DHC
Internet-Draft
Expires: March 17, 2005

B. Volz
Cisco Systems, Inc.
September 16, 2004

The DHCPv6 Client FQDN Option
draft-ietf-dhc-dhcpv6-fqdn-00.txt

Status of this Memo

Copyright Notice

Abstract

This document specifies a new DHCP for IPv6, DHCPv6, option which can be used to exchange information about a DHCPv6 client's fully-qualified domain name and about responsibility for updating DNS RRs related to the client's address assignments.

Table of Contents

1. Introduction

DNS ([2], [3]) maintains (among other things) the information about mapping between hosts' Fully Qualified Domain Names (FQDNs) [8] and IP addresses assigned to the hosts. The information is maintained in two types of Resource Records (RRs): AAAA and PTR [11]. The DNS update specification ([4]) describes a mechanism that enables DNS information to be updated over a network.

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [5] provides a mechanism by which a host (a DHCPv6 client) can acquire certain configuration information, along with its stateful IPv6 address(es). This document specifies a new DHCPv6 option, the Client FQDN option, which can be used by DHCPv6 clients and servers to exchange information about the client's fully-qualified domain name and who has the responsibility for updating the DNS with the associated AAAA and PTR RRs.

2. Terminology

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 [1].

Familiarity with the DNS Update protocol [4], DHCPv6, and DHCPv6 terminology as defined in [5] is assumed.

3. Models of Operation

When a DHCPv6 client acquires an address, a site's administrator may desire that the AAAA RR for the client's FQDN and the PTR RR for the acquired address be updated. Therefore, two separate DNS update transactions may occur. Acquiring an address via DHCPv6 involves two entities: a DHCPv6 client and a DHCPv6 server. In principle each of these entities could perform none, one, or both of the DNS update transactions. However, in practice not all permutations make sense. The DHCPv6 Client FQDN option is primarily intended to operate in the following two cases:

1. DHCPv6 client updates the AAAA RR, DHCPv6 server updates the PTR RR
2. DHCPv6 server updates both the AAAA and the PTR RRs

The only difference between these two cases is whether the FQDN to IPv6 address mapping is updated by a DHCPv6 client or by a DHCPv6 server. The IPv6 address to FQDN mapping is updated by a DHCPv6 server in both cases.

The reason these two are important, while others are unlikely, has to do with authority over the respective DNS domain names. A DHCPv6 client may be given authority over mapping its own AAAA RRs, or that authority may be restricted to a server to prevent the client from listing arbitrary addresses or associating its addresses with arbitrary domain names. In all cases, the only reasonable place for the authority over the PTR RRs associated with the address is in the DHCPv6 server that allocates the address.

Note: A third case is supported - the client requests that the server perform no updates. However, this case is presumed to be rare because of the authority issues.

In any case, whether a site permits all, some, or no DHCPv6 servers and clients to perform DNS updates into the zones which it controls is entirely a matter of local administrative policy. This document does not require any specific administrative policy, and does not propose one. The range of possible policies is very broad, from sites where only the DHCPv6 servers have been given credentials that the DNS servers will accept, to sites where each individual DHCPv6 client has been configured with credentials which allow the client to modify its own domain name. Compliant implementations MAY support some or all of these possibilities. Furthermore, this specification applies only to DHCPv6 client and server processes: it does not apply to other processes which initiate DNS updates.

This document describes a new DHCPv6 option which a client can use to convey all or part of its domain name to a DHCPv6 server. Site-specific policy determines whether DHCPv6 servers use the names that clients offer or not, and what DHCPv6 servers may do in cases where clients do not supply domain names.

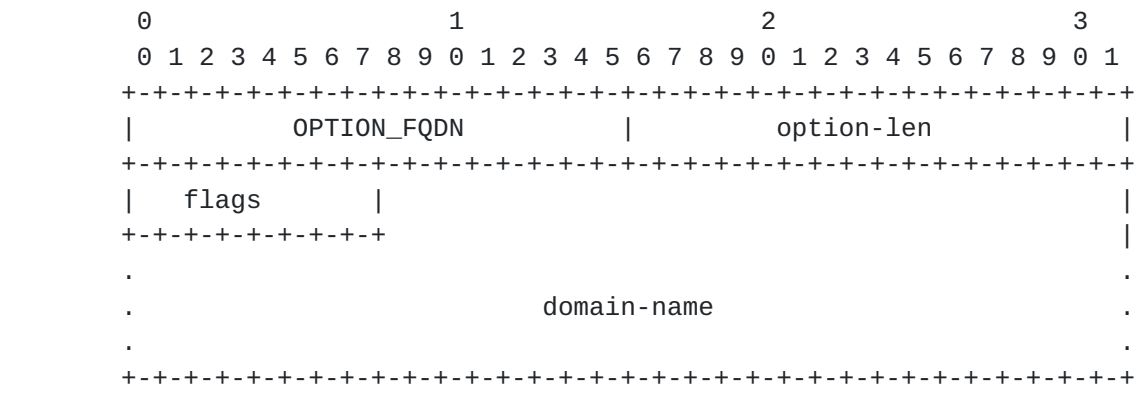
Other work, such as "Resolving Name Conflicts" [6], may define procedures for establishing policy and arbitrating conflicts when collisions occur in the use of FQDNs by DHCPv6 clients.

4. The DHCPv6 Client FQDN Option

To update the IPv6 address to FQDN mapping a DHCPv6 server needs to know the FQDN of the client for the addresses in a binding. To allow the client to convey its FQDN to the server this document defines a new DHCPv6 option, called "Client FQDN". The Client FQDN option also contains Flags which DHCPv6 clients and servers use to negotiate who does which updates.

The code for this option is TBD. Its minimum length is 2.

The Format of the DHCPv6 Client FQDN option is shown below:

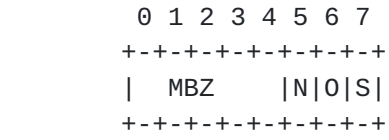


option-code	OPTION_CLIENT_FQDN (TBD)
option-len	1 + length of domain name
flags	flag bits used between client and server to negotiate who performs which updates
domain-name	the partial or fully qualified domain name (with length option-len - 1)

The Client FQDN option MUST only appear in IA_NA-options and IA_TA-options (see [12]) fields and applies to all addresses for that binding.

4.1 The Flags Field

The Format of the Flags field:



When a DHCPv6 client sends the Client FQDN option, it sets the "S" bit to indicate that it will not perform any DNS updates, and that it expects the DHCPv6 server to perform any FQDN-to-IPv6 (the AAAA RR) DNS updates on its behalf. If this bit is clear, the client indicates that it intends to perform the FQDN-to-IPv6 DNS updates.

If a DHCPv6 server intends to take responsibility for the AAAA RR updates, whether or not the client sending the Client FQDN option has set the "S" bit, it sets both the "O" and "S" bits, and sends the

Client FQDN option in its response message. Clients SHOULD clear the "O" bit before sending the Client FQDN option and servers MUST ignore the received state of the "O" bit.

A client MAY set the "N" bit in its request messages to indicate that the server should not perform any DNS updates on its behalf. As mentioned in Section 3, in general the DHCPv6 server will be maintaining DNS PTR records on behalf of clients. However, there may be deployments in which clients are configured to perform all desired DNS updates or may not want any DNS updates. The server MAY be configured to honor this configuration. If the server has been configured to honor a client's "N" indication, it SHOULD set the "N" bit in Client FQDN options which it sends to the client in its response messages. Clients which have set the "N" bit in their requests SHOULD use the state of the "N" bit in server responses to determine whether the server was prepared to honor the client's indication. If a client has set the "N" bit but its server does not, the client SHOULD conclude that the server was not configured to honor the client's suggestion, and that the server may attempt to perform DNS updates on its behalf.

The remaining bits in the Flags field are reserved for future assignment. DHCPv6 clients and servers which send the Client FQDN option MUST set the MBZ bits to 0, and they MUST ignore these bits.

4.2 The Domain Name Field

The Domain Name field of the option carries all or part of the FQDN of a DHCPv6 client. The data in the Domain Name field MUST appear in uncompressed DNS encoding as specified in [3]. In order to determine whether a name has changed between message exchanges, an unambiguous canonical form is necessary. Eventually, the IETF IDN Working Group is expected to produce a standard canonicalization specification, and this specification may be updated to include its standard. Until that time, servers and clients should be sensitive to canonicalization when comparing names in the Domain Name field and the name canonicalization defined in [9] MAY be used.

A client may be configured with a fully-qualified domain name, or with a partial name that is not fully-qualified. If a client knows only part of its name, it MAY send a name that is not fully-qualified, indicating that it knows part of the name but does not necessarily know the zone in which the name is to be embedded. A client which wants to convey part of its FQDN sends a non-terminal sequence of labels in the domain name field of the option. Clients and servers should assume that the name field contains a fully-qualified name unless this partial-name format exists.

Servers MUST always send the complete fully-qualified domain name in Client FQDN options.

5. DHCPv6 Client behavior

The following describes the behavior of a DHCPv6 client that implements the Client FQDN option.

A client MUST only include Client FQDN options in the IA_NA-options and IA_TA-options fields in SOLICIT, REQUEST, RENEW, or REBIND messages.

A client that sends the Client FQDN option MUST also include the option in the Option Request option if it expects the server to include the Client FQDN option in any responses.

A client sends the Client FQDN option with no Flags bits set, the "S" Flags bit set, or the "N" Flags bit set and with the desired partial or fully qualified domain name.

There is no requirement that the client send identical Client FQDN options data in each of its messages to a server. In particular, if a client has sent Client FQDN options to its server, and the configuration of the client changes so that its notion of its domain name changes, it MAY send the new name data in a Client FQDN options when it communicates with the server again. This may cause the DHCPv6 server to update the name associated with the PTR record, and, if the server updated the AAAA record representing the client, to delete that record and attempt an update for the client's current domain name.

Once the client's DHCPv6 configuration is completed (the client receives a REPLY message, and successfully completes a final check on the parameters passed in the message), the client SHOULD originate the DNS updates for the AAAA RR (associated with the client's FQDNs) for any Client FQDN options for which the received "S" and the "O" bits in the option's Flags field are not set and if it is otherwise configured to perform the DNS updates. The update SHOULD be originated following the procedures described in [4]. If the DHCPv6 server from which the client is requesting addresses includes Client FQDN options in its REPLY message, and if the server sets both the "S" and "O" bits in the option's Flags field, the DHCPv6 client MUST NOT initiate an update for the name in the Domain Name field and the addresses in that binding.

A client that delegates the responsibility for updating the FQDN-to-IPv6 address mapping to a server does not receive any indication (either positive or negative) from the server whether the

server was able to perform the update. If the client needs to confirm the DNS update, it SHOULD use a DNS query to check whether the mapping is updated.

If a client releases an address prior to the valid lifetime expiration or is unable to extend the lifetimes for an address and the valid lifetime expires, and the client is responsible for updating its AAAA RRs, the client SHOULD delete the AAAA RR associated with the address before sending a RELEASE message or the lifetime expires. A DHCPv6 client which has not been able to delete an AAAA RR which it added (because it has lost the use of addresses of sufficient scope to communicate with the DNS server or has exhausted retry limits) should attempt to notify its administrator, perhaps by emitting a log message.

6. DHCPv6 Server Behavior

Servers MUST only include Client FQDN options for a binding in ADVERTISE and REPLY messages if the client included a Client FQDN option for that binding and the Client FQDN option is requested by the Option Request Option in the client's message to which the server is responding. Servers MUST only include Client FQDN options in the IA_NA-options and IA_TA-options fields in messages sent by the server.

When a server allocates a new address from a binding, it uses the Client FQDN option, if any, in the IA_NA-options or IA_TA-options field of that binding to determine the fully qualified domain name and who will take responsibility for the DNS updates. It records the results in the Client FQDN option. The DHCPv6 server SHOULD send its notion of the complete FQDN for the client in the Domain Name field. The server MAY simply copy the Domain Name field from the Client FQDN option that the client sent to the server. The DHCPv6 server MAY be configured to complete or modify the domain name which a client sent, or it MAY be configured to substitute a different name.

If a client's SOLICIT, REQUEST, RENEW, or REBIND message doesn't include the Client FQDN option for a binding (e.g., the client doesn't implement the Client FQDN option), the server MAY be configured to update either or both of the AAAA and PTR RRs.

If a client's message includes a Client FQDN option for a binding and the requested domain-name is different from the server's current knowledge of the fully-qualified domain name and the server is configured to allow use of that name, the server SHOULD perform the necessary DNS updates - the server SHOULD remove the old PTR and AAAA RRs it added, if any, and add the new RRs - if it has that responsibility.

When a server receives a RELEASE or DECLINE for an address, detects that the valid lifetime on an address that the server bound to a client has expired, or terminates a binding on an address prior to the binding's expiration time (for instance, by sending a REPLY with a zero valid lifetime for an address), the server SHOULD delete any PTR RRs which it associated with the address via DNS update. In addition, if the server took responsibility for the AAAA RR, the server SHOULD also delete that AAAA RR.

A server MAY initiate and complete the DNS update(s) before the server sends the REPLY message to the client. Alternatively, the server MAY send the REPLY message to the client without waiting for the update to be initiated or completed. The choice between the two alternatives is entirely determined by the configuration of the DHCPv6 server. Servers SHOULD support both configuration options.

If the server initiates a DNS update that is not complete until after the server has replied to the client, the server's interaction with the DNS server may cause the DHCPv6 server to change the domain name that it associates with an address for the client. This may occur, for example, if the server detects and resolves a domain-name conflict. In such cases, the domain name that the server returns to the client may change between two DHCPv6 exchanges.

7. DNS Update Conflicts

This document does not resolve how a DHCPv6 client or server prevent name conflicts. This document addresses only how a DHCPv6 client and server negotiate the fully qualified domain name and who will perform the DNS updates.

Implementers of this work will need to consider how name conflicts will be prevented. It may be that the DNS updater must hold a security token in order to successfully perform DNS updates on a specific name, in which case name conflicts can only occur if multiple clients are given a security token for that name. Or, the fully qualified domains may be based on the specific address bound to a client or the client's DUID, and in these cases conflicts should not occur. However, without this level of security in the DNS system or use of non-conflicting names, other techniques need to be developed. This is an area for future work (see [6]).

8. Security Considerations

Unauthenticated updates to the DNS can lead to tremendous confusion, through malicious attack or through inadvertent misconfiguration. Administrators should be wary of permitting unsecured DNS updates to zones which are exposed to the global Internet. Both DHCPv6 clients

and servers SHOULD use some form of update request origin authentication procedure (e.g., Secure DNS Dynamic Update [10]) when performing DNS updates.

Whether a DHCPv6 client may be responsible for updating an FQDN to IPv6 address mapping or whether this is the responsibility of the DHCPv6 server is a site-local matter. The choice between the two alternatives may be based on the security model that is used with the DNS update protocol (e.g., only a client may have sufficient credentials to perform updates to the FQDN to IP address mapping for its FQDN).

Whether a DHCPv6 server is always responsible for updating the FQDN to IPv6 address mapping (in addition to updating the IPv6 to FQDN mapping), regardless of the wishes of an individual DHCPv6 client, is also a site-local matter. The choice between the two alternatives may be based on the security model that is being used with DNS updates. In cases where a DHCPv6 server is performing DNS updates on behalf of a client, the DHCPv6 server should be sure of the DNS name to use for the client, and of the identity of the client.

Depending on the prescence of or type of authentication used with the Authentication option, a DHCPv6 server may not have much confidence in the identities of its clients. There are many ways for a DHCPv6 server to develop a DNS name to use for a client, but only in certain circumstances will the DHCPv6 server know for certain the identity of the client.

9. Acknowledgements

Many thanks to Mark Stapp and Yakov Rekhter as this document is based on the DHCPv4 Client FQDN option (draft-ietf-dhc-fqdn-option [7]). And, to Ted Lemon, Mark Stapp, Josh Littlefield, Kim Kinnear, and Ralph Droms for discussions on this work.

10. References

10.1 Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[3] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[4] Vixie, P., Thomson, S., Rekhter, Y. and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

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

10.2 Informative References

[6] Stapp, M., "Resolution of DNS Name Conflicts Among DHCP Clients (draft-ietf-dhc-ddns-resolution-*.txt)", October 2003.

[7] Stapp, M., Volz, B. and Y. Rekhter, "The DHCP Client FQDN Option (draft-ietf-dhc-fqdn-option-*.txt)", July 2004.

[8] Marine, A., Reynolds, J. and G. Malkin, "FYI on Questions and Answers - Answers to Commonly asked "New Internet User" Questions", RFC 1594, March 1994.

[9] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

[10] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.

[11] Thomson, S., Huitema, C., Ksinant, V. and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.

[12] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

Author's Address

Bernard Volz
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA

Phone: +1 978 936 0382
EMail: volz@cisco.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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