Network Working Group
Internet Draft
Expiration Date: May 1998

Yakov Rekhter
Cisco Systems
November 1997

Interaction between DHCP and DNS
draft-ietf-dhc-dhcp-dns-05.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. 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 [DynDNS] 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.

4. 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

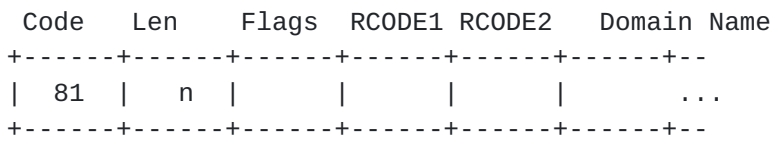
(2) DHCP server updates both the A and the PTR RRs

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.

4.1. 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.

4.2. DHCP Client behavior

If a client 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 shall include the Client FQDN option in the DHCPREQUEST message originated by the client. The Flags field in the option shall

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 shall originate an update for the A RR (associated with the client's FQDN). The update shall be originated following the procedures described in [DynDNS].

If a client does not want to be responsible for updating the FQDN to IP address mapping for the FQDN and address(es) used by the client, then the client shall include the Client FQDN option in the DHCPREQUEST message originated by the client. The Flags field in the option shall be set to 1.

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 may use DNS query to check whether the mapping is updated.

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

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).

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 [DynDNS]) associated with the leased address before sending DHCP RELEASE message.

4.3. 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 may originate an update for the PTR RR (associated with the address leased to the client). The update shall be originated following the procedures described in Section 4.4. The server may originate the update before the server sends the DHCPACK message to the client. In this case the RCODE from the update [DynDNS] shall be carried to the client in the RCODE1 field of the Client FQDN option in the DHCPACK message and the

RCODE2 field shall 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 shall be set to 255, and the RCODE2 field shall 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 shall originate an update for the A RR (associated with the FQDN carried in the option). The update shall be originated following the procedures described in Section 4.4. The server may originate the update before the server sends the DHCPACK message to the client. In this case the RCODE from the update [DynDNS] shall 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 shall 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 could (under configuration control) update the A RR. The update shall be originated following the procedures described in Section 4.4. The server may originate the update before the server sends the DHCPACK message to the client. In this case the RCODE from the update [DynDNS] shall 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 shall 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 shall be set to 255, and the Flags field in the Client FQDN option shall be set to 3. The choice between the two alternatives is a local to the server matter.

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.

When a server receives a DHCPREQUEST message from a client, and the message contains the Client FQDN option, the server shall 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 shall 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, 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. In this scenario the DHCPOFFER message originated by the server shall carry the Domain Name option, and the client acknowledges the use of the FQDN carried in this option by including the option (with the FQDN) in the DHCPREQUEST originated by the client. The updates shall be originated following the procedures described in Section 4.4.

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 should follow the procedures described in [DynDNS].

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 should follow the procedures described in [DynDNS].

4.4. 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 [DynDNS].

5. 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.

6. Security Considerations

Security issues are not discussed in this document.

7. 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

[RFC1541] R. Droms, "Dynamic Host Configuration Protocol", RFC1541, 10/27/1993

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

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

8. Acknowledgements

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

9. Author Information

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