Dynamic Host Congiguration   T. Chown
Internet-Draft   University of Southampton
Expires: August 30, 2004   S. Venaas
                                                                 UNINETT
                                                       A. Vijayabhaskar
                                              Hewlett-Packard STSD-I
                                                              March 2004

Renumbering Requirements for Stateless DHCPv6
draft-ietf-dhc-stateless-dhcpv6-renumbering-01

Status of this Memo

Copyright Notice

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, changes 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

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; the additional parameters do not have an explicit life-time associated with them in the same way that IP addresses do, and hence the DHCPv6 server does not need to maintain the state of the clients.

This combination of Stateless Address Autoconfiguration and stateless DHCPv6 could be used quite commonly in IPv6 networks. In the absence of an alternative method for DNS, NTP and other options to be automatically configured, it may become the most common combination for statelessly configuring hosts.

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 intiate 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.

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 Changes 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.

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 wishing to change 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.

The unplanned renumbering event, which may be more common in smaller, unmanaged networks, is more difficult to cater for. Ideally, any solution for the problem should consider planned and unplanned events.

The solution should also be secure, such that additional security concerns are not added to the stateless DHCPv6 networking environment.

5. Considerations in choosing a solution

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

- o It should support planned renumbering; it is desirable to support unplanned renumbering.
- o Security is important; e.g., avoiding denialof service attacks mounted through Reconfigure messages sent from an attacker.
- 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.
- 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.

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 statemement per se. However, whatever mechanism is designed or chosen to address this problem should avoid the introduction of new security concerns for (stateless) DHCPv6.

9. Acknowledgements

The authors would like to thank Ralph Droms and Bermie Volz for their comments on this draft.

10 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.

[4] Baker, F., Lear, E. and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", draft-baker-ipv6-renumber-procedure-01 (work in progress), October 2003.

[5] Choi, J., "Detecting Network Attachment in IPv6 Goals", draft-ietf-dna-goals-00 (work in progress), June 2004.

Authors' Addresses

Tim Chown
University of Southampton
School of Electronics and Computer Science
Southampton, Hampshire SO17 1BJ
United Kingdom

EMail: tjc@ecs.soton.ac.uk

Stig Venaas
UNINETT
Trondheim NO 7465
Norway

EMail: venaas@uninett.no

Vijayabhaskar A K
Hewlett-Packard STSD-I
29, Cunningham Road
Bangalore 560052
India

EMail: vijayak@india.hp.com

Acknowledgment

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