

Network Working Group
Internet-Draft
Expires: August 30, 2002

R. Droms
Cisco Systems
T. Narten
IBM Corporation
B. Aboba
Microsoft
Mar 2002

Using DHCPv6 for DNS Configuration in Hosts
draft-droms-dnsconfig-dhcpv6-01.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

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 August 30, 2002.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

An IPv6 device can configure its addresses and locate neighboring routers through stateless address autoconfiguration ([RFC2462](#)) and router discovery ([RFC2461](#)). Most IPv6 devices will require information about DNS services to make use of the basic IPv6 connectivity. The current version of DHCPv6 already supports the features needed to provide a simple DNS configuration mechanism. DNS configuration requires only a small subset of the DHCPv6 protocol and can be provided through relatively simple client and server

implementations.

[1](#). Introduction

An IPv6 device configures its IPv6 addresses through stateless address autoconfiguration [[3](#)] and/or through DHCP [[5](#)]. In addition, Neighbor Discovery [[2](#)] provides an IPv6 device with a set of neighboring routers it can use. With addresses and a list of neighboring routers, a node has IP-level connectivity to the Internet.

In many cases, packet-level connectivity is not enough. Devices typically also need to be configured to be able to use DNS [[1](#)]. Needed DNS configuration information can include the address of one or more DNS servers, the DNS name of the device itself, a list of DNS domain names to append to queries to make them fully qualified, etc. Specifically, [Section 2](#) of the DNS Discovery team report [[4](#)], defines the information for DNS name resolution to be:

- o One or more addresses of DNS servers. If a list is obtained, a client need only rediscover DNS servers if all addresses in the list are unreachable. However, if a list is obtained from a single point, such as one of the DNS servers, then a requirement exists that the list of servers be up-to-date and easily maintainable.
- o Domain name
- o Search path. It is currently common practice, for the search path to be computed by a device based on its domain name obtained. However, a DHCPv6 option [[5](#)] is being proposed in the DHC WG, and so search path configuration is likely to be a requirement in general.

This document describes how to use DHCPv6 messages to obtain DNS configuration information without necessarily requiring a "stateful" DHCPv6 server to perform address assignment.

[2](#). Terminology

DHCP - Dynamic Host Configuration Protocol; unless otherwise qualified, "DHCP" refers to DHCP for IPv6

DHCP option - A component of a DHCP message that carries configuration information for a DHCP client

Configuration information - Information used by the host to configure its IP stack, DNS name resolver, etc.

DNS configuration information - Configuration information used specifically to configure a DNS name resolver, including the addresses of DNS servers, the host's domain name and a search list for name resolution

[3.](#) Summary of DHCP operation

DHCPv6 is conceptually similar to DHCP for IPv4 [\[7\]](#). DHCPv6 can provide configuration that includes address assignment, where the DHCP server selects an address for each DHCP client and maintains state about the assignment of that address to the client.

DHCPv6 also provides configuration parameters to clients that do not need to have an address assigned. This mode of operation is expected to be much more widely used than in IPv4 networks, because hosts can use stateless autoconfiguration to select IPv6 addresses rather than depending on a DHCP server or manual configuration.

A host that has selected IPv6 addresses through stateless autoconfiguration uses a single message exchange with a DHCP server to obtain configuration information. As in DHCPv4, the host sends a message to a well-known multicast address to contact a DHCP server. The server may return the same configuration information to every client, or it may be configured with policies to return customized information to groups of hosts or even individual hosts. Each message exchange is independent of other message exchanges so that the server need not retain any dynamic state about each host.

The DHCP specification allows for the coexistence of clients using DHCP for stateful address assignment and clients using DHCP for obtaining configuration information. DHCP clients use different messages for configuration and for stateful address assignment, and a server that receives a stateful configuration request does not respond if it is not configured for stateful configuration. Thus,

even if DHCP messages are multicast to all DHCP servers, only those servers performing stateful address assignment will respond to requests for address assignment through DHCP.

Because a DHCP server may be designed to respond only to Information-Request messages, it is possible to implement a DHCP server that is much less complex than a server that provides stateful address assignment. A DHCP server that provides only DNS configuration information is easier to set up during deployment and requires fewer computational resources. As discussed in [Section 5.1](#), a DHCP server for DNS configuration information can be designed to be almost completely self-configuring. Similarly, a DHCP client that uses only Information-Request messages to obtain other configuration

information would be much simpler than a client that uses DHCP for address assignment.

[4.](#) Client Behavior for DNS Configuration through DHCP

When a host boots, it starts by generating a link-local address and then soliciting a Router Advertisement. Use of DHCP by IPv6 hosts is controlled through two flags in Router Advertisements:

- M - if TRUE, the host invokes stateful autoconfiguration (DHCP) to configure additional addresses. (It may have already configured some address through stateless address autoconfiguration.)
- O - if TRUE, the host obtains other configuration (e.g, non-address) information through DHCP

If the 'M' bit is set TRUE, the host obtains its address through stateful address assignment using DHCP. The host will also obtain other configuration through the same message exchange with the DHCP service. Thus, if the 'M' bit is TRUE, the host will always obtain all of its configuration through DHCP.

If the 'M' bit is set FALSE, the host uses stateless address autoconfiguration exclusively for address assignment. If the 'O' bit is set TRUE in this case, the host will obtain its DNS configuration (and, perhaps, other configuration information) through DHCP. In this case a host will perform the following steps:

1. Send a DHCP Information-Request message to a well-known multicast address requesting DNS configuration information.
2. Wait for the corresponding DHCP Reply message.
3. Extract the DNS configuration information from the Reply message and use it to configure local host behavior with regards to DNS resolution.

If the host is using DHCP for DNS configuration, the DHCP specification allows the host to send DHCP Information-Request messages at times other than just once at boot time. For example, a host may poll the DHCP service periodically to obtain a more up-to-date list of DNS servers. Alternatively, if no servers in the host's current list of DNS servers is responding, the host may choose to send a DHCP Information-Request message to refresh its list of servers to find one that is available. The point here is that DHCP already provides mechanisms to obtain DNS configuration, the mechanism involves a single request/response message, and can be invoked as needed to refresh a client's configuration information.

[5.](#) DHCP service for DNS configuration

To meet the requirements of a host using DHCP for DNS configuration, the DHCP service must return a Reply message in response to an Information-Request message received from the client. The Reply message will contain just the options supplying DNS configuration information.

The capability to carry DNS configuration information already exists in the DHCP specification. As described in the previous section, a host uses the Information-Request message to request configuration information without stateful address assignment. The DHCP specification includes three options for carrying DNS configuration [\[8\]](#):

Domain Name Server option: provides a list of Domain Name System that a client name resolver can use to access DNS services

Domain Name option: informs the DHCP client of its domain name

Domain Search option: provides a list of domain names a client

can use to resolve DNS names

The following sections describe several scenarios in which the requirements for DHCP service in DNS configuration can be met through different configurations of DHCP servers.

[5.1](#) Minimal DHCP servers for DNS configuration

One obvious way to provide DHCP service is to place a DHCP server on every router. Except in the case of a network composed of a single link, every link has at least one router that is already providing router advertisement service in addition to forwarding packets.

Adding DHCP service for DNS configuration to a router does not add unreasonable complexity in terms of implementation or performance, especially for a reduced functionality server that only supplies DNS configuration information. Responding to an Information-Request message requires only the formation and transmission of a Reply message. The contents of every Reply message is the same and contains just the DNS configuration information.

Note that the market in IPv4 has already demonstrated the feasibility of this approach. It is common now for off-the-shelf small routers to provide NAT & DHCP services, requiring little or no configuration by end users. There is no reason to believe that this would be different in IPv6 with DHCPv6, especially considering that the IPv4 implementations are fully functional DHCP servers doing stateful

address assignment.

One question is how would the router determine what DNS configuration information it should advertise through DHCP. The answer is it can determine this in any of several different ways. In the strictly zeroconf manner, this information might come from an upstream ISP. But that ISP can provide the information to the router through DHCP, or whatever mechanism it uses to provide configuration information to the router. (After all, the router needs, for example, a public IP address on the ISP side.) Thus, there is no special problem here that wouldn't also exist in any protocol the provides DNS configuration, and there are a number of ways this could be done without requiring end-user configuration.

[5.2](#) DHCP service provided by DNS servers

Another deployment scenario is to provide DHCP server in a DNS server. In this scenario, the DNS server is extended with the capability to receive Information-Request messages and respond with Reply messages. DHCP would be used as the format to carry the configuration information obtained directly from the DNS server.

In this scenario, a host uses the DHCP Information-Request message to poll for available DNS servers, and builds a list of DNS servers by merging the DNS server addresses in the responses. As described in [Section 4](#), a client can use the Information-Request message to manage its list of available DNS servers dynamically.

Providing DHCP service with DNS servers requires that DHCP Information-Request messages be forwarded across multiple links from the host to the server. The DHCPv6 specification defines a DHCP Relay Agent that receives DHCP messages sent to a link-local multicast address and forwards those messages to DHCP servers. Relay Agents usually reside in routers and are therefore readily available on every link.

DHCP Relay Agents must be deployed and managed so that they are configured with the addresses of DHCP servers. To avoid the overhead of managing DHCP Relay Agents on every link, a host that has used stateless autoconfiguration to determine addresses with site or global scope can use the site local "All DHCP Servers" multicast address to send a DHCP Inform message to DHCP servers without using a local DHCP Relay Agent.

[5.3](#) DHCP servers co-located with DNS servers

A similar deployment scenario is to co-locate DHCP service with a DNS server. The DHCP service returns information about its associated

DNS server, and only responds to messages from hosts if the DNS server is available.

[5.4](#) DHCP servers providing both address assignment and configuration information

A site that is providing address assignment to some DHCP clients can

use the same DHCP server to provide configuration information to hosts that use stateless address autoconfiguration. The DHCP specification allows a server to be configured with policies that allow it to provide address assignment to some clients while providing DNS configuration information to other clients. Thus, the site need not have two different sets of DHCP servers for the two types of DHCP service.

6. Coexistence of DHCP servers

A site may have a mix of hosts using DHCP in three different ways: address assignment; DNS configuration; configuration information including DNS configuration and other parameters. The DHCP service Infrastructure may be mixed, with DNS-only servers in some routers or DNS servers as well as DHCP servers providing address assignment and other parameters. Further, because of DHCP relay agent configuration or use of multicast, a message from any client may be delivered to any server. From the point of view of the host, these servers co-exist as follows:

Address assignment: Hosts requesting address assignment use DHCP Solicit, Request, Renew, and Rebind messages. The DHCP specification requires that servers that do not assign addresses - in particular, DHCP servers doing just DNS configuration - ignore these messages. Routers that have both a relay agent and a DHCP DNS configuration server forward address assignment messages to full DHCP servers. These servers then respond, so clients asking for address assignment receive responses only from configuring servers.

Full configuration: Hosts asking for configuration information specify a list of the information of interest. Any server with corresponding information may respond. Servers providing only DNS configuration won't have all of the requested information and may choose not to respond. If a server providing only DNS configuration does respond, the host has the option to ignore the reply and choose another response from a DHCP server that supplies more complete information.

DNS-only configuration: A host requesting only DNS configuration will identify those DNS configuration options in the Information-

Request message it sends. Any server configured to respond to this host will do so. If the server sends back additional information, clients may choose to ignore the extra information.

7. Open Issues

There are three open issues for the DHCPv6 specification raised by this document:

Site-scoped multicast: The most recent DHCPv6 specification only allows a client to send an Information-Request message to the link-scoped "All_DHCP_Agents" multicast address or to a server's unicast address. To allow for discovery of DHCP servers without the use of relay agents, a client could use the site-scoped "All_DHCP_Servers" multicast address.

DNS and DHCP on one computer: A DNS server providing DNS configuration through DHCP and a DHCP server will experience a conflict in the use of the well-known DHCP port numbers.

Authentication: DHCP includes a framework for authentication of DHCP messages. Use of authentication with DNS configuration will be important because of the potential spoofing attack that can be mounted through the DNS search path. It may be possible to improve on DHCP authentication through the use of IPSEC.

8. Conclusion and Recommendations

DHCP can be used for DNS configuration of hosts. The stateless version of DHCP, in which a host can obtain DNS configuration from a server with a two message exchange, imposes minimal implementation overhead. The configuration of a DHCP server providing DNS configuration information can be automated to minimize deployment and management overhead.

Using an existing protocol has several advantages over designing and deploying a special-purpose protocol for DNS configuration of hosts. Using DHCP will minimize deployment complexity, allowing a site to reuse a single protocol infrastructure for host configuration that will likely be deployed at most sites. Sites with both protocols deployed will have to carefully coordinate the administration of the two protocols to avoid giving conflicting information to hosts. If a second protocol is available, sites will have to decide which to deploy and how to upgrade to DHCP if necessary. Specifying a new protocol for DNS configuration will require analysis of interactions

between the new protocol and DHCP, as well as careful specification of client behavior in the case both sources of DNS configuration information are available.

Almost all of the functions required for using DHCP for DNS configuration are already specified in the latest version of the DHCP document [5]. The open issues are discussed in [Section 7](#) of this document.

Because DHCP can meet the requirements for DNS configuration of hosts,, and because the deployment and management of DHCP for this purpose can be accomplished with minimum overhead, we recommend that DHCP be adopted as standard mechanism for DNS configuration. This recommendation should be documented, along with recommended implementations and deployment strategies, in an Applicability Statement or BCP document.

References

- [1] Mockapetris, P., "Domain names - concepts and facilities", STD 13, [RFC 1034](#), November 1987.
- [2] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", [RFC 2461](#), December 1998.
- [3] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", [RFC 2462](#), December 1998.
- [4] Aboba, B., Bound, J., Deering, S., Guttman, E., HAGINO, J., Hinden, R., JINMEI, T., Onoe, A., Soliman, H. and D. Thaler, "Analysis of DNS Server Discovery Mechanisms for IPv6", [draft-ietf-ipngwg-dns-discovery-analysis](#) (work in progress), July 2001.
- [5] Bound, J., Carney, M., Perkins, C. and R. Droms (ed.), "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [draft-ietf-dhc-dhcpv6](#) (work in progress), February 2002.
- [6] Hagino, J. and D. Thaler, "IPv6 Stateless DNS Discovery", [draft-ietf-ipngwg-dns-discovery](#) (work in progress), July 2001.
- [7] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.

- [8] Bound, J., Carney, M., Perkins, C., Lemon, T., Volz, B. and R. Droms, "The DNS Configuration options for DHCPv6", [draft-ietf-dhc-dhcpv6-opt-dnsconfig](#) (work in progress), Jan 2002.

Droms, et al.

Expires August 30, 2002

[Page 9]

Internet-Draft

Using DHCPv6 for DNS Configuration

Mar 2002

Authors' Addresses

Ralph Droms
Cisco Systems
250 Apollo Drive
Chelmsford, MA 01824
USA

Phone: +1 978 497 4733
EMail: rdroms@cisco.com

Thomas Narten
IBM Corporation
P.O. Box 12195
Research Triangle Park, NC 27709-2195
USA

Phone: +1 919 254 7798
EMail: narten@us.ibm.com

Bernard Aboba
Microsoft
One Microsoft Way
Redmond, WA 98052
USA

EMail: aboba@internaut.com

Full Copyright Statement

Copyright (C) The Internet Society (2002). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

Acknowledgement

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