Dynamic Host Congiguration
Internet-Draft
Expires: August 9, 2004

T. Chown
University of Southampton
S. Venaas
UNINETT
C. Strauf
JOIN (University of Muenster)
February 9, 2004

IPv4 and IPv6 Dual-Stack Issues for DHCPv6
draft-chown-dhc-dual-stack-00

Status of this Memo

Copyright Notice

Abstract

A node may have support for communications using IPv4 and/or IPv6 protocols. Such a node may wish to obtain IPv4 and/or IPv6 configuration settings via the Dynamic Host Configuration Protocol (DHCP). The original version of DHCP [1] designed for IPv4 has now been complemented by a new DHCPv6 [4] for IPv6. This document describes issues identified with dual IP version DHCP interactions.

Table of Contents

1. Introduction 3
2. Configuration scenarios 3
3. Dual-stack issues 4
3.1 Handling multiple responses 4
3.2 Multiple interfaces 4
3.3 DNS load balancing 5
3.4 DNS search path issues 5
3.5 Administrative management 5
3.6 DHCP option variations 5
3.7 Security issues 5
4. Potential solutions 6
4.1 Separate DHCP servers 6
4.2 Single DHCPv6 server 6
4.3 Administrative and other areas 7
5. Summary 7
6. Security Considerations 7
Normative References 7
Authors' Addresses 8
Intellectual Property and Copyright Statements 9

1. Introduction

The original specification of the Dynamic Host Configuration Protocol (DHCP) was made with only IPv4 in mind. That specification has been subsequently revised, up to the latest version of DHCP [1]. With the arrival of IPv6, a new DHCP specification for IPv6 has been designed, and published as DHCPv6 [4].

These protocols allow nodes to communicate via IPv4 or IPv6 to retrieve configuration settings for operation in a managed environment. While an IPv6 node may acquire address-related configuration settings via IPv6 stateless address autoconfiguration [2], such a node may wish to use stateless DHCPv6 [5] for other administratively configured options (e.g. DNS, NTP).

In early IPv6 deployments, a dual-stack mode of operation is typically used. There will thus be nodes that require both IPv4 and IPv6 configuration settings. This document discusses issues with obtaining such settings in a dual-stack environment.

In this document, we refer to a "DHCP server" as a server implementing the original DHCP [1], and a "DHCPv6 server" as a server implementing DHCPv6 [4] or its stateless subset.

2. Configuration scenarios

For a node in an IPv4-only or IPv6-only environment, the choice of DHCP server is a straightforward one; a DHCP server for IPv4, or a DHCPv6 server for IPv6.

In a dual-stack environment a node in a managed environment will need to obtain both IPv4 and IPv6 configuration settings, e.g.

- IPv4 address

- IPv6 address
- NTP server
- DNS server
- NIS server
- DNS search path

While the format of address settings will be IP-specific, the node may equally well acquire IPv4 or IPv6 addresses for some settings, e.g. for DNS or NTP, if those services are available via IPv4 or IPv6

transport. Currently, a DHCP server returns IPv4 data, while a DHCPv6 server returns IPv6 data.

It is worth noting that in an IPv4 environment, with a DHCP server, the choice of whether to use DHCP is made by the node. In an IPv6 environment, the use of the managed and other bits in the Router Advertisement can tell the node whether or not to use DHCPv6. It is perhaps not clear whether a dual-stack node should do DHCP for IPv4 if Managed and OtherConfig flags in the Router Advertisement are both off; it seems most appropriate that the decision to use DHCP for IPv4 or not should be as if the host was IPv4-only.

3. Dual-stack issues

In this section we list issues that have been raised to date related to dual-stack DHCP operation.

3.1 Handling multiple responses

The general question is how to handle configuration information that may be gathered from multiple sources. Where those sources are DHCP and DHCPv6 servers (which may be two physical nodes or two servers running on the same node) the client node needs to know whether to use the most recent data, or whether to perform some merger or union of the responses by certain rules. A node may choose to ask a DHCPv6 server and only use a DHCP server if no response is received.

Merging is possible, but is likely to be complex. There could be

some priority, so that if both DHCP and DHCPv6 servers offer a value, only one is used. Or the node could choose to store and use both, in some order of its choosing.

A node may also obtain information from other sources, e.g. a manual configuration file (e.g. /etc/resolv.conf for DNS data on many Unix systems). A node configured manually to use an IPv6 DNS server via such manual configuration may lose that configuration if it then uses DHCP to obtain IPv4 settings if in a dual-stack environment; that IPv4 configuration may then overwrite the manual IPv6 DNS setting with new IPv4 settings from the DHCP response.

3.2 Multiple interfaces

A node may have multiple interfaces and run IPv4 and IPv6 on different interfaces. A question then is whether the settings are per interface or per node? DHCPv6 introduces the idea of a DHCP Unique Indentifer (DUID) which does not yet exist for DHCP; some effort is being made to retrofit the concept to DHCP [6].

Per interface settings can be complex because a client node needs to know from which interface system settings like NTP server came from. And it may not be apparent which setting should be used, if e.g. an NTP server option is received on multiple interfaces, potentially over different protocols.

3.3 DNS load balancing

In some cases it is preferable to list DNS server information in an ordered way per node for load balancing, giving different responses to different clients. Responses from different DHCP and DHCPv6 servers may make such configuration problematic.

3.4 DNS search path issues

The DNS search path may vary for administrative reasons. For example, a site under the domain foo.com chooses to place an early IPv6 deployment under the subdomain ipv6.foo.com, until it is confident of offering a full dual-stack service under its main domain. The subtlety here is that the DNS search path then affects choice of protocol used, e.g. IPv6 for nodes in ipv6.foo.com.

3.5 Administrative management

In some deployments, the IPv4 and IPv6 services may not be administered by the same organisation or people, e.g. in a community wireless environment. This poses problems for consistency of data offered by either DHCP version.

3.6 DHCP option variations

Some options in DHCP are not available in DHCPv6 and vice-versa. Some IP-version limitations naturally apply, e.g. only IPv6 addresses can be in an IPv6 NTP option. The DHCP and DHCPv6 option numbers may be different.

A site administrator may wish to configure all their dual-stack nodes with (say) two NTP servers, one of which has an IPv4 address, the other an IPv6 address. In this case it may be desirable for an NTP option to carry a list of addresses, where some may be IPv4 and some may be IPv6. In general one could consider having DHCPv6 options that can carry mix of IPv4 and IPv6 addresses.

3.7 Security issues

At this stage in the formation of this draft no specific security issues have been raised. The authors welcome comments on this, should such issues exist.

While there is a specification for authentiation for DHCP messages [3], the standard seems to have very few, if any, implementations. Thus DHCP and DHCPv6 servers are still liable to be spoofed. Adding an additional protocol may give an extra avenue for attack, should an attacker perhaps spoof a DHCPv6 server but not a DHCP server.

4. Potential solutions

While this document did not originally intend to have solutions in its scope, we discuss potential solution spaces in brief here in order to provoke some discussion of the issues. If separate solution document(s) emerge, these notes may be removed from this document; alternatively this document could be expanded to become a best practice guide. Comments on this are welcomed.

4.1 Separate DHCP servers

One solution is to run separate DHCP and DHCPv6 servers. These may or may not be run on the same physical node.

In this approach, some best practice guidance is required for how multiple responses are handled or merged. Administrators have the onus to maintain consistency (e.g. scripts may generate common DHCP and DHCPv6 configuration files).

In some cases, inconsistencies may not matter. In a simple case, an NTP server will give the same time whether accessed by IPv4 or IPv6. Even if different recursive DNS servers are offered via DHCP or DHCPv6, those name servers will provide the same response to a given query. The order of DNS servers in a node's configuration is not important, unless DNS load balancing is required.

In the case of separate servers, there are some options like DNS search path, that aren't used in a specific IP protocol context.

It is worth noting that there has been little effort to date to agree a common method for IPv6 nodes to acquire non-address settings via DHCPv6 because in most dual-stack environments a node will acquire its DNS settings via DHCP and query a local (perhaps dual-stack) resolver.

4.2 Single DHCPv6 server

There is an argument for not having to configure and operate both DHCP and DHCPv6 servers. The use of both servers may also lead to some redundancy in the information served. Thus one solution may be to modify DHCPv6 to be able to return IPv4 information. This solution is hinted at in the DHCPv6 [4] specification: "If there is

sufficient interest and demand, integration can be specified in a document that extends DHCPv6 to carry IPv4 addresses and configuration information." This solution may allow DHCP for IPv4 to be completely replaced by DHCPv6 with additional IPv4 information options, for dual-stack nodes.

This approach may require the listing of a mix of IPv4 and IPv6

addresses for an option. This should be considered when new IPv6 options are introduced.

One problem with this approach is that the client node may then be IPv6-only and receiving IPv4 configuration settings that it does not want or be able to meaningfully handle.

4.3 Administrative and other areas

There are also administrative issues or best practice that could be promoted. For example, it may be recommended that sites do not split their DNS name space for IPv6-specific testbeds.

It may be worth considering whether separate manual configuration files should be kept for IPv4 and IPv6 settings, e.g. separate /etc/resolv.conf files for DNS settings on Unix systems. However, this seems a complex solution that should be better solved by other more generalised methods.

Some differences in DHCP and DHCPv6 may not be reconciled, but may not need to be, e.g. different ways to assign addresses by DUID in DHCPv6, or the non-aligned option numbers for DHCP and DHCPv6.

5. Summary

There are a number of issues in the operation of DHCP and DHCPv6 servers for nodes in dual-stack environments that should be clarified. While some differences in the protocols may not be reconciled, there may not be a need to do so. However, for general operation some best practice should be agreed, the principle choice being whether separate DHCP and DHCPv6 servers should be maintained by a site, or whether DHCPv6 should be extended to carry IPv4 configuration settings for dual-stack nodes.

6. Security Considerations

There are no security considerations in this problem statemement per se, as it does not propose a new protocol.

Normative References

[1] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

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

[3] Droms, R. and W. Arbaugh, "Authentication for DHCP Messages", RFC 3118, June 2001.

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

[5] Droms, R., "A Guide to Implementing Stateless DHCPv6 Service", draft-ietf-dhc-dhcpv6-stateless-01 (work in progress), October 2003.

[6] Lemon, T., "Node-Specific Client Identifiers for DHCPv4", draft-ietf-dhc-3315id-for-v4-00 (work in progress), October 2003.

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

Christian Strauf
JOIN (University of Muenster)
Roentgenstr. 9-13
Muenster D-48149
Germany

EMail: strauf@uni-muenster.de

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

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