC2434]. Future proposed sub-options are to be referenced symbolically in the Internet-Drafts that describe them, and shall be assigned numeric codes by IANA when approved for publication as an RFC.

The following DHCPv6 option codes for PANA Authentication Agent options must be assigned by IANA:

Option	Name	Value	Described in
OPTION_PAA_AGENT_D		TBD	Section 6.1
OPTION_PAA_AGENT_A		TBD	Section 6.2

10. 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 Agent, possibly one that then intercepts call requests or denies service.

11. Acknowledgements

12. Normative References

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

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[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.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[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.

[RFC3396] Lemon, T. and S. Cheshire, "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", RFC 3396, November 2002.

Authors' Addresses

Lionel Morand
France Telecom R&D
38-40 rue du general Leclerc
92794 Issy-Les-Moulineaux Cedex 9
France

Phone: +33 1 45296257
Email: lionel.morand@francetelecom.com

Suraj Kumar
Samsung India Software Operations
No. 66/1, BAGMANE TECH PARK, C V RAMAN NAGAR
Bangalore
India

Phone: +91 80 41819999
Email: suraj.kumar@samsung.com

Alper E. Yegin
Samsung Advanced Institute of Technology
75 West Plumeria Drive

San Jose, CA 95134
USA

Phone: +1 408 544 5656
Email: alper.yegin@samsung.com

Syam Madanapalli
Samsung India Software Operations
No. 66/1, BAGMANE TECH PARK, C V RAMAN NAGAR
Bangalore
India

Phone: +91 80 41819999
Email: syam@samsung.com

Intellectual Property Statement

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.

Disclaimer of Validity

Copyright Statement

Acknowledgment

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