DNS Assignment

Introduction: The dig utility

To carry out this practical assignment we will use the dig utility. Below we resume the main options of this command but we recommend you consult the complete manual page, which can be obtained via the command man dig. If you prefer you may also use the host or nslookup utilities which are similar to dig. The main options of dig are the following (`[]` stands for optional):

```
dig [@server] [-p port#] [name] [type] [queryopt...]
```

- `@server`: specifies the name or IP address of the DNS servers to which the query is to be made; if none is specified, the servers listed in the file /etc/resolv.conf are used.
- `-p port`: is used to indicate a server port in the case where a port different from the default (53) is to be used.
- `name`: specifies the name of the resource registry to be consulted.
- `type`: specifies the type of the resource registry to be consulted: ANY, A, MX, etc.; if none is given, it is assumed to be of type A.
- `queryopt`: one or more of the following options: ..* `+tcp`: used to force the query to be made via TCP (by default UDP is used, except for AXFR or IXFR). +notcp to force UDP. ..* `+ignore`: specifies not to retry the query via TCP if the UDP reply is truncated. ..* `+norecurse`: used to force an iterative query (the default is recursive).

The assignment is divided in two parts:

- in the first we will use dig to query resources from the dns servers
- in the second one we will setup our own DNS server using `named`

Part 1: Queries with a DNS client

Remember the format of a resource record (RR) in DNS is the following:

```
<domain name> <TTL> IN <record type> <value>
```

1. Determine the IP address of the machine `www.mec.es`.

dig www.mec.es
;; ANSWER SECTION:
www.mec.es. 83061 IN A 212.128.114.29

2. Check which machine has the IP address `193.110.128.199`.

dig -x 193.110.128.199
;; ANSWER SECTION:

199.128.110.193.in-addr.arpa. 83238 IN PTR www.elmundo.es.

3. Find out the name and IP address of the DNS servers of the domain `abc.es` and say which of them is primary and which is secondary.

dig NS abc.es
;; ANSWER SECTION:
abc.es. 10930 IN NS ns-cloud-e3.googledomains.com.
abc.es. 10930 IN NS ns-cloud-e1.googledomains.com.
abc.es. 10930 IN NS ns-cloud-e2.googledomains.com.
abc.es. 10930 IN NS ns-cloud-e4.googledomains.com.

dig SOA abc.es
;; ANSWER SECTION:
abc.es. 10589 IN SOA ns-cloud-e1.googledomains.com. cloud-dns-hostmaster.google.com. 2 21600 3600 259200 300

dig googledomains.com SOA => return SOA RR it is a SOA

4. Obtain the SOA registry of the domain `abc.es`, first, by asking the local DNS and, second, by asking the primary server of the `abc.es` domain. Verify that in one case, the response is authoritative and in the other, it isn't.

dig abc.es SOA SAME answer as before, no aa flag => no authoritative dig @ns-cloud-e1.googledomains.com abc.es SOA
Answer contains aa => authoritative

5. If you had a problem with the DNS of `abc.es` and you had to send an e-mail to its administrator, to what address would you send it?

dig SOA abc.es
;; ANSWER SECTION: abc.es. 10589 IN SOA ns-cloud-e1.googledomains.com. '`*cloud-dns-hostmaster.google.com*`'. 2 21600 3600 259200 300

6. Determine the name and IP address of the mail server of the administrator referred to in the previous question

dig google.com MX
;; ANSWER SECTION: google.com. 300 IN MX 10 smtp.google.com. dig smtp.google.com

7. How long will the IP address of `www.vanguardia.es` remain in the cache of your local DNS? Ask your local DNS for this address several times in succession. What do you observe in the TTL of the resource registry?

dig lavanguardia.es NS
dig @dns01.grupogodo.com www.vanguardia.es
TTL in answer is the max TTL with no cache

8. Now ask the same to a root server (for example, `J.ROOT-SERVERS.NET` with IP address `192.58.128.30`) and check in the reply packet that this server does not accept the recursive

mode.

No ra => no recursion available

9. Find out how many computers are carrying out load balancing in the web server `www.elpais.es`. Do you always get the same ones in the same order?

dig www.elpais.es
Two ips

10. By making iterative queries, check the IP address of `www.pcreview.co.uk`. What are the steps you have taken?

> Hint: if your DNS server has this record in the cache it is possible it does not answer with the next step but with the results. In that case, ask directly to a root server in this way: `dig +norecurse www.pcreview.co.uk @A.ROOT-SERVERS.NET`, and continue.

Following the same steps (iterative queries), do you obtain the IP address of `www.bbc.co.uk`?

11. The same can be done with the +trace option of dig. Check the result of doing so.

12. Using the information available via DNS determine the computer or computers (name and IP address) that act as mail servers for the domain `gmail.com`.

dig MX gmail.com
ANSWER SECTION:
gmail.com. 3600 IN MX 5 gmail-smtp-in.l.google.com.
gmail.com. 3600 IN MX 10 alt1.gmail-smtp-in.l.google.com.
gmail.com. 3600 IN MX 20 alt2.gmail-smtp-in.l.google.com.
gmail.com. 3600 IN MX 30 alt3.gmail-smtp-in.l.google.com.
gmail.com. 3600 IN MX 40 alt4.gmail-smtp-in.l.google.com.

13. What would you need to do to obtain all the resource registries of the the zone `lab.it.uc3m.es`?

Find the authoritative name servers
dig NS lab.it.uc3m.es
dig @tamtam.it.uc3m.es lab.it.uc3m.es ANY

14. Find out which of the following domain names are a zone: `google.jobs`, `primevideo.com`, `inf.uc3m.es`, `it.uc3m.es`.

dig domain(no subdomains) SOA. => if no SOA => no Zone

15. Identify the DNS servers, mail servers, the domain administrator's address, and identify the secondary-primary copy times, expiration time, as well as the minimum TTL for the domains `it.uc3m.es` and `csic.es`.

dig domain NS
dig domain MX

dig domain SOA => SOA

Part 2: Creating a domain in a named DNS server

Configuring the named DNS server

`named` is the DNS server that forms part of the most widely-used implementation of DNS in Unix, BIND (Berkeley Internet Name Domain). We are going to use the version of named that can be found in the `directory /usr/dist/sbin/`.

> Warning: it may happen the execution shows an error or warning regarding a library that cannot be loaded. This happens due to the specific library distribution in the lab since 32 bit versions co-exist with 64 versions but it should work despite the error

> Alternativerly, there is a named implementation in `/usr/sbin`

On start-up, `named` reads a configuration file, located by default at `/etc/bind/named.conf`, though we can specify a different file via the command line. Use of the option `-f` is also convenient for this practical (see the named manual page). We will therefore start named using the following command (from the folder in which our config file is located):

```
/usr/dist/sbin/named -c ./named.conf -f
```

The file named.conf is divided into two parts.

- The options section is used to specify configuration aspects such as the port on which named will listen (on startup in user mode it cannot be 53, we will need to specify a non-reserved port such as 10053) and the locaction of certain files that it will need to write during operation (which we will set to be in our account).
- The zone section is used to define one or more DNS zones that this server is responsible for.

An example of a configuration file (where we are supposing that you are working in the subdirectory `rroo/named` of your account; substitute `$HOME` by the complete path of your HOME) is as follows:

```
# file $HOME/rroo/named/named.conf
options {
 port 10053;
directory "$HOME/rroo/named/";
 pid-file "$HOME/rroo/named/named.pid";
};
zone "0.0.127.in-addr.arpa" IN {
 type master;
 file "$HOME/rroo/named/127.0.0";
};
zone "midominio.privado" IN {
 type master;
 file "$HOME/rroo/named/midominio.privado";
};
```

In this case, the file `$HOME/rroo/named/127.0.0` contains the following:

```
$TTL 86400
@       IN      SOA       ns.midominio.privado.       mail.midominio.privado. (
                200403031 ; Numero de Serie: Fecha+Numero
                28800 ; Tiempo de Refresco
                7200 ; Tiempo de Reintento
                604080 ; Caducidad de la informacion
                86400) ; TTL para clientes
        NS      ns.midominio.privado.
1       PTR     localhost.
```

and the file `$HOME/rroo/named/midominio.privado` contains the following:

```
$TTL 86400
@       IN      SOA         ns.midominio.privado.       mail.midominio.privado. (
                            200403031
                            28800
                            7200
                            604800
                            86400 )
                NS          ns.midominio.privado.
                MX          10 mail.midominio.privado.
ns              A           192.168.123.1
mail            A           192.168.123.2
www             CNAME       ns
```

1. Copy the above files, start a named on your computer and use the dig tool to check that it is working properly. Use the following to retrieve all the files:

```
git -c http.sslVerify=false clone https://gitlab.gast.it.uc3m.es/aptel/dns.git
```

2. Stop the named server and modify the configuration files so that it also serves the domain necessary for inverse resolution.

Steps to create a new reverse resolution (BIND)

1️⃣ Decide the IP network

Example:

```
192.168.122.0/24
```

Reverse zone name is written **backwards**:

```
122.168.192.in-addr.arpa
```

2️⃣ Add the reverse zone to `named.conf`

```
zone "122.168.192.in-addr.arpa" IN {
    type master;
    file "/full/path/to/named/192.168.122";
};
```

- Must use **full path**
- `type master` → this server is authoritative

3️⃣ Create the reverse zone file

File: `/full/path/to/named/192.168.122`

```
$TTL 86400
@ IN SOA ns.midominio.privado. mail.midominio.privado. (
    2025121601   ; Serial
    28800        ; Refresh
    7200         ; Retry
    604800       ; Expire
    86400 )      ; Minimum TTL

@   IN NS ns.midominio.privado.

1   IN PTR ns.midominio.privado.
2   IN PTR mail.midominio.privado.
```

Important details

- Only the **last octet** is written (`1`, `2`)
- PTR values must be **fully qualified** (end with dot)

4️⃣ Check file permissions

```
chmod 644 /full/path/to/named/192.168.122
```

BIND must be able to read the file.

5️⃣ Restart (or reload) `named`

```
/usr/dist/sbin/named -c ./named.conf -f
```

(or if already running)

```
rndc reload
```

6️⃣ Test reverse resolution with `dig`

```
dig @localhost -p 10053 -x 192.168.122.1
dig @localhost -p 10053 -x 192.168.122.2
```

Expected:

```
1.122.168.192.in-addr.arpa. PTR ns.midominio.privado.
```
