Network Working Group
Request for Comments: 4076
Category: Informational

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

May 2005

Renumbering Requirements for Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

Status of This Memo

Copyright Notice

Abstract

IPv6 hosts using Stateless Address Autoconfiguration are able to configure their IPv6 address and default router settings automatically. However, further settings are not available. If these hosts wish to configure their DNS, NTP, or other specific settings automatically, 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 this 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

IPv6 hosts using Stateless Address Autoconfiguration [2] are able to configure their IPv6 address and default router settings automatically. Although 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 configured automatically.

The full version of the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [3] 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 configure their DNS, NTP, or other specific settings automatically, the stateless variant [4] of DHCPv6 could be used. This variant is more lightweight. It does not do address assignment; instead, it only provides additional configuration parameters, such as DNS resolver addresses. It does not maintain dynamic state about the information assigned to clients, and therefore there is no need to maintain dynamic per-client state on the server.

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 messages to individual clients to trigger them 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:

- Full site renumbering
- DNS server change of address
- NTP server change of address
- 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 could extend beyond Stateless DHCPv6, since only IP address options have a lifetime; i.e., there is no mechanism even in the full DHCPv6 that "expires" old information or otherwise forces 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. Therefore, a site changing its ISP must renumber its network. Any such site renumbering will require hosts to reconfigure both their own address and default router settings and 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 and is moved to a new network (prefix), or if 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 whereby the hosts are 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 planned or unplanned, from the perspective of the network administrator. There is already work underway toward understanding the planned renumbering [5] scenario for IPv6 networks. However, there is currently no mechanism in stateless DHCPv6 for handling planned renumbering events.

5. Considerations in Choosing a Solution

A number of considerations could be listed for a desirable solution:

- The solution should support planned renumbering; it is desirable that it also supports unplanned renumbering.
- Security is important. No new security concerns should be introduced to Stateless DHCPv6 by the solution.
- It must be possible to update options, even if the network is not renumbered.
- 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 the following:

- Add 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 in order to be realised.

- Convey 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 handle unplanned events to some extent at the expense of the additional request traffic. The selection of recommended lifetime values/ranges would be the subject of future work.

- Use some form of Router Advertisement (RA) [1] as a hint to request new stateless DHCPv6-assigned settings. Using only an observed new RA 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 Goals of Detecting Network Attachment (DNA) in IPv6 [6]).

- Change the semantics of the 'O' flag in RAs [2] so that toggling its value may trigger an Information-request message.

There will also be conditions under which a client should send an Information-request, such as reconnection to a link. Recommendations for these cases are outside the scope of this document, but we expect ongoing work in the DNA WG (as scoped in Goals of Detecting Network Attachment (DNA) in IPv6 [6]) 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 learned through stateless DHCPv6. A short list of candidate solutions is presented, which the authors hope will 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 introducing new security concerns for (stateless) DHCPv6.

The issues of maintaining appropriate security through a renumbering event are outside the scope of this document (if 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, Bernie Volz, and other individuals on the DHC mail list for their comments on this document, 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] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

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

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

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

10.2. Informative References

[5] Baker, F., Lear, E. and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", Work in Progress, July 2004.

[6] Choi, J., "Goals of Detecting Network Attachment (DNA) in IPv6", Work in Progress, October 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 Kalusivalingam
Cisco Systems (India) Private Limited
9, Brunton Road
Bangalore 560025
India

EMail: vibhaska@cisco.com

Full Copyright Statement

Intellectual Property

Acknowledgement

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