Network Working Group	G. Zorn	
Internet-Draft	Network Zen	
Intended status: Standards Track	Q. Wu	
Expires: March 20, 2011	Y. Wang	
	Huawei	
	September 16, 2010	

TOC

The Local Domain Name DHCPv6 Option
draft-ietf-hokey-ldn-discovery-04

Abstract

In order to derive a Domain-Specific Root Key (DSRK) from the Extended Master Session Key (EMSK) generated as a side-effect of an Extensible Authentication Protocol (EAP) method, the EAP peer must discover the name of the domain to which it is attached.

This document specifies a Dynamic Host Configuration Protocol Version 6 (DHCPv6) option designed to allow a DHCPv6 server to inform clients of the name of the local domain..

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
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.”
This Internet-Draft will expire on March 20, 2011.

Copyright Notice

Table of Contents

1. Introduction
2. Terminology
3. Option Format
   3.1. DHCPv6 Local Domain Name Option
4. Client Behavior
5. Relay Agent Behavior
6. Server Behavior
7. Security Considerations
8. IANA considerations
9. References
   9.1. Normative References
   9.2. Informative References

---

1. Introduction

TOC

The EAP Re-authentication Protocol (ERP) [RFC5296] (Narayanan, V. and L. Dondeti, “EAP Extensions for EAP Re-authentication Protocol (ERP),” August 2008.) is designed to allow faster re-authentication of a mobile device which was previously authenticated by means of the Extensible Authentication Protocol [RFC3748] (Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, “Extensible Authentication Protocol (EAP),” June 2004.). Given that the local root key (e.g., DSRK RFC 5295 (Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, “Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK),” August 2008.) [RFC5295]) is generated using the local domain name (LDN), LDN discovery is an important part of re-authentication. As described in RFC 5296 (Narayanan, V. and L. Dondeti, “EAP Extensions for EAP Re-authentication Protocol (ERP),” August 2008.) [RFC5296], the local domain name can be learned by the mobile device through the ERP exchange or via a lower-layer mechanism. However, no lower-layer mechanisms for LDN discovery have yet been defined.

This document specifies an extension to DHCPv6 for local domain name discovery.

---

2. Terminology

TOC

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] (Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.).

---

3. Option Format

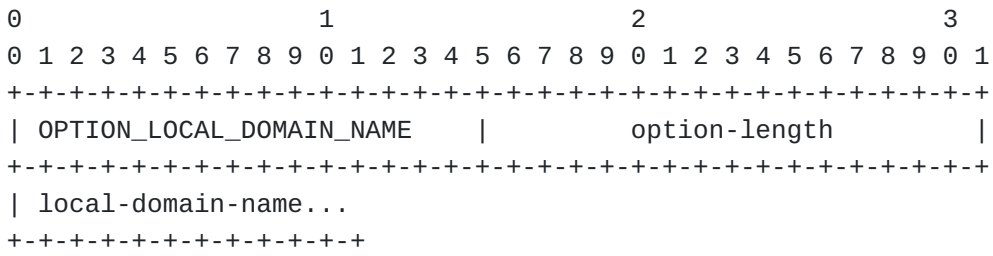
TOC

In DHCPv6-based local domain name discovery, the LDN option is used by the DHCPv6 client to obtain the local domain name from the DHCPv6 Server after full EAP authentication has taken place.

3.1. DHCPv6 Local Domain Name Option

TOC

The format of this option is:



option code OPTION_LOCAL_DOMAIN_NAME (TBD)

option-length Length of the local-domain-name field, in octets

local-domain-name This field contains the name of the local domain and MUST be encoded as specified in Section 8 of RFC 3315 (Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," July 2003.) [RFC3315].

TOC

4. Client Behavior

If a DHCPv6 client doesn't know the local domain name and requires the DHCPv6 Server to provide the DHCPv6 LDN option, it MUST include an Option Request option requesting the DHCPv6 LDN option, as described in Section 22.7 of RFC 3315 [RFC3315] (Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," July 2003.).

When the DHCPv6 client recieves a LDN option with the local domain name present in it, it MUST verify that the option length is no more than 256 octets (the maximum length of a single FQDN allowed by DNS), and that the local domain name is a properly encoded single FQDN, as specified in Section 8, "Representation and Use of Domain Names" of RFC3315 [RFC3315] (Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," July 2003.).

---

5. Relay Agent Behavior

TOC

If a DHCPv6 relay agent has pre-existing knowledge of the local domain name (for example, from a previous AAA exchange), it SHOULD include it in an instance of the DHCPv6 LDN option and forward to the DHPv6 server as a suboption of the Relay-Supplied Options option [I-D.ietf-dhc-dhcpv6-relay-supplied-options] (Lemon, T. and W. Wu, "Relay-Supplied DHCP Options," September 2010.).

---

6. Server Behavior

TOC

If the option code for the LDN option is included in an Option Request option, the server SHOULD return the DHCPv6 LDN option to the client.

---

7. Security Considerations

TOC

The communication between the DHCPv6 client and the DHCPv6 server for the exchange of local domain name information is security sensitive and requires authentication, integrity and replay protection. DHCPv6 security [RFC3315] (Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," July 2003.) can be used for this purpose.

---

8. IANA considerations

TOC

IANA is requested to assign one new option code from the registry of DHCP Option Codes maintained at http://www.iana.org/assignments/dhcpv6-parameters, referencing this document.

---

9. References

TOC

9.1. Normative References

TOC

[I-D.ietf-dhc-dhcpv6-relay-supplied-options]	Lemon, T. and W. Wu, “Relay-Supplied DHCP Options,” draft-ietf-dhc-dhcpv6-relay-supplied-options-00 (work in progress), September 2010 (TXT).
[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[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 (TXT).
[RFC5295]	Salowey, J., Dondeti, L., Narayanan, V., and M. Nakhjiri, “Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK),” RFC 5295, August 2008 (TXT).
[RFC5296]	Narayanan, V. and L. Dondeti, “EAP Extensions for EAP Re-authentication Protocol (ERP),” RFC 5296, August 2008 (TXT).

9.2. Informative References

TOC

[RFC3748]	Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, “Extensible Authentication Protocol (EAP),” RFC 3748, June 2004 (TXT).

Authors' Addresses

TOC

	Glen Zorn
	Network Zen

	77/440 Soi Phoomjit, Rama IV Road
	Phra Khanong, Khlong Toie
	Bangkok 10110
	Thailand
Phone:	+66 (0) 87-040-4617
EMail:	gwz@net-zen.net
	Qin Wu
	Huawei Technologies Co., Ltd.
	101 Software Avenue, Yuhua District
	Nanjing, Jiangsu 21001
	China
Phone:	+86-25-84565892
EMail:	sunseawq@huawei.com
	Yungui Wang
	Huawei Technologies Co., Ltd.
	Site B, Floor 10, HuiHong Mansion, No.91 BaiXia Rd.
	Nanjing, Jiangsu 210001
	P.R. China
Phone:	+86 25 84565893
EMail:	w52006@huawei.com