          The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client
                   Fully Qualified Domain Name (FQDN) Option

Status of This Memo

Copyright Notice

Abstract

   This document specifies a new Dynamic Host Configuration Protocol for
   IPv6 (DHCPv6) option that can be used to exchange information about a
   DHCPv6 client's Fully Qualified Domain Name (FQDN) and about
   responsibility for updating DNS resource records (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) [10] and
   IPv6 addresses assigned to the hosts. The information is maintained
   in two types of Resource Records (RRs): AAAA and PTR [12]. 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 about 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] and with DHCPv6 and its
   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 in which 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 that 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 that 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
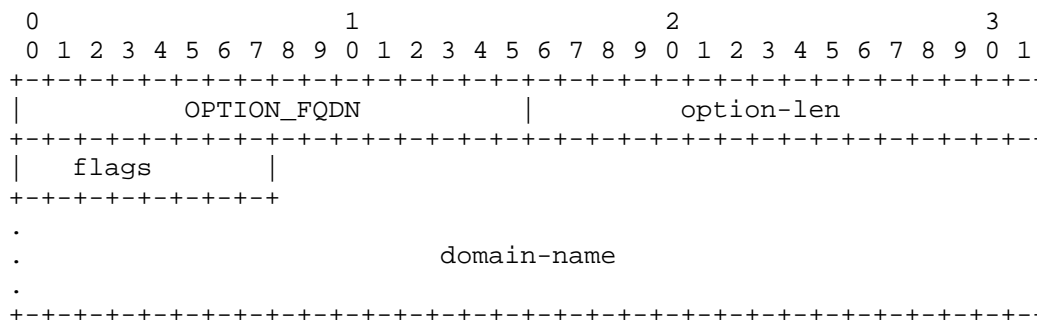processes that initiate DNS updates.

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

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 for the client's IA_NA
bindings. 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 that DHCPv6 clients and
servers use to negotiate who does which updates.

The code for this option is 39. Its minimum length is 1 octet.

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          OPTION_FQDN          |         option-len            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    flags      |                                               |
+-+-+-+-+-+-+-+-+                                               |
.                                                               .
.                          domain-name                          .
.                                                               .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

        option-code   OPTION_CLIENT_FQDN (39)

        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 a message's options field
   and applies to all addresses for all IA_NA bindings in the
   transaction.

4.1. The Flags Field

   The format of the Flags field is:

```
     0 1 2 3 4 5 6 7
    +-+-+-+-+-+-+-+-+
    |  MBZ    |N|O|S|
    +-+-+-+-+-+-+-+-+
```
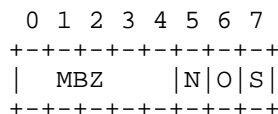

   The "S" bit indicates whether the server SHOULD or SHOULD NOT perform
   the AAAA RR (FQDN-to-address) DNS updates. A client sets the bit to
   0 to indicate that the server SHOULD NOT perform the updates and 1 to
   indicate that the server SHOULD perform the updates. The state of
   the bit in the reply from the server indicates the action to be taken
   by the server; if it is 1, the server has taken responsibility for
   AAAA RR updates for the FQDN.

The "O" bit indicates whether the server has overridden the client's
preference for the "S" bit. A client MUST set this bit to 0. A
server MUST set this bit to 1 if the "S" bit in its reply to the
client does not match the "S" bit received from the client.

The "N" bit indicates whether the server SHOULD NOT perform any DNS
updates. A client sets this bit to 0 to request that the server
SHOULD perform updates (the PTR RR and possibly the AAAA RR based on
the "S" bit) or to 1 to request that the server SHOULD NOT perform
any DNS updates. A server sets the "N" bit to indicate whether the
server SHALL (0) or SHALL NOT (1) perform DNS updates. If the "N"
bit is 1, the "S" bit MUST be 0.

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

4.2. The Domain Name Field

The Domain Name part of the option carries all or part of the FQDN of
a DHCPv6 client. The data in the Domain Name field MUST be encoded
as described in Section 8 of [5]. In order to determine whether the
FQDN has changed between message exchanges, the client and server
MUST NOT alter the Domain Name field contents unless the FQDN has
actually changed.

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.

To send a fully qualified domain name, the Domain Name field is set
to the DNS-encoded domain name including the terminating zero-length
label. To send a partial name, the Domain Name field is set to the
DNS-encoded domain name without the terminating zero-length label.

A client MAY also leave the Domain Name field empty if it desires the
server to provide a name.

Servers SHOULD 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 the Client FQDN option 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.

5.1. Client Desires to Update AAAA RRs

   If a client that owns/maintains its own FQDN wants to be responsible
   for updating the FQDN-to-IPv6-address mapping for the FQDN and
   address(es) used by the client, the client MUST include the Client
   FQDN option in the SOLICIT with Rapid Commit, REQUEST, RENEW, and
   REBIND message originated by the client. A client MAY choose to
   include the Client FQDN option in its SOLICIT messages. The "S",
   "O", and "N" bits in the Flags field in the option MUST be 0.

   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 MAY originate an
   update for the AAAA RRs (associated with the client's FQDN) unless
   the server has set the "S" bit to 1. If the "S" is 1, the DHCPv6
   client SHOULD NOT initiate an update for the name in the server's
   returned Client FQDN option Domain Name field. However, a DHCPv6
   client that is explicitly configured with a FQDN MAY ignore the state
   of the "S" bit if the server's returned name matches the client's
   configured name.

5.2. Client Desires Server to Do DNS Updates

   A client can choose to delegate the responsibility for updating the
   FQDN-to-IPv6-address mapping for the FQDN and address(es) used by the
   client to the server. In order to inform the server of this choice,
   the client SHOULD include the Client FQDN option in its SOLICIT with
   Rapid Commit, REQUEST, RENEW, and REBIND messages and MAY include the
   Client FQDN option in its SOLICIT. The "S" bit in the Flags field in
   the option MUST be 1, and the "O" and "N" bits MUST be 0.

5.3. Client Desires No Server DNS Updates

   A client can choose to request that the server perform no DNS updates
   on its behalf. In order to inform the server of this choice, the
   client SHOULD include the Client FQDN option in its SOLICIT with

Rapid Commit, REQUEST, RENEW, and REBIND messages and MAY include the
Client FQDN option in its SOLICIT. The "N" bit in the Flags field in
the option MUST be 1, and the "S" and "O" bits MUST be 0.

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 MAY originate its
DNS updates provided the server's "N" bit is 1. If the server's "N"
bit is 0, the server MAY perform the PTR RR updates; it MAY also
perform the AAAA RR updates if the "S" bit is 1.

5.4. Domain Name and DNS Update Issues

As there is a possibility that the DHCPv6 server is configured to
complete or replace a domain name that the client sends, the client
MAY find it useful to send the Client FQDN option in its SOLICIT
messages. If the DHCPv6 server returns different Domain Name data in
its ADVERTISE message, the client could use that data in performing
its own eventual AAAA RR update, or in forming the Client FQDN option
that it sends in its subsequent messages. There is no requirement
that the client send identical Client FQDN option data in its
SOLICIT, REQUEST, RENEW, or REBIND messages. In particular, if a
client has sent the Client FQDN option 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 option
when it communicates with the server again. This MAY cause the
DHCPv6 server to update the name associated with the PTR records 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.

A client that delegates the responsibility for updating the FQDN-to-
IPv6-address mapping to a server will not receive any indication
(either positive or negative) from the server as to whether the
server was able to perform the update. The client MAY use a DNS
query to check whether the mapping is up to date. However, depending
on the load on the DHCPv6 and DNS servers and the DNS propagation
delays, the client can only infer success. If the information is not
found to be up to date in DNS, the authoritative servers might not
have completed the updates or zone transfers, or caching resolvers
may yet have updated their caches.

If a client releases an address prior to the expiration of the valid
lifetime and the client is responsible for updating its AAAA RR, the
client SHOULD delete the AAAA RR associated with the address before
sending a RELEASE message. Similarly, if a client is responsible for
updating its AAAA RRs, but is unable to renew the lifetimes for an
address, the client SHOULD attempt to delete the AAAA RR before the

lifetime on the address is no longer valid. A DHCPv6 client that has
not been able to delete an AAAA RR that it added SHOULD attempt to
notify its administrator, perhaps by emitting a log message.

A client SHOULD NOT perform DNS updates to AAAA RRs for its non-
Global Unicast addresses [7] or temporary addresses [6].

6. DHCPv6 Server Behavior

The following describes the behavior of a DHCPv6 server that
implements the Client FQDN option when the client's message includes
the Client FQDN option.

Servers MUST only include a Client FQDN option in ADVERTISE and REPLY
messages if the client included a Client FQDN option and the Client
FQDN option is requested by the Option Request option in the client's
message to which the server is responding.

The server examines its configuration and the Flag bits in the
client's Client FQDN option to determine how to respond:

o The server sets to 0 the "S", "O", and "N" bits in its copy of the
   option it will return to the client.

o If the client's "N" bit is 1 and the server's configuration allows
   it to honor the client's request for no server-initiated DNS
   updates, the server sets the "N" bit to 1.

o Otherwise, if the client's "S" bit is 1 and the server's
   configuration allows it to honor the client's request for the
   server to initiate AAAA RR DNS updates, the server sets the "S" to
   1. If the server's "S" bit does not match the client's "S" bit,
   the server sets the "O" bit to 1.

The server MAY be configured to use the name supplied in the client's
Client FQDN option, or it MAY be configured to modify the supplied
name or to substitute a different name. The 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.

6.1. When to Perform DNS Updates

The server SHOULD NOT perform any DNS updates if the "N" bit is 1 in
the Flags field of the Client FQDN option in the REPLY messages (to
be) sent to the client. However, the server SHOULD delete any RRs
that it previously added via DNS updates for the client.

The server MAY perform the PTR RR DNS update (unless the "N" bit is 1).

The server MAY perform the AAAA RR DNS update if the "S" bit is 1 in the Flags field of the Client FQDN option in the REPLY message (to be) sent to the client.

The server MAY perform these updates even if the client's message did not carry the Client FQDN option. The server MUST NOT initiate DNS updates when responding with an ADVERTISE message to the client.

The server MAY complete its DNS updates (PTR RR or PTR and AAAA RR) before or after sending the REPLY message to the client.

If the server's AAAA RR DNS update does not complete until after the server has replied to the DHCPv6 client, the server's interaction with the DNS server MAY cause the DHCPv6 server to change the domain name that it associates with the client. This can occur, for example, if the server detects and resolves a domain-name conflict [8]. In such cases, the domain name that the server returns to the DHCPv6 client would change between two DHCPv6 exchanges.

If the server previously performed DNS updates for the client and the client's information has not changed, the server MAY skip performing additional DNS updates.

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 RR that it associated with the address via DNS update. In addition, if the server took responsibility for AAAA RRs, the server SHOULD also delete the AAAA RR.

7. DNS RR TTLs

RRs associated with DHCP clients may be more volatile than statically configured RRs. DHCP clients and servers that perform dynamic updates should attempt to specify resource record TTLs that reflect this volatility, in order to minimize the possibility that answers to DNS queries will return records that refer to DHCP IP address assignments that have expired or been released.

The coupling among primary, secondary, and caching DNS servers is 'loose'; that is a fundamental part of the design of the DNS. This looseness makes it impossible to prevent all possible situations in which a resolver may return a record reflecting a DHCP-assigned IP

address that has expired or been released. In deployment, this
rarely, if ever, represents a significant problem. Most DHCP-managed
clients are infrequently looked up by name in the DNS, and the
deployment of IXFR [13] and NOTIFY [14] can reduce the latency
between updates and their visibility at secondary servers.

We suggest these basic guidelines for implementers. In general, the
TTLs for RRs added as a result of DHCP IP address assignment activity
SHOULD be less than the initial lifetime. The RR TTL on a DNS record
added SHOULD NOT exceed 1/3 of the lifetime, but SHOULD NOT be less
than 10 minutes. We recognize that individual administrators will
have varying requirements: DHCP servers and clients SHOULD allow
administrators to configure TTLs and upper and lower bounds on the
TTL values, either as an absolute time interval or as a percentage of
the lease lifetime.

While clients and servers MAY update the TTL of the records as the
lifetime is about to expire, there is no requirement that they do so
as this puts additional load on the DNS system with likely little
benefit.

8. 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. If a DNS updater needs a security token in order
to successfully perform DNS updates on a specific name, name
conflicts can only occur if multiple updaters are given a security
token for that name. Or, if the fully qualified domains are based on
the specific address bound to a client, conflicts will not occur.
Or, a name conflict resolution technique as described in "Resolving
Name Conflicts" [8]) SHOULD be used.

9. IANA Considerations

The IANA has assigned DHCPv6 option code 39 for the Client FQDN
option.

10. Security Considerations

   Unauthenticated updates to the DNS can lead to tremendous confusion,
   through malicious attack or through inadvertent misconfiguration.
   Administrators need to be wary of permitting unsecured DNS updates to
   zones that 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 [11]) when
   performing DNS updates.

   Whether a DHCPv6 client is 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 is likely 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-IPv6-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 is
   likely 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 presence 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.

   It is critical to implement proper conflict resolution, and the
   security considerations of conflict resolution apply [8].

11. Acknowledgements

   Many thanks to Mark Stapp and Yakov Rekhter, as this document is
   based on the DHCPv4 Client FQDN option [9], and to Ralph Droms, Ted
   Lemon, Josh Littlefield, Kim Kinnear, Pekka Savola, and Mark Stapp
   for their review and comments.

12. References

12.1. 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.

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

   [7]   Hinden, R. and S. Deering, "IP Version 6 Addressing
         Architecture", RFC 4291, February 2006.

   [8]   Stapp, M. and B. Volz, "Resolution of Fully Qualified Domain
         Name (FQDN) Conflicts among Dynamic Host Configuration Protocol
         (DHCP) Clients", RFC 4703, October 2006.

12.2. Informative References

   [9]   Stapp, M., Volz, B., and Y. Rekhter, "The Dynamic Host
         Configuration Protocol (DHCP) Client Fully Qualified Domain
         Name (FQDN) Option", RFC 4702, October 2006.

   [10] Marine, A., Reynolds, J., and G. Malkin, "FYI on Questions and
         Answers - Answers to Commonly asked "New Internet User"
         Questions", FYI 4, RFC 1594, March 1994.

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

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

   [13] Ohta, M., "Incremental Zone Transfer in DNS", RFC 1995,
         August 1996.

   [14] Vixie, P., "A Mechanism for Prompt Notification of Zone Changes
         (DNS NOTIFY)", RFC 1996, August 1996.

Author's Address

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

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