

Dynamic Host Configuration
Internet-Draft
Expires: April 25, 2005

T. Chown
University of Southampton
S. Venaas
UNINETT
A. Vijayabhaskar
Cisco Systems (India) Private
Limited
October 25, 2004

**Renumbering Requirements for Stateless DHCPv6
draft-ietf-dhc-stateless-dhcpv6-renumbering-02**

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, 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>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on April 25, 2005.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

IPv6 hosts using Stateless Address Autoconfiguration are able to automatically configure their IPv6 address and default router settings. However, further settings are not available. If such hosts wish to automatically configure their DNS, NTP or other specific settings the stateless variant of the Dynamic Host

Configuration Protocol for IPv6 (DHCPv6) could be used. This combination of Stateless Address Autoconfiguration and stateless DHCPv6 could be used quite commonly in IPv6 networks. However, hosts using such a combination currently have no means by which to be informed of changes in stateless DHCPv6 option settings, e.g. the addition of a new NTP server address, a change in DNS search paths, or full site renumbering. This document is presented as a problem statement from which a solution should be proposed in a subsequent document.

Table of Contents

- [1. Introduction](#) [3](#)
- [2. Problem Statement](#) [3](#)
- [3. Renumbering Scenarios](#) [4](#)
 - [3.1 Site renumbering](#) [4](#)
 - [3.2 Changes to a DHCPv6-assigned setting](#) [4](#)
- [4. Renumbering Requirements](#) [4](#)
- [5. Considerations in choosing a solution](#) [5](#)
- [6. Solution Space](#) [5](#)
- [7. Summary](#) [6](#)
- [8. Security Considerations](#) [6](#)
- [9. Acknowledgements](#) [6](#)
- [10. References](#) [6](#)
 - [10.1 Normative References](#) [6](#)
 - [10.2 Informative References](#) [7](#)
- [Authors' Addresses](#) [7](#)
- [Intellectual Property and Copyright Statements](#) [8](#)

1. Introduction

IPv6 hosts using Stateless Address Autoconfiguration [[1](#)] are able to automatically configure their IPv6 address and default router settings. While Stateless Address Autoconfiguration for IPv6 allows automatic configuration of these settings, it does not provide a mechanism for additional, non IP-address settings to be automatically configured.

The full version of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [[2](#)] is designed to provide both stateful address assignment to IPv6 hosts, as well as additional (non IP-address) configuration including DNS, NTP and other specific settings. A full stateful DHCPv6 server allocates the addresses and maintains the clients bindings to keep track of client leases.

If hosts using Stateless Address Autoconfiguration for IPv6 wish to automatically configure their DNS, NTP or other specific settings the stateless variant [[3](#)] of DHCPv6 could be used. The stateless variant of DHCPv6 is more lightweight. It does not do address assignment, instead it only provides additional configuration parameters like DNS resolver addresses. It does not maintain state about the information assigned to clients, hence there is no need to maintain per-client state on the server. In other words, all clients can be given the same information, in the same way that the information in Router Advertisements is not client-specific.

This combination of Stateless Address Autoconfiguration and stateless DHCPv6 could be used quite commonly in IPv6 networks.

2. Problem Statement

A problem however lies in the ability, or lack of ability, of clients using this combination to be informed of (or to deduce) changes in DHCPv6 assigned settings.

While a DHCPv6 server unicasts Reconfigure message to individual clients to trigger the clients to initiate Information-request/reply configuration exchanges to update their configuration settings, the stateless variant of DHCPv6 cannot use the Reconfigure mechanism because it does not maintain a list of IP addresses (leases) to send

the unicast messages to. Note that in DHCPv6, Reconfigure messages must be unicast; multicast is not allowed.

Thus events including the following cannot be handled:

- o Full site renumbering

- o DNS server change of address

- o NTP server change of address

- o A change in DNS search paths

It would be highly desirable that a host using the combination of Stateless Address Autoconfiguration and stateless DHCPv6 could handle a renumbering or reconfiguration event, whether planned or unplanned by the network administrator.

Note that the scope of the problem can also be seen to extend beyond Stateless DHCPv6, since only IP address options have a lifetime, i.e. there is no mechanism even in the full DHCPv6 to "expire" old information or otherwise force a client to recheck that new/updated information is available. However, with full DHCPv6, a node may learn of updates to non-address options when renewing its address lease.

3. Renumbering Scenarios

There are two main scenarios for changes to DHCPv6-assigned settings, that would require the client to initiate an Information-request/reply exchange to update the configuration.

3.1 Site renumbering

One of the fundamental principles of IPv6 is that sites receive their IPv6 address allocations from an ISP using provider assigned (PA) address space. There is currently no provider independent (PI) address space in IPv6. A site changing its ISP must thus renumber its network. Any such site renumbering will require hosts to reconfigure both their own address and default router settings as well as their stateless DHCPv6-assigned settings.

3.2 Changes to a DHCPv6-assigned setting

An administrator may need to change one or more stateless DHCPv6-assigned settings, e.g. an NTP server, DNS server, or the DNS

search path. This may be required if a new, additional DNS server is brought online, is moved to a new network (prefix), or an existing server is decommissioned or known to be unavailable.

4. Renumbering Requirements

Ideally, any of the above scenarios should be handled automatically by the hosts on the network. For this to be realised, a method is required for the hosts to be informed that they should request new

stateless DHCPv6-assigned setting information.

The solution to the problem may depend on whether the renumbering or configuration change is a planned or unplanned one, from the perspective of the network administrator. There is already work underway in understanding the planned renumbering [4] scenario for IPv6 networks. However, there is currently no mechanism in stateless DHCPv6 to even handle planned renumbering events.

5. Considerations in choosing a solution

There are a number of considerations that could be listed for a desirable solution:

- o The solution should support planned renumbering; it is desirable that it also supports unplanned renumbering.
- o Security is important. No new security concerns should be introduced to Stateless DHCPv6 by the solution.
- o It must be possible to update options even if the network is not renumbered.
- o It is desirable to maintain the "stateless" property; i.e., no per-client state should need to be kept in the server.

6. Solution Space

Solutions should be designed and presented in a separate document. An initial, brief set of candidate solutions might include:

- o Adding a Reconfigure message mechanism that would work in the stateless DHCPv6 environment. This could enable planned or unplanned events, but may require a multicast mechanism to be realised.
- o Conveying a valid lifetime timer to clients for stateless

DHCPv6-assigned settings. This could primarily enable planned events, but with a small time-out it could to some extent handle unplanned events at the expense of the additional request traffic. The selection of recommended lifetime values/ranges would be the subject of future work.

- o Using some form of Router Advertisement as a hint to request new stateless DHCPv6-assigned settings. Using only an observed new Router Advertisement prefix as a hint to re-request settings would not handle changes that are purely to NTP, DNS or other options.

Other possible means of detection of network (re)attachment could also be used as cues (e.g. see IPv6 DNA Goals [5]).

- o Changing semantics of the DHCPv6 'O' flag such that toggling its value may trigger an Information-request message.

There will also be conditions under which a client should also send an Information-request, such as reconnection to a link. Such specific recommendations are outside the scope of this document but we expect ongoing work in the Detecting Network Attachment (DNA) WG (as scoped in IPv6 DNA Goals [5]) to yield recommendations.

7. Summary

This document presents a problem statement for how IPv6 hosts that use the combination of Stateless Address Autoconfiguration and stateless DHCPv6 may be informed of renumbering events or other changes to the settings that they originally learnt through stateless DHCPv6. A short list of candidate solutions is presented, which the authors hope may be expanded upon in subsequent documents.

8. Security Considerations

There are no security considerations in this problem statement per se. However, whatever mechanism is designed or chosen to address this problem should avoid the introduction of new security concerns for (stateless) DHCPv6.

The issues of maintaining appropriate security through a renumbering event are outside the scope of this document (in the case where specific servers within the network are being added or removed, firewall configurations and ACLs, for example, will need to reflect this). However, this is an important area for further work.

9. Acknowledgements

The authors would like to thank Ralph Droms, Bermie Volz and other individuals on the DHC mail list for their comments on this draft, as well as colleagues on the 6NET project. We also thank the review comments, particularly those from Thomas Narten.

10. References

10.1 Normative References

- [1] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", [RFC 2462](#), December 1998.

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

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

10.2 Informative References

- [4] Baker, F., Lear, E. and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", [draft-ietf-v6ops-renumbering-procedure-01](#) (work in progress), July 2004.

- [5] Choi, J., "Detecting Network Attachment in IPv6 Goals", [draft-ietf-dna-goals-03](#) (work in progress), October 2004.

Authors' Addresses

Tim Chown
University of Southampton
School of Electronics and Computer Science
Southampton, Hampshire S017 1BJ
United Kingdom

EEmail: tjc@ecs.soton.ac.uk

Stig Venaas
UNINETT
Trondheim NO 7465
Norway

EEmail: venaas@uninett.no

Vijayabhaskar A Kalusivalingam
Cisco Systems (India) Private Limited

9, Brunton Road
Bangalore 560025
India

E-Mail: vibhaska@cisco.com

Chown, et al.

Expires April 25, 2005

[Page 7]

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 (2004). 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.

Acknowledgment

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

Chown, et al.

Expires April 25, 2005

[Page 8]