DHC
Internet-Draft
Expires: September 23, 2006

M. Stapp
B. Volz
Cisco Systems, Inc.
Y. Rekhter
Juniper Networks
March 22, 2006

The DHCP Client FQDN Option
<draft-ietf-dhc-fqdn-option-13.txt>

Status of this Memo

Copyright Notice

Abstract

This document describes a Dynamic Host Configuration Protocol for IPv4, DHCPv4, option which can be used to exchange information about a DHCPv4 client's fully-qualified domain name and about responsibility for updating the DNS RR related to the client's address assignment.

Table of Contents

1. Introduction

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

The Dynamic Host Configuration Protocol for IPv4 (DHCPv4 or just DHCP in this document) [5] provides a mechanism by which a host (a DHCP client) can acquire certain configuration information, along with its address. This document specifies a DHCP option, the Client FQDN option, which can be used by DHCP clients and servers to exchange information about the client's fully-qualified domain name for an address and who has the responsibility for updating the DNS with the associated A and PTR RRs.

1.1. 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 [1].

1.2. 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 primarily 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.

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.

It is considered local policy to permit DHCP clients and servers to perform DNS updates to zones. This document does not require any specific administrative policy, and does not propose one. 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 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.

2. The Client FQDN Option

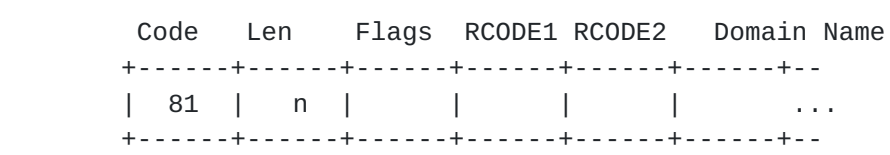
To update the IP address to FQDN mapping a DHCP server needs to know the FQDN of the client to which the server leases the address. To allow the client to convey its FQDN to the server this document defines a new DHCP option, called "Client FQDN". The Client FQDN option also contains Flags, which DHCP servers can use to convey information about DNS updates to clients, and two deprecated RCODEs.

Clients MAY send the Client FQDN option, setting appropriate Flags values, in both their DHCPDISCOVER and DHCPREQUEST messages. If a client sends the Client FQDN option in its DHCPDISCOVER message, it MUST send the option in subsequent DHCPREQUEST messages though the contents of the option MAY change.

Only one Client FQDN option MAY appear in a message, though it may be instantiated in a message as multiple options [9]. DHCP clients and servers supporting this option, MUST implement DHCP option concatenation [9]. In the terminology of [9], the Client FQDN option is a concatenation-requiring option.

The code for this option is 81. Len contains the number of octets that follow the Len field, and the minimum value is 3 (octets).

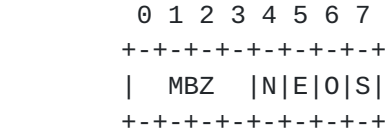
The format of the Client FQDN option is:



The above figure follows the conventions of [12].

2.1. The Flags Field

The format of the 1-octet Flags field is:



The "S" bit indicates whether the server SHOULD or SHOULD NOT perform the A RR (FQDN to address) DNS updates. A client sets the bit to 0 to indicate the server SHOULD NOT perform the updates and 1 to indicate 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 1, the server has taken responsibility for A 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 A 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 "E" bit indicates the encoding of the Domain Name field. 1 indicates canonical wire format, without compression, as described in [3], section 3.1. This encoding SHOULD be used by clients and MUST be supported by servers. 0 indicates a now deprecated ASCII encoding (see Section 2.3.1). A server MUST use the same encoding as that used by the client. A server that does not support the deprecated ASCII encoding MUST ignore Client FQDN options that use that

encoding.

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

2.2. The RCODE Fields

The two 1-octet RCODE1 and RCODE2 fields are deprecated. A client SHOULD set these to 0 when sending the option and SHOULD ignore them on receipt. A server SHOULD set these to 255 when sending the option and MUST ignore them on receipt.

As this option with these fields is already in wide use, the fields are retained. These fields were originally defined for use by a DHCP server to indicate to a DHCP client the Response Code from any A (RCODE1) or PTR (RCODE2) RR DNS updates it has performed or a value of 255 was used to indicate that an update had been initiated but had not yet completed. Each of these fields is one octet long. These fields were defined before EDNS0 [13], which describes a mechanism for extending the length of a DNS RCODE to 12 bits, which is another reason to deprecate them.

If the client needs to confirm the DNS update has been done, it MAY use a DNS query to check whether the mapping is up to date. However, depending on the load on the DHCP 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.

2.3. 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 canonical wire format as specified in [3], section 3.1. If the DHCP client uses the canonical wire format, it MUST set the "E" bit in the Flags field to 1. 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.

2.3.1. Deprecated ASCII Encoding

A substantial population of clients implemented an earlier draft version of this specification, which permitted an ASCII encoding of the Domain Name field. Server implementations SHOULD be aware that clients which send the Client FQDN option with the "E" bit set to 0 are using an ASCII encoding of the Domain Name field. Servers MAY be prepared to return an ASCII encoded version of the Domain Name field to such clients. Servers that are not prepared to return an ASCII encoded version MUST ignore the Client FQDN option if the "E" bit is 0. 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.

Clients and servers SHOULD follow the character set rules of [6]RFC 952, fourth section ("Assumptions"), first 5 sentences, as modified by [7] section 2.1. However, implementers SHOULD also be aware that some client software may send data intended to be in other character sets. This specification does not require support for other character sets.

3. DHCP Client Behavior

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

3.1. Interaction With Other Options

Other DHCP options MAY carry data that is related to the Domain Name field of the Client FQDN option. The Host Name option [12], for example, contains an ASCII string representation of the client's host name. In general, a client does not need to send redundant data, and therefore clients which send the Client FQDN option in their messages MUST NOT also send the Host Name option. Clients which receive both the Host Name option and the Client FQDN option from a server SHOULD prefer Client FQDN option data. Section 4 instructs servers to

ignore the Host Name option in client messages which include the Client FQDN option.

3.2. Client Desires to Update A RRs

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, 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 DHCPDISCOVER messages as well as its DHCPREQUEST messages. The "S", "O", and "N" bits in the Flags field in the option MUST be 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) unless the server has set the "S" bit to 1. If the "S" is 1, the DHCP client SHOULD NOT initiate an update for the name in the server's returned Client FQDN option Domain Name field. However, a DHCP 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.

3.3. Client Desires Server to Do DNS Updates

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 and MAY include the Client FQDN option in its DHCPDISCOVER. The "S" bit in the Flags field in the option MUST be 1 and the "O" and "N" bits MUST be 0.

3.4. 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 DHCPREQUEST message and MAY include the Client FQDN option in its DHCPDISCOVER. 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 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 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; and, MAY also perform the A RR updates if the "S" bit is 1.

3.5. Domain Name and DNS Update Issues

As there is a possibility that the DHCP 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 DHCPDISCOVER messages. If the DHCP server returns different Domain Name data in its DHCPOFFER message, the client could use that data in performing its own eventual A RR update, or in forming the Client FQDN option that it sends in its DHCPREQUEST message. There is no requirement that the client send identical Client FQDN option data in its DHCPDISCOVER and DHCPREQUEST 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 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 will not receive any indication (either positive or negative) from the server 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 (see Section 2.2).

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 associated with the leased address before sending a DHCPRELEASE 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.

A client that desires to perform DNS updates to A RRs SHOULD NOT do so if the client's address is a private address [8].

4. DHCP Server Behavior

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

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

- If the client's "E" bit is 0 and the server does not support ASCII encoding (Section 2.3.1), the server SHOULD ignore the Client FQDN option.
- The server sets to 0 the "S", "O", and "N" bits in its copy of the option it will return to the client. The server copies the client's "E" bit.
- 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.
- 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 A 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 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. The server MUST use the same encoding format (ASCII or DNS binary encoding) that the client used in the Client FQDN option in its DHCPDISCOVER or DHCPREQUEST, and MUST set the "E" bit in the option's Flags field accordingly.

If a client sends both the Client FQDN and Host Name option, the server SHOULD ignore the Host Name option.

The server SHOULD set the RCODE1 and RCODE2 fields to 255 before sending the Client FQDN message to the client in a DHCPOFFER or DHCPACK.

4.1. 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 DHCPACK messages (to be) sent to the client. However, the server SHOULD delete any RRs which 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 A RR DNS update if the "S" bit is 1 in the Flags field of the Client FQDN option in the DHCPACK message (to be) sent to the client.

The server MAY perform these updates even if the client's DHCPREQUEST did not carry the Client FQDN option. The server MUST NOT initiate

DNS updates when responding to DHCPDISCOVER messages from a client.

The server MAY perform its DNS updates (PTR RR or PTR and A RR) before or after sending the DHCPACK message to the client.

If the server's A RR DNS update does 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 can occur, for example, if the server detects and resolves a domain-name conflict [10]. In such cases, the domain name that the server returns to the DHCP client would change between two DHCP 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 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.

When 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.

5. 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 which 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 ([16]) and NOTIFY ([17]) 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 lease time. The RR TTL on a DNS record added SHOULD NOT exceed 1/3 of the lease time, 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 time.

While clients and servers MAY update the TTL of the records as the lease 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.

6. DNS Update Conflicts

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

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" [10]) SHOULD be used.

7. IANA Considerations

IANA has already assigned DHCP option 81 to the Client FQDN option. As this document describes the option's use, IANA is requested to reference this document for option 81.

8. 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 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 [14]) when

performing DNS updates.

Whether a DHCP client is 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 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 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 is likely 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 [15] 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.

It is critical to implement proper conflict resolution, and the security considerations of conflict resolution apply [10].

9. Acknowledgements

Many thanks to Mark Beyer, Jim Bound, Ralph Droms, Robert Elz, Peter

Ford, Olafur Gudmundsson, Edie Gunter, Andreas Gustafsson, David W. Hankins, R. Barr Hibbs, Kim Kinnear, Stuart Kwan, Ted Lemon, Ed Lewis, Michael Lewis, Josh Littlefield, Michael Patton, Pekka Savola, Jyrki Soini, and Glenn Stump for their review and comments.

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., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[6] Harrenstien, K., Stahl, M., and E. Feinler, "DoD Internet host table specification", RFC 952, October 1985.

[7] Braden, R., "Requirements for Internet Hosts - Application and Support", STD 3, RFC 1123, October 1989.

[8] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[9] Lemon, T. and S. Cheshire, "Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)", RFC 3396, November 2002.

[10] Stapp, M. and B. Volz, "Resolution of DNS Name Conflicts Among DHCP Clients (draft-ietf-dhc-ddns-resolution-*.txt)", February 2006.

10.2. Informative References

[11] Marine, A., Reynolds, J., and G. Malkin, "FYI on Questions and Answers - Answers to Commonly asked "New Internet User"

Questions", RFC 1594, March 1994.

[12] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

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

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

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

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

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

Authors' Addresses

Mark Stapp
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA

Phone: 978.936.1535
Email: mjs@cisco.com

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

Phone: 978.936.0382
Email: volz@cisco.com

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

Phone: 408.745.2000
Email: yakov@juniper.net

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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