Dynamic Host Configuration Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 16, 2010

D. Hankins
ISC
T. Mrugalski
Gdansk University of Technology
November 12, 2009

Dynamic Host Configuration Protocol (DHCPv6) Option for Dual-Stack Lite

draft-dhankins-softwire-tunnel-option-05

Abstract

This document describes how Dual-Stack Lite configuration (the Softwire Concentrator (SC)'s address) can be obtained by a Softwire Initiator (SI) via DHCPv6.

Table of Contents

1. Requirements Language

In this document, the key words "MAY", "MUST", "MUST NOT", "OPTIONAL", "RECOMMENDED", "SHOULD", and "SHOULD NOT", are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

2. Introduction

Dual-Stack Lite [draft-ietf-softwire-dual-stack-lite-02] is a method to extend IPv4 access to an IPv6-only addressed host. One of its key components is an IPv4-over-IPv6 tunnel, commonly referred to as a Softwire, but a host will not know if the network it is attached to offers Dual-Stack Lite support, and if it did would not know the remote end of the tunnel to establish a connection.

These are two separate pieces of information; 1) Should the client shut down its dual-stack IPv4 side, and use the softwire exclusively for IPv4 access? 2) At what IPv6 address should the client establish a softwire connection?

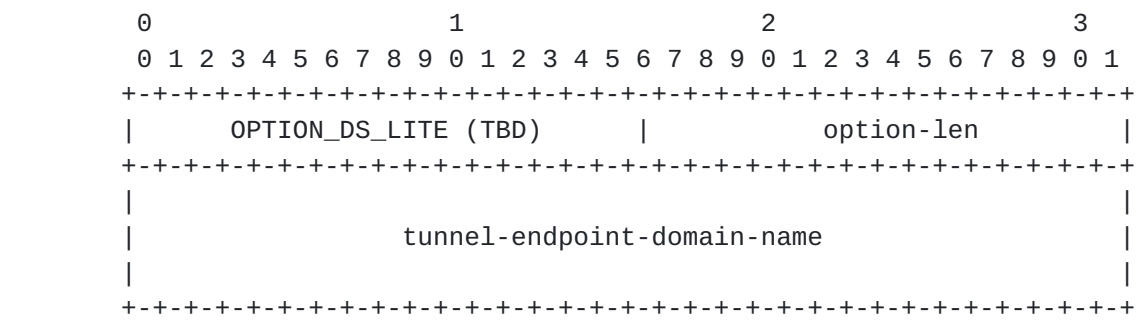
These two questions can be answered with one DHCPv6 [RFC3315] option.

DISCUSSION: It can be argued that if you inform a client it should perform Dual-Stack Lite, but fail to deliver an IPv6 tunnel endpoint, then its IPv4 access is certainly broken. If you give the client an IPv6 tunnel endpoint but fail to inform it that it must use Dual-Stack Lite for IPv4 access, then again its access is likely broken, or is operating in a degraded mode of service (if an operator offers a Dual-Stack Lite method of access, there either isn't any native IPv4 access, or the Dual-Stack Lite method works better than native access - if a network had better native IPv4 access than Dual-Stack Lite access, there would be no reason to extend the service). So the presence of a tunnel address also indicates the operator's intent for the client to use the Softwire.

3. The Dual-Stack Lite DHCPv6 Option

The Dual-Stack Lite DHCPv6 Option is simply a fully qualified domain name that specifies the remote tunnel endpoint, expected to be located at the AFTR (DS-Lite Address Family Transition Router element).

The Dual-Stack Lite Option Format is presented in Figure 1.



DS Lite option format.

Figure 1

option-code: OPTION_DS_LITE (TBD)

option-len: Length of the tunnel-endpoint-domain-name field.

tunnel-endpoint-domain-name: Fully Qualified Domain Name of the remote tunnel endpoint, located at the AFTR.

The DS Lite option MAY appear in the root scope of a DHCPv6 packet. It MUST NOT appear inside any IA_NA, IA_TA, IA_PD, IAADDR, or similar.

The DS Lite option MUST NOT appear more than once in a message.

tunnel-endpoint-domain-name field MUST be encoded as specified in Section 8 "Representation and Use of Domain Names" of the [RFC3315].

4. DHCPv6 Server behavior

If configured with a value, DHCPv6 servers will include the DS Lite option if it appears on the client's Option Request Option (OPTION_ORO). RFC 3315 Section 17.2.2 [RFC3315] describes how a DHCPv6 client and server negotiate configuration values using the ORO.

DHCPv6 servers will not send the DS Lite option if it has not been requested by the client.

The provided domain name must be a resolvable fully qualified domain name.

It is RECOMMENDED that server will be configured to also provide OPTION_DNS_SERVERS defined in [RFC3646] together with the DS Lite option, so that clients will be able to ask for DNS servers locations

to resolve domain name provided in DS Lite option.

5. DHCPv6 Client behavior

A client that supports B4 functionality of the DS Lite (defined in [draft-ietf-softwire-dual-stack-lite-02]) MUST include OPTION_DS_LITE on its OPTION_ORO.

When requesting OPTION_DS_LITE option, the client also SHOULD request OPTION_DNS_SERVERS defined in [RFC3646] to be able to resolve the received domain name.

If the client receives a DS Lite Option, it MUST verify that the option length is less than or equal to 256 octets (the maximum length of a single FQDN allowed by DNS), and that the tunnel endpoint domain name is a properly encoded single FQDN, as specified in Section 8 "Representation and Use of Domain Names" of the [RFC3315]. If the option is not of valid length or content (for example, if it contains compression tags), it MUST be ignored (and the client SHOULD continue in attempts to acquire native IPv4 access).

Once the client receives and verifies validity of the DS Lite option, it should resolve the received domain name using standard DNS resolution as defined in [RFC3596]. If the DNS response contains more than one IPv6 address, the client picks the first IPv6 address in the response and uses it as a remote tunnel endpoint. The client MUST NOT establish more than one DS Lite tunnel at the same time. For a redundancy and high availability discussion, see Section 7.2 "High availability" of the [draft-ietf-softwire-dual-stack-lite-02].

The client SHOULD terminate or withdraw any native DHCPv4 [RFC2131] configuration on the same interface. If DHCPv4 configuration has concluded, the client SHOULD perform a DHCPRELEASE as it tears down its IPv4 configuration.

DISCUSSION: The author's best understanding of the current epistemology on IPv6 multihoming is that the client will have IPv6 addresses on multiple different IPv6 prefixes. If a host is multihomed, then, it is strange enough to wonder how DHCPv6 configuration will work as most DHCPv6 clients will attach to only one DHCPv6 server. It is even stranger to wonder how the client would react if all of its multiple homes wished to provide IPv4 access via DS Lite. Would a client establish more than one tunnel?

6. Security Considerations

This document does not present any new security issues, but as with all DHCPv6-derived configuration state, it is completely possible that the configuration is being delivered by a third party (Man In The Middle). As such, there is no basis to trust that the access the DS-Lite softwire connection represents can be trusted, and it should not therefore bypass any security mechanisms such as IP firewalls.

RFC 3315 [RFC3315] discusses DHCPv6 related security issues.

[draft-ietf-softwire-dual-stack-lite-02] discusses DS Lite related security issues.

7. IANA Considerations

IANA is requested to allocate one DHCPv6 Option code, referencing this document.

8. Normative References

[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.

[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.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.

[RFC3646] Droms, R., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

[draft-ietf-softwire-dual-stack-lite-02] Durand, A., Ed., "Dual-stack lite broadband deployments post IPv4 exhaustion", October 2009.

Authors' Addresses

David W. Hankins
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
US

Phone: +1 650 423 1307
Email: David_Hankins@isc.org

Tomasz Mrugalski
Gdansk University of Technology
Storczykowa 22B/12
Gdansk,
Poland

Phone: +48 698 088 272
Email: tomasz.mrugalski@eti.pg.gda.pl