Network Working Group
Internet Draft
Expiration Date: August 1998

Yakov Rekhter
Cisco Systems
February 1998

Interaction between DHCP and DNS
draft-ietf-dhc-dhcp-dns-07.txt

1. Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as ``work in progress.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

2. Abstract

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

This document specifies how DHCP clients and servers should use the Dynamic DNS Updates mechanism to update the DNS name to address and address to name mapping, so that the mappings for DHCP clients would be consistent with the IP addresses that the clients acquire via DHCP.

3. Terminology

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

- "MUST"
  This word or the adjective "REQUIRED" means that the item is an absolute requirement of this specification.

- "MUST NOT"
  This phrase means that the item is an absolute prohibition of this specification.

- "SHOULD"
  This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

- "SHOULD NOT"
  This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

- "MAY"
  This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

4. Interaction between DHCP and DNS

DNS [RFC1034, RFC1035] maintains (among other things) the information about mapping between hosts' Fully Qualified Domain Names (FQDNs) [RFC1594] 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.

DHCP [RFC1541] provides a mechanism by which a host (a DHCP client) could acquire certain configuration information, and specifically 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 the information maintained by DNS for a DHCP client 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.

Dynamic DNS Updates [RFC2136] is a mechanism that enables DNS information to be updated DNS over a network.

The Dynamic 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 Dynamic DNS Updates protocol) to reflect the new address. Likewise, when an IP address gets assigned to a host with a particular FQDN, the PTR RR associated with this address would be updated (using the Dynamic DNS Updates protocol) to reflect the new FQDN.

5. Models of operations

When a DHCP client acquires a new address, both the A RR (for the client's FQDN) and the PTR RR (for the acquired address) have to be updated. Therefore, we have two separate Dynamic DNS Update transactions. 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, upon some introspection one could realize that not all permutations make sense. This document covers the possible design permutations:

(1) DHCP client updates the A RR, DHCP server updates the PTR RR

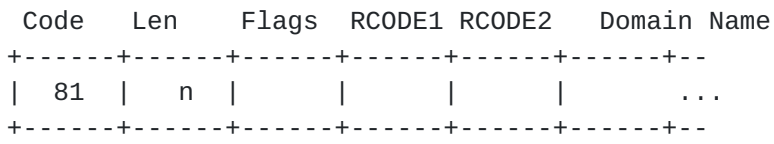
(2) DHCP server updates both the A and the PTR RRs

One could observe that 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.

5.1. Client FQDN Option

To update the IP address to FQDN mapping a DHCP server needs to know 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 option, called "Client FQDN".

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



The Flags field allows a DHCP client to indicate to a DHCP server whether (a) the client wants to be responsible for updating the FQDN to IP address mapping (if Flags is set to 0), or (b) the client wants the server to be responsible for updating the FQDN to IP address mapping (if Flags is set to 1). The Flags field also allows a DHCP server to indicate to a DHCP client that the server assumes the responsibility for updating the FQDN to IP address mapping, even if the client wants to be responsible for this update (if Flags is set to 3).

The RCODE1 and RCODE2 fields are used by a DHCP server to indicate to a DHCP client the Response Code from Dynamic DNS Updates.

The Domain Name part of the option carries FQDN of a client.

5.2. DHCP Client behavior

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

If a client that owns/maintains is 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. 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 completed a final check on the parameters passed in the message), the client MUST originate an update for the A RR (associated with the client's FQDN). The update

MUST be originated following the procedures described in [RFC2136].

A client that owns/maintains its own FQDN 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 MUST include the Client FQDN option in the DHCPREQUEST message originated by the client. The Flags field in the option MUST be set to 1. In this case, the client MAY supply an FQDN in the Client FQDN option, or it MAY leave that field empty as a signal to the server to determine an FQDN for the client in a local to the server manner.

A client that delegates the responsibility for updating the FQDN to IP address mapping to a server MAY not receive any indications (either positive or negative) from the server whether the server was able to perform the update. In this case the client SHOULD use 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 address lease prior to the lease expiration time, and the client is responsible for updating its A RR(s), the client SHOULD delete the A RR (following the procedures described in [RFC2136]) associated with the leased address before sending DHCP RELEASE message.

5.3. 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 SHOULD originate an update for the PTR RR (associated with the address leased to the client). The update MUST be originated following the procedures described in Section 5.4. 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] MUST be carried to the client in the RCODE1 field of the Client FQDN option in the DHCPACK message and the RCODE2 field MUST be set to 0. 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, and the RCODE2 field MUST be set to 0. The choice between the two alternatives is a local to a DHCP server matter.

In addition, if the Client FQDN option carried in the DHCPREQUEST message has its Flags field set to 1, then the server MUST originate

an update for the A RR (associated with the FQDN carried in the option). The update MUST be originated following the procedures described in Section 5.4. 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] 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 DHCKACK message MUST be set to 255. The choice between the two alternatives is a local to the server matter.

Even, if the Client FQDN option carried in the DHCPREQUEST message has its Flags field set to 0 (indicating that the client wants to update the A RR), the server MAY (under configuration control) update the A RR. The update MUST be originated following the procedures described in Section 5.4. 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] MUST be carried to the client in the RCODE2 field of the Client FQDN option in the DHCPACK message, and the Flags field in the Client FQND option MUST be set to 3. 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 DHCKACK message MUST be set to 255, and the Flags field in the Client FQDN option MUST be set to 3. The choice between the two alternatives is a local to the server matter.

When a server receives a DHCPREQUEST message from a client, and the message contains the Client FQDN option, the server MUST ignore the value carried in the RCODE1 and RCODE2 fields of the option.

When a DHCP server sends the Client FQDN option to a client in the DHCPACK message, the server MUST copy the Domain Name fields from the Client FQDN option that the client sent to the server in the DHCPREQUEST message.

If the DHCPREQUST message received by a DHCP server from a DHCP client doesn't carry the Client FQDN option (e.g., the client doesn't implement the Client FQDN option), and the DHCP client acquires its FQDN from a DHCP server (as part of a normal DHCP transaction), then the server MAY be configured to update both A and PTR RRs. The updates MUST be originated following the procedures described in Section 5.4.

If a server originates updates for both the A and PTR RRs, then the order in which the updates are generated is not significant.

If a server detects that a lease on an address that the server leases to a client expires, the server SHOULD delete the PTR RR associated with the address. In addition, if the client authorized the server to update its A RR, the server SHOULD also delete the A RR. The deletion MUST follow the procedures described in [RFC2136].

If a server terminates a lease on an address prior to the lease expiration time, the server SHOULD delete the PTR RR associated with the address. In addition, if the client (that leased the address) authorized the server to update its A RR, the server SHOULD also delete the A RR. The deletion MUST follow the procedures described in [RFC2136].

5.4. Procedures for performing DNS updates

When a DHCP server needs to update the PTR RR for a particular IP address, the server just adds a new PTR RR for that address.

When a DHCP server needs to update the A RR for a particular FQDN, the server first has to delete all the A RRs associated with that FQDN, and then add a new A RR for that FQDN. Note that this rule precludes the ability to support multi-homed hosts in the scenario where A RRs are updated by a DHCP server. Therefore, multi-homed hosts SHOULD perform updates to their A RRs by themselves.

Procedures for deleting and adding RRs are described in [RFC2136].

6. Updating other RRs

The procedures described in this document cover updates only to the A and PTR RRs. Updating other types of RRs is outside the scope of this document.

7. Security Considerations

Whether the client wants to be responsible for updating the FQDN to IP address mapping, or whether the client wants to delegate this responsibility to a server is a local to the client matter. The choice between the two alternatives may be based on a particular security model that is used with the Dynamic 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),

regarless of the wishes of a DHCP client, is a local to the server matter. The choice between the two alternatives may be based on a particular security model.

The client SHOULD use some form of data origin authentication procedures (e.g., DNSSEC [DNSSEC]) when performing DNS updates.

While the DHCP client SHOULD be the one to update the DNS A record, in certain specialized cases a DHCP server MAY do so instead. In this case, the DHCP server MUST be sure of both the name to use for the client, as well as the identity of the client.

In the general case, both of these conditions are not satisfied -- one needs to be mindful of the possibility of MAC address spoofing in a DHCP packet. It is not difficult for a DHCP server to know unambiguously the DNS name to use for a client, but only in certain relatively unusual circumstances will the DHCP server know for sure the identity of the client. One example of such a circumstance is where the DHCP client is connected to a network through an MCNS cable modem, and the CMTS (head-end) of the cable modem ensures that MAC address spoofing simply does not occur.

Another example where the DHCP server would know the identity of the client would be in a case where it was interacting with a remote access server which encoded a client identification into the DHCP client-id option. In this case, the remote access server as well as the DHCP server would be operating within a trusted environment, and the DHCP server could 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.

In either of these cases, a DHCP server would be able to correctly enter the DNS A record on behalf of a client, since it would know the name associated with a client (through some administrative procedure outside the scope of this protocol), and it would also know the client's identity in a secure manner.

8. References

[RFC1034] P. Mockapetris, "Domain names - concepts and facilities", RFC1034, 11/01/1987

[RFC1035] P. Mockapetris, "Domain names - implementation and specification", RFC1035, 11/01/1987

[RFC2131] R. Droms, "Dynamic Host Configuration Protocol", RFC2131, March 1997

[RFC1594] A. Marine, J. Reynolds, G. Malkin, "FYI on Questions and Answer Answers to Commonly asked ``New Internet User'' Questions", RFC1594, 03/11/1994

[DNSSEC]

[RFC2136] P. Vixie, S. Thomson, Y. Rekhter, J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC2136, April 1997

9. Acknowledgements

Many thanks to Mark Beyer, Jim Bound, Ralph Droms, Peter Ford, Edie Gunter, Kim Kinnear, Stuart Kwan, Ted Lemon, Michael Lewis, Michael Patton, Mark Stapp, and Glenn Stump for their review and comments.

10. Author Information

Yakov Rekhter
cisco Systems, Inc.
170 Tasman Dr.
San Jose, CA 95134
Phone: (914) 235-2128
email: yakov@cisco.com