Network Lab

Karl 'karlwik' Wikström Vidar 'mvidar' Magnusson

September 2020

1. - **IPV4:** 10.0.0.191
   - **Hostname:** defcon-4.chalmers.it
   - **Command:** dig -x ipv4

   (a) The sections we are getting are an optional *pseudosection*, an *questions* section and a *answers* section. The pseudosection contains some metadat regarding the request, the questions describes the request (i.e. our query) and the answer contains all the answers to this request.

   - **RA** indicates that recursion is available.
   - **IP of the neighbours computer:** 10.0.0.244
   - **IP for the responding server:** 10.0.0.1

   (b) The mappings file tells us which hostnames corresponds to which IP addresses and has the format `*hostname* *ipv4 address*`

   (c) The field indicating the error is the *status* field, which in this case tells us *NXDOMAIN* meaning that the domain does not exist. We did not get an answers sections as no answers were for found for our query.

2. (a) We can use the command `cat /etc/resolv.conf` to find out which DNS server we are currently using.

   (b) We looked up `remote11.chalmers.se`:

   - **The name of the computer:** remote11.
   - **The IP of the computer:** 129.16.29.50.
   - **Responding server IP:** 10.0.0.1

   (c) No, this is because the server that answers is not a DNS server but rather a router or similar device.

3. (a) We got an authoritative answer from `129.16.2.40` which contains (among other things) a list of authoritative name servers, if we now run `dig -x` on the IP that answered (129.16.2.40) and we can see that it corresponded to `ns1.chalmers.se` which was in the list of authoritative server in the initial query.

   (b) We asked `ns1.chalmers.se` for `stanford.edu` but we got a response with no answers, this is due to the fact that ns1 is unaware of that address and is unable to recursivly forward the query to get an answer from a server that knows it.

   (c) We use the command `dig kth.se ns` and get that the authoritative name servers for `kth.se` is (all of the responses are of RR type NS):

   - a.ns.kth.se

- b.ns.kth.se
- nic2.lth.se
- ns2.chalmers.se

(d) When we query `ns2.chalmers.se` we get a rich response with a lot of data, however, when we query `sunic.sunet.se` we don't get an answer at all. This is because ns2 is an authorative name server for kth but sunic is authorative but not for kth and does not do a recursive query to get the information from any higher node that knows of / is an authorative name server for kth.

4. (a) Caching is practical to save performance, however, it could become problematic if it's too outdated, therefore the TTL value is used to make sure that the cache is always relatively updated, or at least will be up to date within the next few minutes or so. TTL means Time To Live and appears to be initially set to 600 for kth.se

   (b) In the response we get from `ns2.chalmers.se` the TTL value is always 600. This is probably because the authorative nameservers answer is not cached but is the original answer and the TTL value here represents what we should set the TTL to, if we cached the result.