DNS Exercises

Daniel Díaz Sánchez

September 2024

1. Problems

1. Consider the following DNS information (NS records). In the solution, use the word "root" to indicate any root DNS server since their names or IP addresses are not available.

```
;; ANSWER SECTION:
com.                     129301   IN      NS      g.gtld-servers.net.
com.                     129301   IN      NS      k.gtld-servers.net.
;; ANSWER SECTION:
aptel.com.               123101   IN      NS      aku.aptel.com.
aptel.com.               123101   IN      NS      uka.aptel.com.
;; ANSWER SECTION:
target.aptel.com.        86400    IN      NS      arrakis.aptel.com.
target.aptel.com.        86400    IN      NS      dune.aptel.com.
;; ANSWER SECTION:
www.target.aptel.com.    86400    IN       A      163.117.141.114
```

Considering zones .com, aptel.com, target.aptel.com, .es, .prov.es.

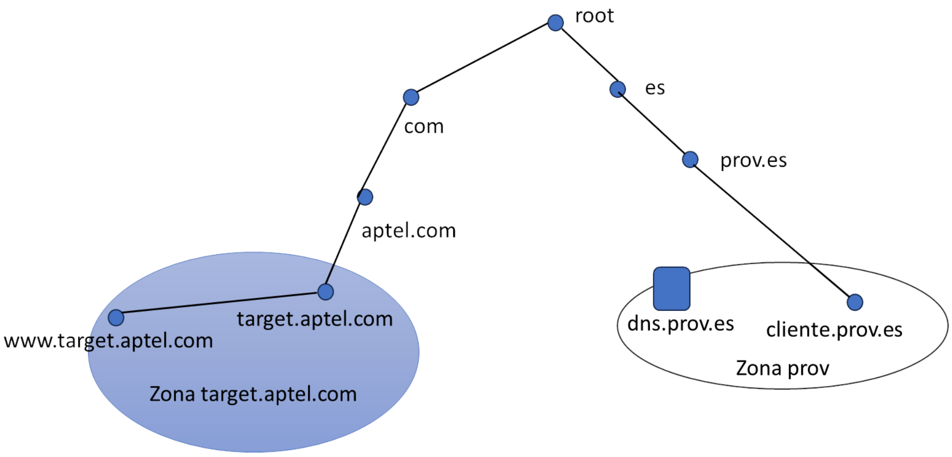

Figura 1: DNS domains

(a) Observe Figure 1. What DNS queries and responses will **cliente.prov.es generate/receive if it requests the RR A record for** `www.target.aptel.com`**?** Indicate each DNS query and response in the provided table. Use the blank space if you need to explain anything. Provide the order, specify whether it is a query or a response, the source (from), the destination (to) of the query or response. You must also indicate the RR requested in the query as well as the RR returned in the response (the important part) and the flags. Also, consider the following:

- The DNS server name for the client is `dns.prov.es` and it accepts recursive queries.
- The rest of the DNS servers involved in the process do not accept recursive queries.
- All servers do not have records in their cache memory.

Order	Req.	Res.	origin	destination	Inf. REQuested / RESponded	Flags
1			cliente.prov.es	dns.prov.es	REQ: A record of www.target.aptel.com	rd (recursion desired)
2						
3						
4						
5						
6						
7						
8						

Order	Req.	Res.	origin	destination	Inf. requested / responded	Flags
9						
10						

2. Considering the following information and DNS responses...

Response 1 (truncated - not fully shown in the statement - without additional section)

```
; <<>> DiG 9.16.33-Debian <<>> NS .
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2805
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: b1bf5f2773fa55bdeb6072a6635a6684e11b104840604e14 (good)
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       518400  IN      NS      c.root-servers.net.
.                       518400  IN      NS      f.root-servers.net.
.                       518400  IN      NS      l.root-servers.net.
.                       518400  IN      NS      j.root-servers.net.
.                       518400  IN      NS      a.root-servers.net.
;; Query time: 63 msec
;; SERVER: 163.117.141.212#53(163.117.141.212)
;; WHEN: Thu Oct 27 13:07:48 CEST 2022
;; MSG SIZE  rcvd: 839
```

Respuesta 2 (truncated - not fully shown in the statement - without additional section)

```
; <<>> DiG 9.16.33-Debian <<>> NS com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22377
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 201c6296f60c64c9eafabba4635a66cca2421b494748b481 (good)
;; QUESTION SECTION:
;com.                           IN      NS

;; ANSWER SECTION:
com.                    64854   IN      NS      m.gtld-servers.net.
com.                    64854   IN      NS      l.gtld-servers.net.
com.                    64854   IN      NS      d.gtld-servers.net.
com.                    64854   IN      NS      a.gtld-servers.net.
com.                    64854   IN      NS      k.gtld-servers.net.

;; Query time: 3 msec
;; SERVER: 163.117.141.212#53(163.117.141.212)
;; WHEN: Thu Oct 27 13:09:00 CEST 2022
;; MSG SIZE  rcvd: 856
```

Respuesta 3 (truncated - not fully shown in the statement - without additional section)

```
; <<>> DiG 9.16.33-Debian <<>> NS google.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43767
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: b4e9c111658f89ef60181ab2635a66f56e21e3fb427792fa (good)
;; QUESTION SECTION:
;google.com.                    IN      NS
```

```
;; ANSWER SECTION:
google.com.             65713   IN      NS      ns1.google.com.
google.com.             65713   IN      NS      ns3.google.com.
google.com.             65713   IN      NS      ns4.google.com.
google.com.             65713   IN      NS      ns2.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.         183404  IN      A       216.239.32.10
ns2.google.com.         65931   IN      A       216.239.34.10
ns3.google.com.         65931   IN      A       216.239.36.10
ns4.google.com.         65931   IN      A       216.239.38.10

;; Query time: 23 msec
;; SERVER: 163.117.141.212#53(163.117.141.212)
;; WHEN: Thu Oct 27 13:09:41 CEST 2022
;; MSG SIZE  rcvd: 315
```

Consider the diagram in Figure 2

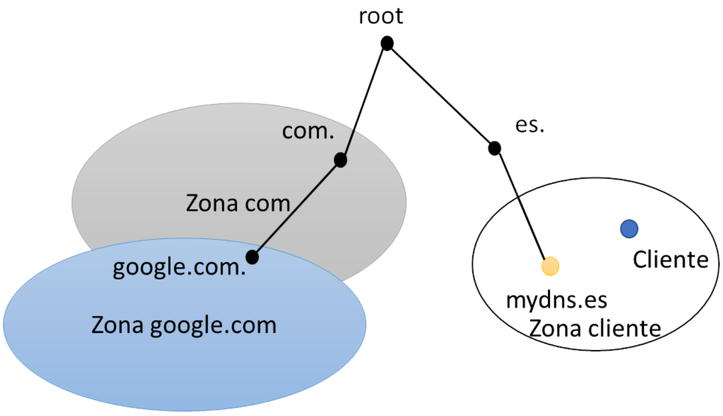

Figura 2: DNS Servers

(a) Indicate all the queries and responses (including the type of records returned and queried as well as flags) that will be generated if the Client requests the A record of the machine www.google.com, considering that:

- The domain name server for the Client is mydns.es and it accepts recursive queries.
- The other DNS servers involved do not respond recursively.
- All servers have an empty cache.

(b) Indicate, with justification, the maximum and minimum number of RRs that a zone must have for the record types SoA, MX, and NS.

3. Suppose a primary DNS server has the following RRs for the A type of `www.uc3m.es`:

```
www.uc3m.es. 240 IN A 163.117.141.114
www.uc3m.es. 240 IN A 163.117.141.130
```

Two clients named `cliente1.prov.es` and `cliente2.prov.es` have `dns.prov.es` configured as their default DNS server (see Figure 3). The servers `tamtam.uc3m.es` and `postel.uc3m.es` are authoritative servers for the domain `uc3m.es`.

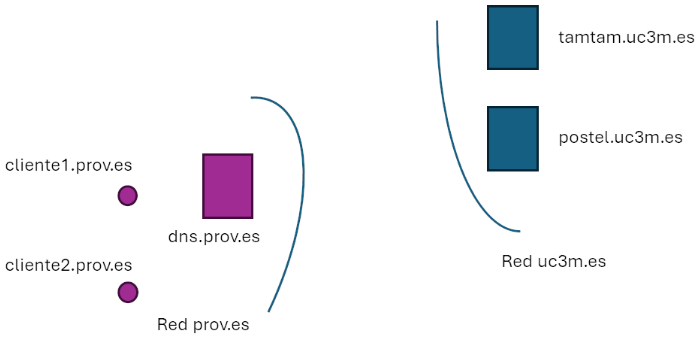

Figura 3: DNS Servers

To answer these questions, consider that at the beginning of each section, the server `dns.prov.es` has an empty cache.

(a) If `cliente1.prov.es` queries the A record of `www.uc3m.es`, what information will it obtain? Will it be received in exactly the written order?

(b) What is the purpose of `www.uc3m.es` having two A records? Explain the functionality and benefit (if any) of this setup and argue with an example that comes to mind.

(c) If `cliente1.prov.es` queries the A record of `www.uc3m.es` at $t = 0$ and `cliente2.prov.es` makes the same query at $t = 120$. What differences will there be in the information received between the response obtained by `cliente1.prov.es` and `cliente2.prov.es`?

(d) If the administrator of `uc3m.es` wants to alternate connections between the IP addresses of `www.uc3m.es` for requests separated by more than 60 seconds, what parameter should the administrator change and why?

(e) Regardless of the number of authoritative servers that exist in the domain `uc3m.es`, where is the only place where the change should be made? Explain the replication procedure and how it is configured. Consider the record shown below:

```
uc3m.es.   86400   IN      SOA     vorteX.uc3m.es. netmaster.uc3m.es.
2024091603 86400 7200 2592000 172800
```