Internet Engineering Task Force
Internet Draft
Expiration Date: July 2005

S. Venaas
University of Southampton

T. Chown
University of Southampton

B. Volz
Cisco Systems, Inc.

January 2005

Information Refresh Time Option for DHCPv6

draft-ietf-dhc-lifetime-03.txt

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, or will be disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

To view the list Internet-Draft Shadow Directories, see http://www.ietf.org/shadow.html

Copyright Notice

Copyright (C) The Internet Society (2005). All Rights Reserved.

Abstract

This document describes a DHCPv6 option for specifying an upper bound for how long a client should wait before refreshing information retrieved from DHCPv6. It is used with stateless DHCPv6 as there are no addresses or other entities with lifetimes that can tell the client when to contact the DHCPv6 server to refresh its configuration.

Table of Contents

1. Introduction 2
2. Terminology 3
3. Information refresh time option definition 3
  3.1. Constants 4
  3.2. Client behaviour 4
  3.3. Server behaviour 5
  3.4. Option format 5
4. IANA Considerations 6
5. Acknowledgements 6
6. Security Considerations 6
7. References 6
  7.1. Normative References 6
  7.2. Informative References 7
Authors' Addresses 7
Intellectual Property and Copyright Statements 7

1. Introduction

DHCPv6 [RFC 3315] specifies stateful autoconfiguration for IPv6 hosts. However, many hosts will use stateless autoconfiguration as specified in [RFC 2462] for address assignment, and use DHCPv6 only for other configuration data, see [RFC 3736]. This other configuration data will typically have no associated lifetime, hence there may be no information telling a host when to refresh its DHCPv6 configuration data. Therefore, an option that can be used from server to client to inform the client when it should refresh the other configuration data is needed.

This option is useful in many situations:

- Unstable environments where unexpected changes are likely to occur.

- For planned changes, including renumbering. An administrator can gradually decrease the time as the event nears.

- Limit the amount of time before new services or servers are available to the client, such as the addition of a new NTP server or a change of address of a DNS server. See [RENUMREQS].

2. Terminology

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 BCP 14, RFC 2119 [RFC 2119].

3. Information refresh time option definition

The information refresh time option specifies an upper bound for how long a client should wait before refreshing information retrieved from DHCPv6. It is only used in Reply messages in response to Information-Request messages. In other messages there will usually be other options that indicate when the client should contact the server, e.g. addresses with lifetimes.

Note that it is only an upper bound. If the client has any reason to make a DHCPv6 request before the refresh time expires, it should attempt to refresh all the data.

A client may contact the server before the refresh time expires. Reasons it may do this include the need for additional configuration parameters (such as by an application), a new IPv6 prefix announced by a router, or that it has an indication it may have moved to a new link.

The refresh time option specifies a common refresh time for all the data. It doesn't make sense to have different refresh time values for different data, since when the client has reason to refresh some of its data, it should also refresh the remaining data. Because of this, the option must only appear in the options area of the Reply message.

The expiry of the refresh time in itself does not in any way mean that the client should remove the data. The client should keep its

current data while attempting to refresh it. The client is however free to fall back to other mechanisms than DHCPv6 if it cannot refresh the data within a reasonable amount of time.

When a client receives a Reply to an Information-Request that contains configuration information, it should install that new configuration information after removing any previously received configuration information. It should also remove information that is missing from the new information set, e.g. an option might be left out or contain only a subset of what it did previously.

3.1. Constants

We define two constants for use by the protocol. How they are used is specified in the sections below.

IRT_DEFAULT 86400
: In some cases the client uses a default refresh time IRT_DEFAULT. The recommended value for IRT_DEFAULT is 86400 (24 hours). The client implementation SHOULD allow for this value to be configurable.

IRT_MINIMUM 600
: This defines a minimum value for the refresh time.

3.2. Client behaviour

A client MUST request this option in the Option Request Option (ORO) when sending Information-Request messages to the DHCPv6 server. A client MUST NOT request this option in the ORO in any other messages.

If the Reply to an Information-Request message does not contain this option, the client MUST behave as if the option with value IRT_DEFAULT was provided.

A client MUST use the refresh time IRT_MINIMUM if it receives the option with a value less than IRT_MINIMUM.

As per section 5.6 of [RFC 3315], the value 0xffffffff is taken to mean "infinity" and implies that the client should not refresh its configuration data without some other trigger (such as detecting movement to a new link).

If a client contacts the server to obtain new data or refresh some existing data before the refresh time expires, then it SHOULD also refresh all data covered by this option.

When the client detects that the refresh time has expired, it SHOULD try to update its configuration data by sending an Information-Request as specified in section 18.1.5 of [RFC 3315], except that the client MUST delay sending the first Information-Request by a random amount of time between 0 and INF_MAX_DELAY.

A client MAY have a maximum value for the refresh time, where that value is used whenever the client receives this option with a value higher than the maximum. This also means that the maximum value is used when the received value is "infinity". A maximum value might make the client less vulnerable to attacks based on forged DHCP messages. Without a maximum value, a client may be made to use wrong information for a possibly infinite period of time. There may however be reasons for having a very long refresh time, so it may be useful for this maximum value to be configurable.

3.3. Server behaviour

A server sending a Reply to an Information-Request message SHOULD include this option if it is requested in the ORO of the Information-Request.

The option value MUST NOT be smaller than IRT_MINIMUM. The server SHOULD give a warning if it is configured with a smaller value.

The option MUST only appear in the options area of Reply messages.

3.4. Option format

The format of the information refresh time option is:

```
 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-code          |           option-len          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    information-refresh-time                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code
    OPTION_INFORMATION_REFRESH_TIME (to be decided)

option-len
    4

information-refresh-time
Time duration relative to the current time, expressed in units of seconds

4. IANA Considerations

IANA is requested to assign an option code for the information refresh time option from the DHCPv6 option-code space [RFC 3315].

5. Acknowledgements

The authors thank Mat Ford, Tatuya Jinmei, Ted Lemon, Thomas Narten, Joe Quanaim and A.K. Vijayabhaskar for valuable discussions and comments.

6. Security Considerations

Section 23 of [RFC 3315] outlines the DHCPv6 security considerations. This option does not change these in any significant way. An attacker could send faked Reply messages with a low information refresh time value, which would trigger use of IRT_MINIMUM to minimize this threat. Another attack might be to send a very large value, to make the client use forged information for a long period of time. A possible maximum limit at the client is suggested, which would reduce this problem.

7. References

7.1. Normative References

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

[RFC 2462] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

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

[RFC 3736] R. Droms, "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

7.2. Informative References

[RENUMREQS] T. Chown, S. Venaas, A.K. Vijayabhaskar, "Renumbering Requirements for Stateless DHCPv6", work-in-progress, draft-ietf-dhc-stateless-dhcpv6-renumbering-01, March 2004.

Authors' Addresses

Stig Venaas
University of Southampton
School of Electronics and Computer Science
Southampton, Hampshire SO17 1BJ
United Kingdom
EMail: sv@ecs.soton.ac.uk

Tim Chown
University of Southampton
School of Electronics and Computer Science
Southampton, Hampshire SO17 1BJ
United Kingdom
EMail: tjc@ecs.soton.ac.uk

Bernard Volz
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA
EMail: volz@cisco.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

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

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgement

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