DHC Working Group
Internet Draft

Carl Smith
Sun Microsystems, Inc.
Ted Lemon
Nominum, Inc.

Updates: RFC 2132

November 2002
Expires May 2003

Considerations for the use of the Host Name option
<draft-ietf-dhc-host-option-considerations-01.txt>

Status of this Memo

Abstract

This document clarifies the use of the DHCP Host Name option. The primary point of this clarification addresses the use of the option by clients to request proxy DNS updates by DHCP servers.

1. Introduction

The initial concept of the Host Name option, as documented in RFC 1533[1] and duplicated in RFC 2132 [2], was simply to allow a DHCP server to supply a client with its name (``This option specifies the name of the client''). The DHCP client was merely a consumer of the option information. Even in this case, confusion has been reported in interactions with various domain name options.

Behavior of client and server when the client supplies the option was, and still is, unspecified. In the intervening years, the

ability to easily update Domain Name Service information [3] has encouraged the use of this option by DHCP clients as a way to request that DHCP servers issue proxy DNS updates on their behalf. Lack of a document describing its exact usage has led, as one would surely expect, to interoperability problems. It is the purpose of this document to outline the expectations that clients and servers should have when using the Host Name option.

2. Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [4]. This document also uses the following terms:

"DHCP client"

DHCP client or "client" is an Internet host using DHCP to obtain configuration parameters such as a network address.

"DHCP server"

A DHCP server or "server" is an Internet host that returns configuration parameters to DHCP clients.

"FQDN"

A fully-qualified name, including the host part and Domain Name system domain.

3. Interactions with Name Services

RFC 2132 [2] indicates that the value supplied in the Host Name option may or may not be fully-qualified, suggesting the use of the Domain Name option to retrieve the domain name. This, plus the possibility of interactions between DNS (RFC 1034 [5] and RFC 1035 [6]) and other naming services motivates us to clarify and expand the description of the expected behavior:

if a DHCP server supplies both Host Name and Domain Name options to a client, the host name SHOULD NOT be fully-qualified

if a DHCP server supplies only a Host Name option, the host name SHOULD be fully qualified; the server MUST append only DNS domain names in forming a fully-qualified name

a client MUST check to see whether a Host Name option contains a fully-qualified name and if so, MUST NOT append the value of the

Domain Name option (if present) in forming its fully-qualified domain name

since a Host Name option's value may be fully-qualified only by supplying the DNS domain name, a client that receives a fully-qualified name in the Host Name option MAY infer the DNS domain name from the suffix of the supplied host name. This inference remains valid even in the presence of client configuration information or policies that prefer other name services in favor of, or in place of, DNS.

In summary,

	Host Name not fully-qualifled	Host Name fully-qualified
Domain Name option absent	no derivable FQDN	infer Domain Name from Host Name suffix
Domain Name option present	derive FQDN by Host and Domain Name concatenation	Domain Name MUST be a suffix of Host Name

4. DNS Updates for DHCP Clients

DNS maintains Resource Records (RRs) for mapping between IP addresses FQDNs. Specifically, A records map FQDNs to IP addresses and PTR records map IP addresses to FQDNs. Several options are available to DHCP clients interested in updating A and PTR records:

issuing direct updates to DNS

using the DHCP client FQDN option [7]

using the DHCP Host Name option

Either of the first two methods has the advantage of offering the client a number of approaches for fine-tuning DNS update requests as well as direct feedback on the success or failure of the intended operations. Both are to be preferred over the latter: use of the Host Name option does not even guarantee that the DHCP server will attempt any DNS updates on a client's behalf. It should be considered deprecated. Nevertheless, support for this method of requesting proxy DNS updates is widespread and it may be viewed as appropriate for situations in which there are no requirements for other finely-tunable methods.

4.1 DHCP Client Considerations and Behavior

A DHCP client that uses the Host Name option to request a DNS update MUST be prepared to independently verify the success or failure of the request before using the name in a manner that would imply its validity. If a DHCP server returns the requested name in the DHCPACK's Host Name option, the client MAY infer that the server has honored its request.

There are a number of reasons that a DHCP server may fail to return a Host Name option; nothing should be inferred from the option's absence in the DHCPACK. The client MAY supply the option on subsequent RENEW operations as a method of retrying the request. However, if the Host Name option is absent in the DHCPACK, the client MUST NOT use the requested name until it has verified the validity of the association between it and the IP address supplied in the yiaddr field. Moreover, if the name returned in the DHCPACK is different from the one requested, the client MUST use the new name.

A DHCP client MAY send either an unqualified or fully-qualified name in the Host Name option. Clients sending unqualified names are implicitly relying on DHCP servers to associate the clients with the appropriate zone before issuing any updates to DNS. A DHCP client in INIT state SHOULD fill in the requested host name in the DHCPDISCOVER packet. It MUST do so in its subsequent DHCPREQUEST packet.

Clients in states other than INIT SHOULD avoid ambiguity in their requests by supplying the same Host Name option value on subsequent DHCPREQUESTs as was supplied on their original (INIT state) DHCPREQUEST.

A client that wishes to change its host name MAY request it by supplying a Host Name option with the new name in a subsequent RENEW request. As with the initial request, a client MUST NOT use the newly-requested name until it has verified that it is now valid.

4.2 DHCP Server Considerations and Behavior

Use of the FQDN option makes it possible to easily separate update operations into pieces corresponding to what are thought of as the traditional ownership boundaries: DHCP servers own the addresses they lease, while the clients own their names. This boundary is not present when the Host Name option is used: the implied proxy update request assumes that the DHCP server has sufficient privilege to change both the A and PTR records. That is, it ``owns'' both.

For this and other reasons, use of the FQDN option is preferred: a DHCP server that receives both a Host Name option and a client FQDN

option MUST prefer the FQDN option. In such a case, the server SHOULD behave as if the Host Name option is not present.

A DHCP server MAY use the value of the Host Name option in a DHCPDISCOVER packet in some limited ways: it may check to see whether the requested name belongs to an address that ls leaseable to the client, saving the need for a DNS update, or it may begin preparation of an update request. The server MUST wait for the DHCPREQUEST before initiating any update operations.

DNS updates may not complete in a timely manner, forcing the DHCP server to reply to a client before the update has finished. Alternatively, an error may be reported in response to the update request. It is not possible to distinguish these cases for the client's benefit, and the the DHCP server simply omits the Host Name option from its DHCPACK. For simplicity of implementation, servers may choose to ``orphan'' any outstanding requests, taking no note of subsequent reports of success or failure. Servers that choose to keep track of the results of update requests SHOULD use successful completion reports to avoid subsequent unnecessary work; those servers SHOULD ignore reports of soft, transitory errors. Hard errors SHOULD be logged by the server so that corrective action, if any, may be taken by an administrator. Servers MAY choose to not cache hard failures, retrying on subsequent DHCPREQUESTs in the hope that the errors logged have led to a remedy.

Issuing DNS updates on behalf of DHCP clients is an inherently stateful operation. A DHCP server MUST commit to stable storage the necessary information regarding any updates it successfully makes on behalf of its clients. This state may be needed

- when a lease expires
- when communicating with a failover partner
- on subsequent lease renewals

and may need to be recovered when the server is restarted.

When a lease expires, a DHCP server MAY use this stored information to expunge the name-to-address association it created on the client's behalf. Because the use of the Host Name option cedes the ownership of the name to the server, a server MAY instead choose to allow the association to continue, saving itself work now and possibly sparing the need for a future update.

A server SHOULD reevaluate the Host Name option each time a client sends a RENEW request via a DHCPREQUEST, or the server MAY choose to

view the update request as an action to be taken once, upon initial lease of an address. Servers that take the former view offer their clients the possibility of changing the name associated with a currently valid lease, but may incur additional processing costs because of it. Servers taking the latter view do not afford clients the opportunity to change names, but more importantly do not allow them to retry failed requests, possibly even with different host names. For this reason, the former behavior is preferred: servers SHOULD reevaluate the Host Name option on each RENEW.

Some servers interpret a Host Name option on the initial DHCPREQUEST, followed by the absence of the option on subsequent RENEW DHCPREQUESTs as a request by the client to delete a name-to-address association. Because clients that expect DNS updates to apply for the duration of a lease may not send a Host Name option when RENEWing, servers SHOULD NOT interpret the absence of the option as a request for deletion of the association.

The manner in which the client might express its desire to have the association destroyed is currently under discussion. Two methods have been suggested: a zero-length Host Name option and an additional (``remove'') bit in the FQDN option. WG discussion at Minneapolis did not lead to concensus.

5. Security Considerations

Use of the Host Name option to petition DHCP servers to do proxy DNS updates is undeniably convenient for the clients but it also opens the door for denial of service attacks and identity impersonation. Administrators MUST carefully evaluate the balance between offering the convenience of proxy DNS updates and the attendant risks.

Clients using the Host Name option to request a DNS update will likely lack a means of authenticating themselves (otherwise, they might have dealt directly, and securely, with DNS). DHCP servers SHOULD use all means at their disposal to verify the requests. Use of DHCP Authentication ([8]) is far from common but other means, such as previous authentication to a network access server via PPP or proprietary controls such as exist in many broadband cable systems, may be available.

A DHCP server must be prepared to arbitrate between multiple clients that all claim the same fully-qualified name. It SHOULD give preference to a client whose identity it can verify. Failing that, it MUST use the method described in [9] to ensure that an association made on behalf of one client is not inadvertently changed by another.

6. References

[1] Alexander, S. and Droms, R., "DHCP Options and BOOTP Vendor Extensions", RFC 1533, October 1993.
[2] Alexander, S. and Droms, R., "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.
[3] Vixie, P., Thomson, S., Rekhter, Y., Bound, J., "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.
[4] Bradner, S., "Key words for use in RFCs to indicate requirement levels", RFC 2119, March 1997.
[5] Mockapetris, P., "Domain names - Concepts and Facilities", RFC 1034, November 1987.
[6] Mockapetris, P., "Domain names - Implementation and Specification", RFC 1035, November 1987.
[7] Stapp, M. and Rekhter, Y., "The DHCP Client FQDN Option", draft-ietf-dhc-fqdn-option-04.txt, June 2002.
[8] Droms, R. and Arbaugh, W., "Authentication for DHCP Messages", RFC 3118, June 2001.
[9] Stapp, M., "Resolution of DNS Name Conflicts Among DHCP Clients", draft-ietf-dhc-ddns-resolution-04.txt, June 2002.

6. Author Information

Carl Smith
Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94043
USA
email: cs@Eng.Sun.COM

Ted Lemon
Nominum, Inc.
950 Charter Street
Redwood City, CA 94043
USA
email: Ted.Lemon@nominum.com

7. Expiration

This document will expire on May 6, 2003.

8. Full Copyright Statement