Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite
draft-ietf-softwire-ds-lite-tunnel-option-06

Abstract

This document specifies a DHCPv6 option which is meant to be used by
a Dual-Stack Lite client (Basic Bridging BroadBand element, B4) to
discover its Address Family Transition Router (AFTR) address.

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 June 2, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.
Table of Contents

1. Requirements Language ........................................ 3
2. Introduction ................................................. 3
3. The AFTR-Name DHCPv6 Option .................................. 3
4. DHCPv6 Server Behavior ....................................... 5
5. DHCPv6 Client Behavior ....................................... 5
6. Security Considerations ..................................... 6
7. IANA Considerations .......................................... 6
8. Acknowledgements ............................................. 6
9. Normative References ......................................... 6
Authors’ Addresses ............................................... 7
1. 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].

2. Introduction

Dual-Stack Lite [I-D.softwire-ds-lite] is a solution to offer both IPv4 and IPv6 connectivity to customers which are addressed only with an IPv6 prefix (no IPv4 address is assigned to the attachment device). One of its key components is an IPv4-over-IPv6 tunnel, commonly referred to as a Softwire. A DS-Lite "Basic Bridging BroadBand" (B4) device 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.

To inform the B4 of the Address Family Transition Router’s (AFTR) location, a DNS [RFC1035] hostname may be used. Once this information is conveyed, the presence of the configuration indicating the AFTR’s location also informs a host to initiate Dual-Stack Lite (DS-Lite) service and become a Softwire Initiator.

To provide the conveyance of the configuration information, a single DHCPv6 [RFC3315] option is used, expressing the AFTR’s Fully Qualified Domain Name to the B4 element.

The details of how the B4 establishes an IPv4-in-IPv6 tunnel to the AFTR are out of scope for this document.

3. The AFTR-Name DHCPv6 Option

The AFTR-Name option consists of option-code and option-len fields (as all DHCPv6 options have), and a variable length tunnel-endpoint-name field containing a fully qualified domain name that refers to the AFTR which the client is asked to connect to.

The OPTION_AFTR_NAME 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. Any OPTION_AFTR_NAME option received inside any other option MUST be ignored.

The OPTION_AFTR_NAME option MUST NOT appear more than once in a message. Clients that receive more than one OPTION_AFTR_NAME options MUST discard all instances of that option, acting as if none were sent.
The format of the AFTR-Name option is shown in the following figure:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-------------------------------+-------------------------------+
| OPTION_AFTR_NAME: (TBD)     |          option-len           |
+-------------------------------+-------------------------------+
|                                                               |
+---------------------------------------------------------------+
|                  tunnel-endpoint-name (FQDN)                  |
|                                                               |
+---------------------------------------------------------------+
```

- **OPTION_AFTR_NAME**: (TBD)
- **option-len**: Length of the tunnel-endpoint-name field.
- **tunnel-endpoint-name**: A fully qualified domain name identifying the tunnel endpoint, located at the DS-Lite AFTR.

Figure 1: AFTR-Name DHCPv6 Option Format

The tunnel-endpoint-name field is formatted as required in DHCPv6 [RFC3315] Section 8 ("Representation and Use of Domain Names"). Briefly, the format described is using a single octet noting the length of one DNS label (limited to at most 63 octets), followed by the label contents. This repeats until all labels in the FQDN are exhausted, including a terminating zero-length label. Any updates to Section 8 of DHCPv6 [RFC3315] also apply to encoding of this field. An example format for this option is shown in Figure 2, which conveys the FQDN "aftr.example.com.".

```
+------+------+------+------+------+------+------+------+------+
| 0x04 |   a  |   f  |   t  |   r  | 0x07 |   e  |   x  |   a  |
+------+------+------+------+------+------+------+------+------+
|   m  |   p  |   l  |   e  | 0x03 |   c  |   o  |   m  | 0x00 |
+------+------+------+------+------+------+------+------+------+
```

Figure 2: Example tunnel-endpoint-name.

Note that in the specific case of the example tunnel-endpoint-name, (Figure 2) the length of the tunnel-endpoint-name is 18 octets, and so an option-len field value of 18 would be used.

The option is validated by confirming that the option-len is greater than 3, that the option data can be contained by the option length (that the option length does not run off the end of the packet), that individual label lengths do not exceed the option length, and that
the tunnel-endpoint-name is of valid format as described in DHCPv6 Section 8 [RFC3315]; there are no compression tags, there is at least one label of nonzero length.

4. DHCPv6 Server Behavior

A DHCPv6 server MUST NOT send more than one OPTION_AFTR_NAME option.

A DHCPv6 server MUST NOT send the OPTION_AFTR_NAME option as a suboption in other options; it MUST appear only in the root scope of any DHCPv6 messages made in response to clients (Reply, Advertise, et al).

RFC 3315 Section 17.2.2 [RFC3315] describes how a DHCPv6 client and server negotiate configuration values using the Option Request Option (OPTION_ORO). As a convenience to the reader, we mention here that a server will not reply with a value for the OPTION_AFTR_NAME if the client has not explicitly enumerated it on its OPTION_ORO.

5. DHCPv6 Client Behavior

A client that supports the B4 functionality of DS-Lite (defined in [I-D.softwire-ds-lite]) and conforms to this specification MUST include OPTION_AFTR_NAME on its OPTION_ORO.

Because it requires DNS name to address resolution, a client MAY also wish to include the OPTION_DNS_SERVERS option on its OPTION_ORO.

If the client receives the OPTION_AFTR_NAME option, it MUST verify the option contents as described in Section 3.

If the client receives more than one OPTION_AFTR_NAME option, it MUST discard all instances of that option.

The client performs standard DNS resolution using the provided FQDN to resolve a AAAA record, as defined in [RFC3596] and STD 13 [RFC1034] [RFC1035].

If any DNS response contains more than one IPv6 address, the client picks only one IPv6 address 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 [I-D.softwire-ds-lite].
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.


7. IANA Considerations

IANA is requested to allocate single DHCPv6 option code referencing this document, delineating OPTION_AFTR_NAME.

8. Acknowledgements

Authors would like to thank Alain Durand, Rob Austein, Dave Thaler, Paul Selkirk, Ralph Droms, Mohamed Boucadair and Maglione Roberta for their valuable feedback and suggestions.

This work has been partially supported by the Polish Ministry of Science and Higher Education under the European Regional Development Fund, Grant No. POIG.01.01.02-00-045/09-00 (Future Internet Engineering Project).

9. Normative References

[I-D.softwire-ds-lite]


Authors’ Addresses

David W. Hankins
Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
USA

Email: dhankins@google.com

Tomasz Mrugalski
Gdansk University of Technology
Storczykowa 22B/12
Gdansk 80-177
Poland

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