DNS Exercises[1]

The Domain Name System

The Domain Name System (DNS) plays a key role in the Internet today as it allows applications to use fully qualified domain names (FQDN) instead of IPv4 or IPv6 addresses. Many tools allow to perform queries through DNS servers. For this exercise, we will use `dig` which is installed on most Unix systems.

A typical usage of `dig` is as follows

```
dig @server -t type fqdn
```

where

- `server` is the IP address or the name of a DNS server or resolver
- `type` is the type of DNS record that is requested by the query such as NS for a name server, A for an IPv4 address, AAAA for an IPv6 address, MX for a mail relay, …
- `fqdn` is the fully qualified domain name being queried

1. What are the IP addresses of the resolvers that the dig implementation you are using relies on?
2. What is the IP address that corresponds to *www.fauser.it*? Which type of DNS query does `dig` send to obtain this information?
3. Which type of DNS request do you need to send to obtain the name servers that are responsible for a given domain?
4. What are the name servers that are responsible for the “it” top-level domain? Where are they located? Is it possible to use IPv6 to query them?
5. When run without any parameter, `dig` queries one of the root DNS servers and retrieves the list of the names of all root DNS servers. For technical reasons, there are only 13 different root DNS servers. This information is also available as a text file from *http://www.internic.net/zones/named.root* . What are the IP addresses of all these servers. Can they be queried by using IPv6?
6. Assume now that you are residing in a network where there is no DNS resolver and that you need to start your query from the DNS root.
   - Use `dig` to send a query to one of these root servers to find the IP address of the DNS server(s) (NS record) responsible for the “*org*” top-level domain
   - Use `dig` to send a query to one of these DNS servers to find the IP address of the DNS server(s) (NS record) responsible for “*root-servers.org*”
   - Continue until you find the server responsible for *www.root-servers.org*
   - What is the lifetime associated to this IP address?

1 These exercises are taken from *Computer Networking: Principles, Protocols and Practice* by Olivier Bonaventure. (http://cnp3book.info.ucl.ac.be/1st/html/application/exercises/ex-application.html)

7. Perform the same analysis for a popular website such as *www.google.com*. What is the lifetime associated to this IP address? If you perform the same request several times, do you always receive the same answer? Can you explain why a lifetime is associated to the DNS replies?
8. Use `dig` to find the mail relays used by the *fauser.it* and *gmail.com* domains. What is the *TTL* of these records (use the `+ttlid` option when using `dig`)? Can you explain the preferences used by the *MX* records. You can find more information about the *MX* records in RFC 974.
9. Use `dig` to query the IPv6 address (DNS record AAAA) of the following hosts:
   - *www.sixxs.net*
   - *www.google.com*
   - *ipv6.google.com*
10. When `dig` is run, the header section in its output indicates the id the DNS identifier used to send the query. Does your implementation of `dig` generates random identifiers?

    A typical usage of `dig` is as follows

```
dig -t MX fauser.it

<<>> DiG 9.10.3 <<>> -t MX fauser.it
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5626
```

11. The DNS protocol can run over UDP and over TCP. Most DNS servers prefer to use UDP because it consumes fewer resources on the server. However, TCP is useful when a large answer is expected or when a large answer must. You can force the utilisation of TCP by using `dig +tcp`. Use TCP and UDP to query a root DNS server. Is it faster to receive an answer via TCP or via UDP?