Internet Engineering Task Force
Internet-Draft
Expires: September 4, 2006

S. Kumar
Samsung India Software Operations
L. Morand
France Telecom R&D
A. Yegin
Samsung Advanced Institute of Technology
S. Madanapalli
Samsung India Software Operations

March 3, 2006

DHCP option for PANA Authentication Agents
draft-ietf-dhc-paa-option-01.txt

Status of this Memo

Copyright Notice

Abstract

This document defines new Dynamic Host Configuration Protocol 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).

Table of Contents

1. Introduction

The Protocol for carrying Authentication for Network Access (PANA) [1] 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 option [2] and DHCPv6 option [7] 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 [1].

This document uses the DHCP terminology defined in [2] , [3] and[7].

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 [4].

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 [2] , [3] and DHCPv6 specification [7].

Definitions for terms and acronyms not specifically defined in this document are defined in [2] , [3] and DHCPv6 specification [7].

5. PANA Authentication Agent DHCPv4 Option

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

The option has two encodings, specified by the encoding byte ('enc') that follows the code byte. If the encoding byte has the value 0, it is followed by a list of domain names, as described below (Section 5.1). If the encoding byte has the value 1, it is followed by one or more IPv4 addresses (Section 5.2). All implementations MUST support both encodings. The 'option-length' field indicates the total number of octets in the option following the 'option-length' field, including the encoding byte.

5.1. PANA Authentication Agent Domain Name List

If the 'enc' byte has a value of 0, the encoding byte is followed by a sequence of labels, encoded according to Section 3.1 of RFC 1035 [5], 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.

RFC 1035 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 and SRV records, but rather to allow a single DHCPv4 server to indicate multiple PANA Authentication Agents available in the same access network.

Clients MUST support compression according to the encoding in Section 4.1.4 of [5].

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 [6].

The DHCPv4 option for this encoding has the format shown in Fig. 1.

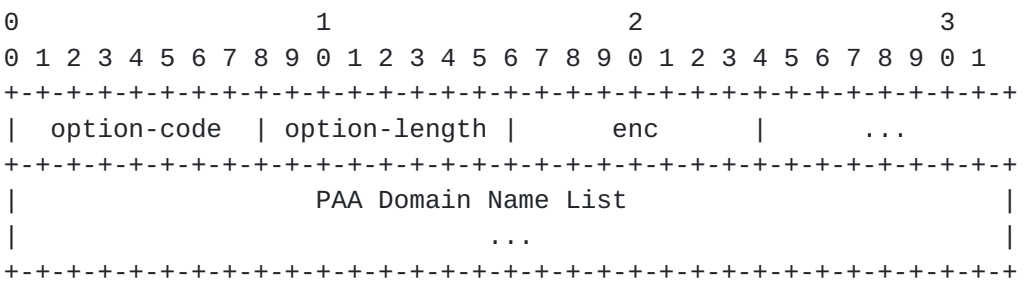

Figure 1: DHCPv4 option for PAA Domain Name List

option-code: OPTION_PANA_AGENT(TBD)

option-length: Number of octets following the 'option-length' field, including the encoding byte, in octets; variable.

enc: Encoding byte set to 0

PAA Domain Name List: The domain names of the PANA Authentication Agents for the client to use. The domain names are encoded according to Section 3.1 of RFC 1035 [5].

5.2. PANA Authentication Agent IPv4 Address List

If the 'enc' byte has a value of 1, the encoding byte is followed by 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.

The DHCPv4 option for this encoding has the format shown in Fig. 2.

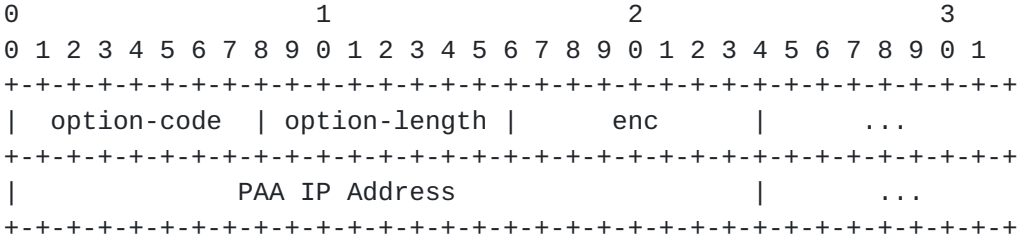

Figure 2: DHCPv4 option for PAA IPv4 Address List

option-code: OPTION_PANA_AGENT(TBD)

option-length: Number of octets following the 'option-length' field, including the encoding byte in octets; Must be a multiple

of 4 plus one.

enc: Encoding byte set to 1

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

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 (Section 6.1), the other a list of 128-bit (binary) IPv6 addresses (Section 6.2).

> Since DHCPv6 does not suffer from a shortage of option codes, we avoid the encoding byte found in the DHCPv4 option for PAA (Section 5). This makes the option shorter, easier to parse, simplifies appropriate word alignment for the numeric addresses and allows the DHCPv6 client to request either numeric or domain name options using the "option request option" (ORO).

An implementation implementing this specification MUST support both options.

6.1. PANA Authentication Agent Domain Name List

The option length is followed by a sequence of labels, encoded according to Section 3.1 of RFC 1035 [3],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."

RFC 1035 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

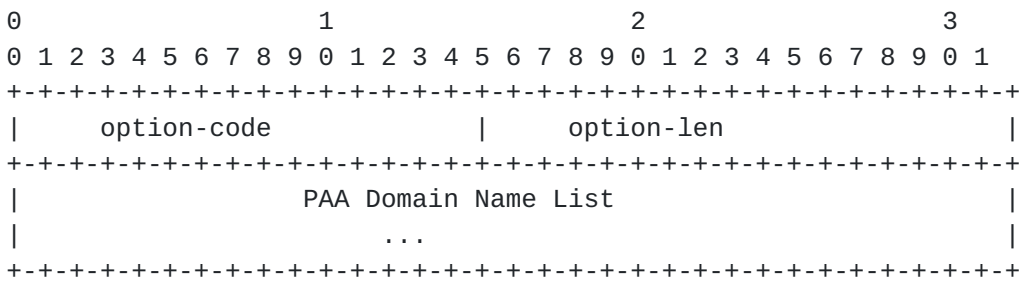

Figure 3: DHCPv6 option for PAA Domain Name List

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 [7].

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.

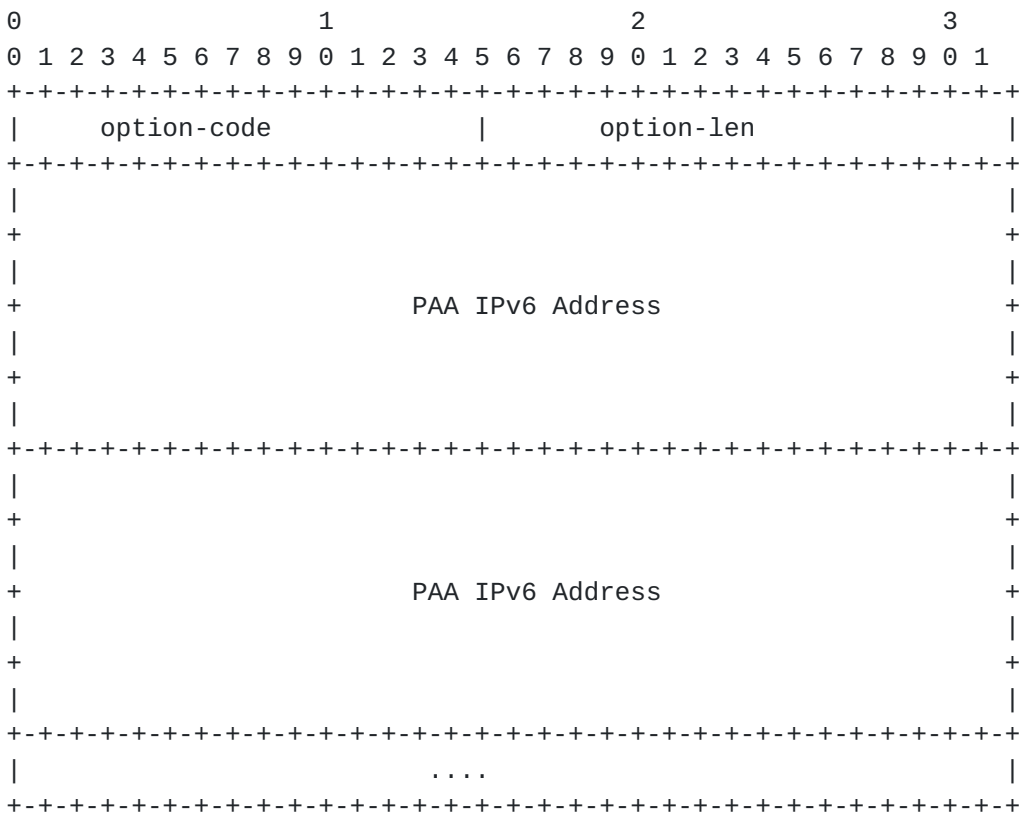

Figure 4: DHCPv6 option for PAA IPv6 Address List

option-code: OPTION_PANA_AGENT_A (TBD).

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

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.

7. Client Operation

7.1. DHCPv4 Client

The client requests PAA DHCPv4 Option in a Parameter Request List as described in [2] and [3].

If the PAA DHCPv4 option provided in response by the DHCPv4 server contains multiple domain names, 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 the PAA DHCPv4 option provided in response by the DHCPv4 server contains multiple IP addresses, the client MUST try the records in the order listed.

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 [7].

8. DHCP Server Operation

8.1. DHCPv4 Server

If a DHCPv4 server is 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.

A DHCP server MUST NOT mix the two list types (domain names and IPv4 address) in the same DHCPv4 message, even if it sends two different instances of the same option.

8.2. DHCPv6 Server

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 [7]).

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. Security Considerations

The security considerations in [2] , [3] and [7] 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.

10. IANA Considerations

IANA assignment for the following DHCPv4 option code is needed.

Option	Name	Value
OPTION_PAA_AGENT		TBD

The following option codes for PANA Authentication Agent DHCPv6 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

11. Normative References

[1] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA), draft-ietf-pana-pana-08 (work in progress)", Novemeber 2005.

[2] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[3] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

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

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

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

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

Authors' Addresses

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

Lionel Morand
France Telecom R&D
38-40 rue du general Leclerc
Issy-les-Moulineaux, F-92130
France

Phone: +33 1 4529 6257
Email: lionel.morand@francetelecom.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

Disclaimer of Validity

Copyright Statement

Acknowledgment

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