DHC Working Group M. Stapp
Internet-Draft Cisco Systems, Inc.
Expires: May 2, 2003 Y. Rekhter
Juniper Networks
November 1, 2002

The DHCP Client FQDN Option
<draft-ietf-dhc-fqdn-option-05.txt>

Status of this Memo

Copyright Notice

Abstract

DHCP provides a powerful mechanism for IP host configuration. However, the configuration capability provided by DHCP does not include updating DNS, and specifically updating the name to address and address to name mappings maintained in the DNS.

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

Table of Contents

1. 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 RFC 2119[1].

2. Introduction

DNS (RFC1034[2], RFC1035[3]) maintains (among other things) the information about mapping between hosts' Fully Qualified Domain Names (FQDNs)[4] and IP addresses assigned to the hosts. The information is maintained in two types of Resource Records (RRs): A and PTR. The A RR contains mapping from a FQDN to an IP address; the PTR RR contains mapping from an IP address to a FQDN. The DNS update specification (RFC2136[5]) describes a mechanism that enables DNS information to be updated over a network.

DHCP[6] provides a mechanism by which a host (a DHCP client) can acquire certain configuration information, along with its IP address(es). However, DHCP does not provide any mechanisms to update the DNS RRs that contain the information about mapping between the host's FQDN and its IP address(es) (A and PTR RRs). Thus DNS information for a DHCP client may not exist or may be incorrect - a host (the client) could acquire its address by using DHCP, but the A RR for the host's FQDN wouldn't reflect the address that the host acquired, and the PTR RR for the acquired address wouldn't reflect the host's FQDN.

The DNS Update protocol can be used to maintain consistency between the information stored in the A and PTR RRs and the actual address assignment done via DHCP. When a host with a particular FQDN acquires its IP address via DHCP, the A RR associated with the host's FQDN would be updated (by using the DNS Update protocol) to reflect the new address. Likewise, when an IP address is assigned to a host with a particular FQDN, the PTR RR associated with this address would be updated (using the DNS Update protocol) to reflect the new FQDN.

Although this document refers to the A and PTR DNS record types and to DHCP assignment of IPv4 addresses, the same procedures and requirements apply for updates to the analogous RR types that are used when clients are assigned IPv6 addresses via DHCPv6.

3. Models of Operation

When a DHCP client acquires a new address, a site's administrator may desire that one or both of the A 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

DHCP involves two entities: a DHCP client and a DHCP server. In principle each of these entities could perform none, one, or both of the transactions. However, in practice not all permutations make sense. The DHCP client FQDN option is intended to operate in the following two cases:

1. DHCP client updates the A RR, DHCP server updates the PTR RR
2. DHCP server updates both the A and the PTR RRs

The only difference between these two cases is whether the FQDN to IP address mapping is updated by a DHCP client or by a DHCP server. The IP address to FQDN mapping is updated by a DHCP 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 DHCP client may be given authority over mapping its own A RRs, or that authority may be restricted to a server to prevent the client from listing arbitrary addresses or associating its address 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 DHCP server that allocates the address.

In any case, whether a site permits all, some, or no DHCP 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 DHCP servers have been given credentials that the DNS servers will accept, to sites where each individual DHCP 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 DHCP client and server processes: it does not apply to other processes which initiate DNS updates.

This document describes a new DHCP option which a client can use to convey all or part of its domain name to a DHCP server. Site-specific policy determines whether DHCP servers use the names that clients offer or not, and what DHCP servers may do in cases where clients do not supply domain names. Another document, "Resolving Name Conflicts"[7], defines a protocol for establishing policy and arbitrating conflicts when collisions occur in the use of FQDNs by DHCP clients.

4. The Client FQDN Option

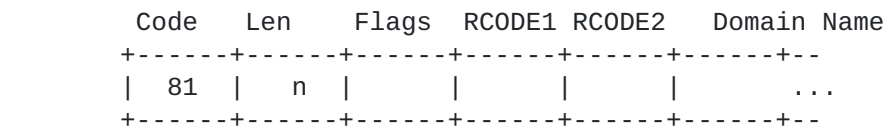
To update the IP address to FQDN mapping a DHCP server needs to know the FQDN of the client to which the server leases the address. To

allow the client to convey its FQDN to the server this document defines a new DHCP option, called "Client FQDN". The FQDN Option also contains Flags and RCode fields which DHCP servers can use to convey information about DNS updates to clients.

Clients MAY send the FQDN option, setting appropriate Flags values, in both their DISCOVER and REQUEST messages. If a client sends the FQDN option in its DISCOVER message, it MUST send the option in subsequent REQUEST messages.

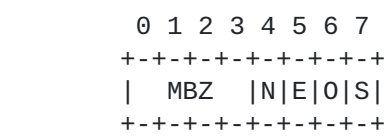
The code for this option is 81. Its minimum length is 4.

The Format of the FQDN Option:



4.1 The Flags Field

The Format of the Flags Field:



When a DHCP client sends the FQDN option in its DHCPDISCOVER and/or DHCPREQUEST messages, it sets the least-significant bit (labelled "S") to indicate that it will not perform any DNS updates, and that it expects the DHCP server to perform any FQDN-to-IP (the A RR) DNS update on its behalf. If this bit is clear, the client indicates that it intends to maintain its own FQDN-to-IP mapping update.

If a DHCP server intends to take responsibility for the A RR update whether or not the client sending the FQDN option has set the "S" bit, it sets both the "O" bit and the "S" bit, and sends the FQDN option in its DHCPOFFER and/or DHCPACK messages.

The data in the Domain Name field SHOULD appear in DNS-style binary encoding (without compression, of course), as described in RFC1035[3]. A client which sends the FQDN option SHOULD use this encoding. The client MUST set the "E" bit when the data in the Domain Name field is in DNS binary encoding. If a server receives an FQDN option from a client, and intends to include an FQDN option in its reply, it MUST use the same encoding that the client used, and

MUST set the "E" bit accordingly.

Server implementors should note that earlier draft versions of this specification permitted an ASCII encoding of the domain name. Clients which implemented this encoding were deployed before this specification was completed. Server implementors which need to support these clients should note the section on the deprecated ASCII encoding (Section 4.3.1).

A client MAY set the "N" flag in its request messages to indicate that the server should not perform any DNS updates on its behalf. As we mentioned in Section 3, we believe that in general the DHCP 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. 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 fqdn options which it sends to the client in its OFFER or ACK 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. DHCP clients and servers which send the FQDN option MUST set the MBZ bits to 0, and they MUST ignore values in the part of the field labelled "MBZ".

4.2 The RCODE Fields

The RCODE1 and RCODE2 fields are used by a DHCP server to indicate to a DHCP client the Response Code from any A or PTR RR DNS updates it has performed. The server may also use these fields to indicate whether it has attempted such an update before sending the DHCPACK message. Each of these fields is one byte long.

Implementors should note that EDNS0 describes a mechanism for extending the length of a DNS RCODE to 12 bits. EDNS0 is specified in RFC2671[8]. Only the least-significant 8 bits of the RCODE from a DNS update will be carried in the Client FQDN DHCP Option. This provides enough number space to accomodate the RCODEs defined in the DNS update specification.

4.3 The Domain Name Field

The Domain Name part of the option carries all or part of the FQDN of a DHCP client. The data in the Domain Name field SHOULD appear in

uncompressed DNS encoding as specified in RFC1035[3]. If the DHCP client uses DNS encoding, it MUST set the third bit in the Flags field (the "E" bit). 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 RFC2535[11] 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 part of the option. Clients and servers should assume that the the name field contains a fully-qualified name unless this partial-name format exists.

4.3.1 Deprecated ASCII Encoding

The DNS encoding specified above MUST be supported by DHCP servers. However, a substantial population of clients implemented an earlier version of this specification, which permitted an ASCII encoding of the Domain Name field. Server implementations should be aware that clients which send the FQDN option with the "E" bit clear are using an ASCII version of the Domain Name field. Servers MAY be prepared to return an ASCII encoded version of the Domain Name field to such clients. The use of ASCII encoding in this option should be considered deprecated.

A DHCP client which used ASCII encoding was permitted to suggest a single label if it was not configured with a fully-qualified name. Such clients send a single label as a series of ASCII characters in the Domain Name field, excluding the "." (dot) character. Such clients SHOULD follow the character-set recommendations of RFC1034[2] and RFC1035[3].

Server implementors should also be aware that some client software may attempt to use UTF-8[10] character encoding. This information is included for informational purposes only: this specification does not require any support for UTF-8.

5. DHCP Client behavior

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

Other DHCP options may carry data that is related to the Domain-Name part of the FQDN option. The Host-Name option, for example, contains an ASCII string representation of the client's host-name. In general, a client should not need to send redundant data, and therefore clients which send the FQDN option in their messages MUST NOT also send the Host-Name option. Clients which receive both the Host-Name option and the FQDN option from a server SHOULD prefer FQDN option data. Servers will be asked in Section 6 to ignore the Host-Name option in client messages which include the FQDN option.

If a client that owns/maintains its own FQDN wants to be responsible for updating the FQDN to IP address mapping for the FQDN and address(es) used by the client, then the client MUST include the Client FQDN option in the DHCPREQUEST message originated by the client. A DHCP client MAY choose to include the Client FQDN option in its DISCOVER messages as well as its REQUEST messages. The least-significant ("S") bit in the Flags field in the option MUST be set to 0. Once the client's DHCP configuration is completed (the client receives a DHCPACK message, and successfully completes a final check on the parameters passed in the message), the client MAY originate an update for the A RR (associated with the client's FQDN). The update SHOULD be originated following the procedures described in RFC2136[5] and "Resolving Name Conflicts"[7]. If the DHCP server from which the client is requesting a lease includes the FQDN option in its ACK message, and if the server sets both the "S" and the "O" bits (the two least-significant bits) in the option's flags field, the DHCP client MUST NOT initiate an update for the name in the Domain Name field.

A client can choose to delegate the responsibility for updating the FQDN to IP 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 DHCPREQUEST message. The least-significant (or "S") bit in the Flags field in the option MUST be set to 1. A client which delegates this responsibility MUST NOT attempt to perform a DNS update for the name in the Domain Name field of the FQDN option. The client MAY supply an FQDN in the Client FQDN option, or it MAY supply a single label (the most-specific label), or it MAY leave that field empty as a signal to the server to generate an FQDN for the client in any manner the server chooses.

Since there is a possibility that the DHCP server may be configured to complete or replace a domain name that the client was configured to send, the client might find it useful to send the FQDN option in its DISCOVER messages. If the DHCP server returns different Domain Name data in its OFFER message, the client could use that data in performing its own eventual A RR update, or in forming the FQDN option that it sends in its REQUEST message. There is no requirement

that the client send identical FQDN option data in its DISCOVER and REQUEST messages. In particular, if a client has sent the 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 an FQDN option when it communicates with the server again. This may allow the DHCP server to update the name associated with the PTR record, and, if the server updated the A 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 IP address mapping to a server might not receive any indication (either positive or negative) from the server whether the server was able to perform the update. In this case the client MAY use a DNS query to check whether the mapping is updated.

A client MUST set the RCODE1 and RCODE2 fields in the Client FQDN option to 0 when sending the option.

If a client releases its lease prior to the lease expiration time and the client is responsible for updating its A RR, the client SHOULD delete the A RR (following the procedures described in "Resolving Name Conflicts"[7]) associated with the leased address before sending a DHCP RELEASE message. Similarly, if a client was responsible for updating its A RR, but is unable to renew its lease, the client SHOULD attempt to delete the A RR before its lease expires. A DHCP client which has not been able to delete an A RR which it added (because it has lost the use of its DHCP IP address) should attempt to notify its administrator, perhaps by emitting a log message.

6. DHCP Server Behavior

When a server receives a DHCPREQUEST message from a client, if the message contains the Client FQDN option, and the server replies to the message with a DHCPACK message, the server may be configured to originate an update for the PTR RR (associated with the address leased to the client). Any such update SHOULD be originated following the procedures described in "Resolving Name Conflicts"[7]. The server MAY complete the update before the server sends the DHCPACK message to the client. In this case the RCODE from the update MUST be carried to the client in the RCODE1 field of the Client FQDN option in the DHCPACK message. Alternatively, the server MAY send the DHCPACK message to the client without waiting for the update to be completed. In this case the RCODE1 field of the Client FQDN option in the DHCPACK message MUST be set to 255. The choice between the two alternatives is entirely determined by the configuration of the DHCP server. Servers SHOULD support both configuration options.

When a server receives a DHCPREQUEST message containing the Client FQDN option, the server MUST ignore the values carried in the RCODE1 and RCODE2 fields of the option.

In addition, if the Client FQDN option carried in the DHCPREQUEST message has the "S" bit in its Flags field set, then the server MAY originate an update for the A RR (associated with the FQDN carried in the option) if it is configured to do so by the site's administrator, and if it has the necessary credentials. The server MAY be configured to use the name supplied in the client's FQDN option, or it MAY be configured to modify the supplied name, or substitute a different name.

Any such update SHOULD be originated following the procedures described in "Resolving Name Conflicts"[7]. The server MAY originate the update before the server sends the DHCPACK message to the client. In this case the RCODE from the update RFC2136[5] MUST be carried to the client in the RCODE2 field of the Client FQDN option in the DHCPACK message. Alternatively the server MAY send the DHCPACK message to the client without waiting for the update to be completed. In this case the RCODE2 field of the Client FQDN option in the DHCPACK message MUST be set to 255. The choice between the two alternatives is entirely a matter of the DHCP server's configuration. In either case, if the server intends to perform the DNS update and the client's REQUEST message included the FQDN option, the server SHOULD include the FQDN option in its ACK message. If the server includes the FQDN option, it MUST set the "S" bit in the option's Flags field and MUST clear the "O" bit.

Even if the Client FQDN option carried in the DHCPREQUEST message has the "S" bit in its Flags field clear (indicating that the client wants to update the A RR), the server MAY be configured by the local administrator to update the A RR on the client's behalf. A server which is configured to override the client's preference SHOULD include an FQDN option in its ACK message, and MUST set both the "O" and "S" bits in the FQDN option's Flags field. The update SHOULD be originated following the procedures described in "Resolving Name Conflicts"[7]. The server MAY originate the update before the server sends the DHCPACK message to the client. In this case the RCODE from the update RFC2136[5] MUST be carried to the client in the RCODE2 field of the Client FQDN option in the DHCPACK message. Alternatively, the server MAY send the DHCPACK message to the client without waiting for the update to be completed. In this case the RCODE2 field of the Client FQDN option in the DHCPACK message MUST be set to 255. Whether the DNS update occurs before or after the DHCPACK is sent is entirely up to the DHCP server's configuration.

When a DHCP server sends the Client FQDN option to a client in the DHCPACK message, the DHCP 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 in the DHCPREQUEST message. The DHCP 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 the server initiates a DNS update that is not complete until after the server has replied to the DHCP client, the server's interaction with the DNS server may cause the DHCP server to change the domain name that it associates with 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 dhcp client may change between two dhcp exchanges.

The server MUST use the same encoding format (ASCII or DNS binary encoding) that the client used in the FQDN option in its DHCPREQUEST, and MUST set the "E" bit in the option's Flags field accordingly.

If a client's DHCPREQUEST message doesn't carry the Client FQDN option (e.g., the client doesn't implement the Client FQDN option), the server MAY be configured to update either or both of the A and PTR RRs. The updates SHOULD be originated following the procedures described in "Resolving Name Conflicts"[7].

If a server detects that a lease on an address that the server leases to a client has expired, the server SHOULD delete any PTR RR which it added via DNS update. In addition, if the server added an A RR on the client's behalf, the server SHOULD also delete the A RR. The deletion SHOULD follow the procedures described in "Resolving Name Conflicts"[7].

If a server terminates a lease on an address prior to the lease's expiration time, for instance by sending a DHCPNAK to a client, the server SHOULD delete any PTR RR which it associated with the address via DNS Update. In addition, if the server took responsibility for an A RR, the server SHOULD also delete that A RR. The deletion SHOULD follow the procedures described in "Resolving Name Conflicts"[7].

7. 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 DHCP clients and servers SHOULD use some form of update request origin authentication procedure (e.g., Secure DNS Dynamic Update[12]) when

performing DNS updates.

Whether a DHCP client may be responsible for updating an FQDN to IP address mapping or whether this is the responsibility of the DHCP 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 DHCP server is always responsible for updating the FQDN to IP address mapping (in addition to updating the IP to FQDN mapping), regardless of the wishes of an individual DHCP 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 DHCP server is performing DNS updates on behalf of a client, the DHCP server should be sure of the DNS name to use for the client, and of the identity of the client.

Currently, it is difficult for DHCP servers to develop much confidence in the identities of its clients, given the absence of entity authentication from the DHCP protocol itself. There are many ways for a DHCP server to develop a DNS name to use for a client, but only in certain relatively unusual circumstances will the DHCP server know for certain the identity of the client. If DHCP Authentication[13] becomes widely deployed this may become more customary.

One example of a situation which offers some extra assurances is one where the DHCP client is connected to a network through an MCNS cable modem, and the CMTS (head-end) ensures that MAC address spoofing simply does not occur. Another example of a configuration that might be trusted is one where clients obtain network access via a network access server using PPP. The NAS itself might be obtaining IP addresses via DHCP, encoding a client identification into the DHCP client-id option. In this case, the network access server as well as the DHCP server might be operating within a trusted environment, in which case the DHCP server could be configured to trust that the user authentication and authorization procedure of the remote access server was sufficient, and would therefore trust the client identification encoded within the DHCP client-id.

8. Acknowledgements

Many thanks to Mark Beyer, Jim Bound, Ralph Droms, Robert Elz, Peter Ford, Edie Gunter, Andreas Gustafsson, R. Barr Hibbs, Kim Kinnear, Stuart Kwan, Ted Lemon, Ed Lewis, Michael Lewis, Josh Littlefield, Michael Patton, and Glenn Stump for their review and comments.

References

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

[2] Mockapetris, P., "Domain names - Concepts and Facilities", RFC 1034, Nov 1987.

[3] Mockapetris, P., "Domain names - Implementation and Specification", RFC 1035, Nov 1987.

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

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

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

[7] Stapp, M., "Resolution of DNS Name Conflicts Among DHCP Clients (draft-ietf-dhc-ddns-resolution-*.txt)", July 2000.

[8] Vixie, P., "Extension Mechanisms for DNS (EDNS0)", RFC 2671, August 1999.

[9] Vixie, P., Gudmundsson, O., Eastlake, D. and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[10] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

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

[12] Wellington, B., "Secure DNS Dynamic Update", RFC 3007, November 2000.

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

Authors' Addresses

Mark Stapp
Cisco Systems, Inc.
250 Apollo Dr.
Chelmsford, MA 01824
USA

Phone: 978.244.8498
EMail: mjs@cisco.com

Yakov Rekhter
Juniper Networks
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA

Phone: 408.745.2000
EMail: yakov@juniper.net

Full Copyright Statement

Acknowledgement

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