1.

a)

Petición/Respuesta	IP origen	IP destino	Mensaje
Petición	134.52.41.23	194.224.52.36	¿Cuál es la IP de www.ietf.org?
Petición	194.224.52. 36	25.36.14.98	¿Cuál es la IP del servidor que gestiona el dominio .org?
Respuesta	25.36.14.98	194.224.52.36	La IP es 14.58.96.12
Petición	194.224.52.36	14.58.96.12	¿Cuál es la IP del servidor que gestiona el dominio ieft.org?
Respuesta	14.58.96.12	194.224.52.36	La IP es 16.48.26.19
Petición	194.224.52.36	16.48.26.19	¿Cuál es la IP del servidor que gestiona el dominio www.ieft.org?
Respuesta	14.58.96.12	194.224.52.36	La IP es 12.94.33.126
Respuesta	194.224.52.36	134.52.41.23	La IP es 12.94.33.126

b)

Petición/Respuesta	IP origen	IP destino	Mensaje
Petición	134.52.41.23	194.224.52.36	¿Cuál es la IP de groups.google.com?
Petición	194.224.52. 36	25.36.14.98	¿Cuál es la IP del servidor que gestiona el dominio .com?
Respuesta	25.36.14.98	194.224.52.36	La IP es 120.25.14.87
Petición	194.224.52.36	120.25.14.87	¿Cuál es la IP del servidor que gestiona el dominio Google.com?
Respuesta	120.25.14.87	194.224.52.36	La IP es 215.69.47.35
Petición	194.224.52.36	215.69.47.35	¿Cuál es la IP del servidor que gestiona el dominio groups.google.com?
Respuesta	215.69.47.35	194.224.52.36	La IP es 72.88.41.55
Respuesta	194.224.52.36	134.52.41.23	La IP es 72.88.41.55

c)

Petición/Respuesta	IP origen	IP destino	Mensaje
Petición	134.52.41.23	194.224.52.36	¿Cuál es la IP de ftp.rediris.es?
Petición	194.224.52. 36	25.36.14.98	¿Cuál es la IP del servidor que gestiona el dominio .es?
Respuesta	25.36.14.98	194.224.52.36	La IP es 72.91.83.17
Petición	194.224.52.36	72.91.83.17	¿Cuál es la IP del servidor que gestiona el dominio rediris.es?
Respuesta	72.91.83.17	194.224.52.36	La IP es 45.36.87.19
Petición	194.224.52.36	45.36.87.19	¿Cuál es la IP del servidor que gestiona el dominio ftp.rediris.es?
Respuesta	45.36.87.19	194.224.52.36	La IP es 212.54.87.86
Respuesta	194.224.52.36	134.52.41.23	La IP es 212.54.87.86

d)

Petición/Respuesta	IP origen	IP destino	Mensaje
Petición	134.52.41.23	194.224.52.36	¿Cuál es la IP de www.rediris.es?
Petición	194.224.52. 36	25.36.14.98	¿Cuál es la IP del servidor que gestiona el dominio .es?
Respuesta	25.36.14.98	194.224.52.36	La IP es 72.91.83.17
Petición	194.224.52.36	72.91.83.17	¿Cuál es la IP del servidor que gestiona el dominio rediris.es?
Respuesta	72.91.83.17	194.224.52.36	La IP es 45.36.87.19
Petición	194.224.52.36	45.36.87.19	¿Cuál es la IP del servidor que gestiona el dominio www.rediris.es?
Respuesta	45.36.87.19	194.224.52.36	La IP es 212.54.87.87
Respuesta	194.224.52.36	134.52.41.23	La IP es 212.54.87.87

e)

Petición/Respuesta	IP origen	IP destino	Mensaje
Petición	134.52.41.23	194.224.52.36	¿Cuál es la IP de kernel.org?
Petición	194.224.52. 36	25.36.14.98	¿Cuál es la IP del servidor que gestiona el dominio .org?
Respuesta	25.36.14.98	194.224.52.36	La IP es 72.91.83.17
Petición	194.224.52.36	72.91.83.17	¿Cuál es la IP del servidor que gestiona el dominio rediris.es?
Respuesta	72.91.83.17	194.224.52.36	La IP es 45.36.87.19
Petición	194.224.52.36	45.36.87.19	¿Cuál es la IP del servidor que gestiona el dominio www.rediris.es?
Respuesta	45.36.87.19	194.224.52.36	La IP es 136.45.72.112
Respuesta	194.224.52.36	134.52.41.23	La IP es 136.45.72.112

f)

Petición/Respuesta	IP origen	IP destino	Mensaje
Petición	134.52.41.23	194.224.52.36	¿Cuál es la IP de www.groups.google.com?
Petición	194.224.52. 36	25.36.14.98	¿Cuál es la IP del servidor que gestiona el dominio .com?
Respuesta	25.36.14.98	194.224.52.36	La IP es 120.25.14.87
Petición	194.224.52.36	120.25.14.87	¿Cuál es la IP del servidor que gestiona el dominio Google.com?
Respuesta	120.25.14.87	194.224.52.36	La IP es 215.69.47.35
Petición	194.224.52.36	215.69.47.35	¿Cuál es la IP del servidor que gestiona el dominio groups.google.com?
Respuesta	215.69.47.35	194.224.52.36	La IP es 72.88.41.55
Petición	194.224.52.36	72.88.41.55	¿Cuál es la IP del servidor que gestiona el dominio www.groups.google.com?
Respuesta	194.224.52.36	134.52.41.23	La IP es 4.2.2.4

2.

a)

Petición/Respuesta	IP origen	IP destino	Mensaje
Petición	134.52.41.23	194.224.52.36	¿Cuál es la IP de www.ietf.org?
Petición	194.224.52. 36	25.36.14.98	¿Cuál es la IP del servidor que gestiona el dominio .org?
Respuesta	25.36.14.98	194.224.52.36	La IP es 14.58.96.12
Petición	194.224.52.36	14.58.96.12	¿Cuál es la IP del servidor que gestiona el dominio ieft.org?
Respuesta	14.58.96.12	194.224.52.36	La IP es 16.48.26.19
Petición	194.224.52.36	16.48.26.19	¿Cuál es la IP del servidor que gestiona el dominio www.ieft.org?
Respuesta	16.48.26.19	194.224.52.36	La IP es 12.94.33.126
Respuesta	194.224.52.36	134.52.41.23	La IP es 12.94.33.126

b)

Petición/Respuesta	IP origen	IP destino	Mensaje
Petición	134.52.41.23	194.224.52.36	¿Cuál es la IP de groups.google.com?
Petición	194.224.52. 36	25.36.14.98	¿Cuál es la IP del servidor que gestiona el dominio .com?
Respuesta	25.36.14.98	194.224.52.36	La IP es 120.25.14.87
Petición	194.224.52.36	120.25.14.87	¿Cuál es la IP del servidor que gestiona el dominio Google.com?
Respuesta	120.25.14.87	194.224.52.36	La IP es 215.69.47.35
Petición	194.224.52.36	215.69.47.35	¿Cuál es la IP del servidor que gestiona el dominio groups.google.com?
Respuesta	215.69.47.35	194.224.52.36	La IP es 72.88.41.55
Respuesta	194.224.52.36	134.52.41.23	La IP es 72.88.41.55

c)

Petición/Respuesta	IP origen	IP destino	Mensaje
Petición	134.52.41.23	194.224.52.36	¿Cuál es la IP de ftp.rediris.es?
Petición	194.224.52. 36	25.36.14.98	¿Cuál es la IP del servidor que gestiona el dominio .es?
Respuesta	25.36.14.98	194.224.52.36	La IP es 72.91.83.17
Petición	194.224.52.36	72.91.83.17	¿Cuál es la IP del servidor que gestiona el dominio rediris.es?
Respuesta	72.91.83.17	194.224.52.36	La IP es 45.36.87.19
Petición	194.224.52.36	45.36.87.19	¿Cuál es la IP del servidor que gestiona el dominio ftp.rediris.es?
Respuesta	45.36.87.19	194.224.52.36	La IP es 212.54.87.86
Respuesta	194.224.52.36	134.52.41.23	La IP es 212.54.87.86

d)

Petición/Respuesta	IP origen	IP destino	Mensaje
Petición	134.52.41.23	194.224.52.36	¿Cuál es la IP de www.rediris.es?
Petición	194.224.52. 36	45.36.87.19	¿Cuál es la IP del servidor que gestiona el dominio www.rediris.es ?
Respuesta	45.36.87.19	194.224.52.36	La IP es 212.54.87.87
Respuesta	194.224.52.36	134.52.41.23	La IP es 212.54.87.87

e)

Petición/Respuesta	IP origen	IP destino	Mensaje
Petición	134.52.41.23	194.224.52.36	¿Cuál es la IP de kernel.org?
Petición	194.224.52. 36	14.58.96.12	¿Cuál es la IP del servidor que gestiona el dominio kernel.org?
Respuesta	14.58.96.12	194.224.52.36	La IP es 136.45.72.112
Respuesta	194.224.52.36	134.52.41.23	La IP es 136.45.72.112

f)

Petición/Respuesta	IP origen	IP destino	Mensaje
Petición	134.52.41.23	194.224.52.36	¿Cuál es la IP de www.groups.google.com?
Petición	194.224.52. 36	72.88.41.55	¿Cuál es la IP del servidor que gestiona el dominio www.groups.google.com ?
Respuesta	72.88.41.55	194.224.52.36	La IP es 4.2.2.4
Respuesta	194.224.52.36	134.52.41.23	La IP es 4.2.2.4

3. ¿Para qué sirven los siguientes comandos?

ipconfig /displaydns: Muestra el contenido de la caché de DNS

ipconfig /flushdns: Limpia la caché de DNS del sistema.

4. Averigua cómo te conectarías a www.hotmail.com sin que el navegador hiciera una consulta DNS.

Con un ping puedo averiguar por mi cuenta la IP del dominio objetivo y luego introducirla en el navegador para que el navegador no haga consultas DNS.

5.

a) ¿Qué contiene el fichero hosts de tu equipo? (Nota: el fichero hosts se encuentra en c:\windows\system32\drivers\etc en Windows XP y en Vista y en /etc/hosts en Linux).

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

b) ¿Qué pasaría si se añadiera la línea siguiente al fichero?

255.255.255.0 www.google.es

Ahora, si pusiera www.google.es en el navegador o le hiciera ping o cualquier cosa, me llevaría a esa IP (pero al no ser una IP valida, daría error).

c) ¿Qué es el “pharming”? Busca información sobre las técnicas de “pharming”.

El pharming es un tipo de ataque que busca redirigir a los usuarios sin que lo sepan a un sitio web fraudulento manipulando la resolución DNS para llevarlos hasta esos sitios.
Las técnicas mas comunes son manipular el archivo de hosts, envenenar la cache DNS, usar proxies o routers controlados por ellos o atacar a servidores DNS.

6.

a) Averigua para qué sirven los dominios .biz, .aero y .info.

.biz: abreviatura e business, para negocios y empresas.

.aero: reservado para la industria de la aviación.

.info: para sitios de información general.

b) Averigua cuáles son los dominios para Dinamarca, Marruecos y Rusia. ¿A

qué países pertenecen los dominios .mt , .tr y .za?
Dinamarca: .dk.

Marruecos: .ma.

Rusia: .ru.

.mt: Malta.

.tr: Turquía.

.za: Sudáfrica.

7. Busca varias direcciones IP de servidores DNS que podrías usar si no funcionaran temporalmente los que tienes.

8.8.8.8, 4.4.4.4 (GOOGLE).

1.1.1.1, 1.0.0.1 (CLOUDFLARE).

208.67.222.222, 208.67.220.220 (OpenDNS).

8. Visita:

http://www.icann.org/

http://www.icann.org/tr/spanish.html

http://red.es

http://www.opendns.com

http://www.dnstools.com/

http://www.dnsstuff.com/tools

http://www.db.ripe.net/whois

http://www.visualroute.com/ (apartado “Live Demo”)

http://root-servers.org

http://f.root-servers.org

¿Cuáles son las IPv4 y v6 de l.root-servers.net?

IPv4: 199.7.83.42

IPv6: 2001:500:9f::42

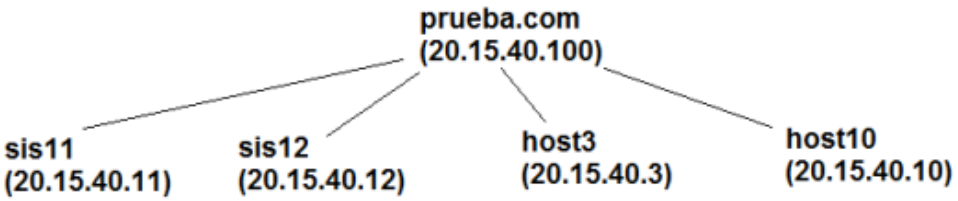
¿Cuántos servidores j.rootservers.net hay en total?

En total hay 87 servidores a nivel global.

¿Cuántos servidores hay en Madrid? ¿Y en Barcelona?

En Madrid hay 3 y en Barcelona 2.

9. Escribe el fichero de zona para el siguiente dominio:



- Los servidores de nombres son sis11 y sis12, siendo sis11 el principal.
- Hay dos servidores de correo, host3 y host10, con prioridades 5 y 10, respectivamente.
- El correo del administrador del servidor DNS es root@prueba.com.
- Los valores numéricos del registro SOA son iguales que los del ejemplo visto en clase.

```
$TTL 86400
@   IN   SOA   sis11.prueba.com. root.prueba.com. (
        2024120601 ; Serial
        3600      ; Refresh
        900       ; Retry
        1209600   ; Expire
        86400 )   ; Minimum TTL
```

; Servidores de nombres

@ IN NS sis11.prueba.com.

@ IN NS sis12.prueba.com.

; Registros A

@ IN A 20.15.40.100

sis11 IN A 20.15.40.11

sis12 IN A 20.15.40.12

host3 IN A 20.15.40.3

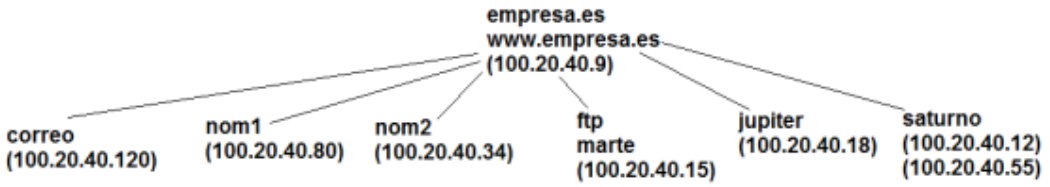
host10 IN A 20.15.40.10

; Servidores de correo

@ IN MX 5 host3.prueba.com.

@ IN MX 10 host10.prueba.com.

10. Escribe el fichero de zona para el siguiente dominio:



- Los servidores de nombres son nom1 y nom2, siendo nom1 el principal.
- Hay un servidor de correo llamado correo, con prioridad 10.
- El correo del administrador del servidor DNS es admin@empresa.es.
- Los valores numéricos del registro SOA son iguales que los del ejemplo visto en clase.

$TTL 86400

@ IN SOA nom1.empresa.es. admin.empresa.es. (

2024120601 ; Serial

3600 ; Refresh

900 ; Retry

1209600 ; Expire

86400) ; Minimum TTL

; Servidores de nombres

@ IN NS nom1.empresa.es.

@ IN NS nom2.empresa.es.

; Registros A

@ IN A 100.20.40.9

nom1 IN A 100.20.40.80

nom2 IN A 100.20.40.34

correo IN A 100.20.40.120

ftp IN A 100.20.40.15

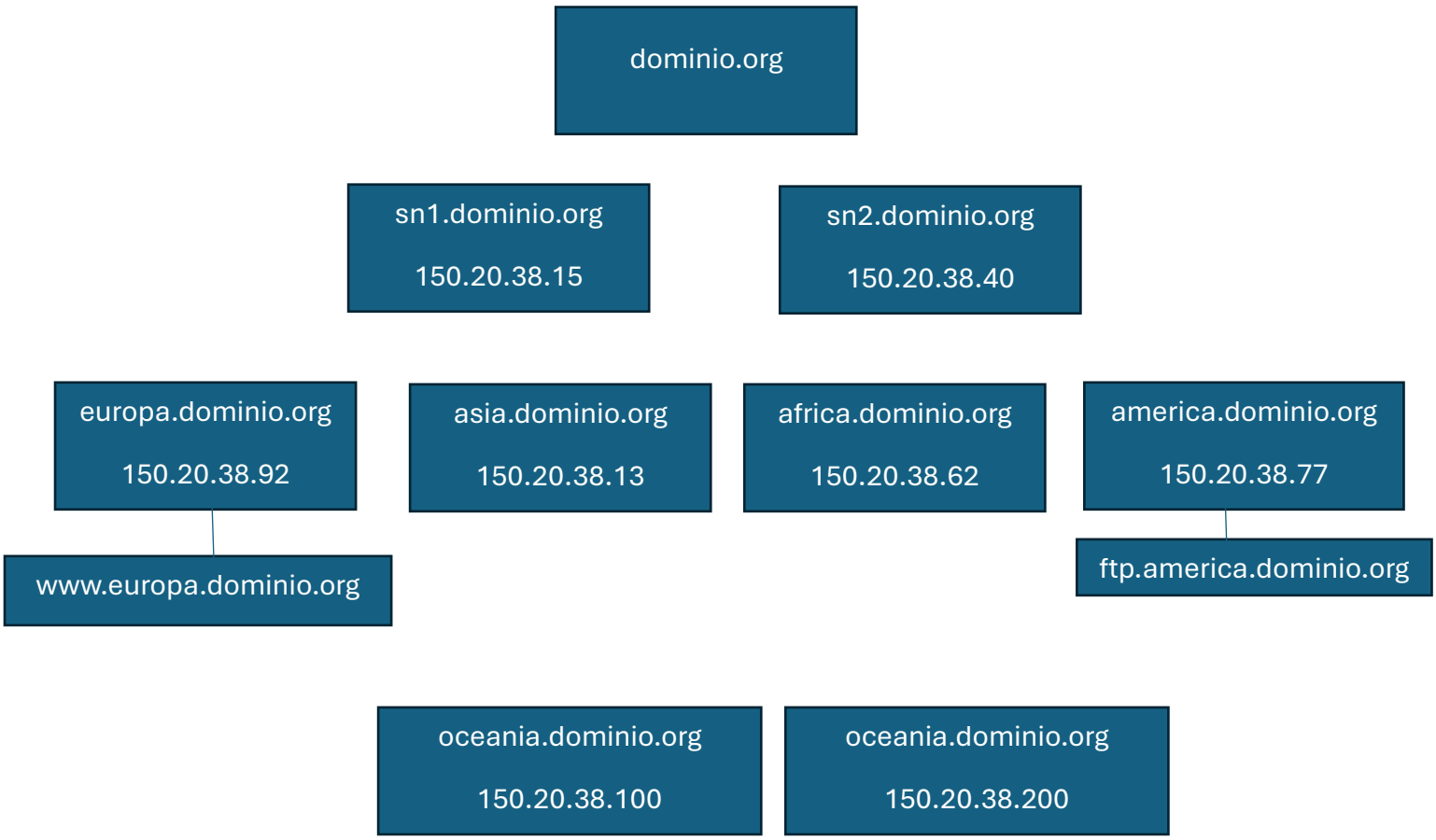
jupiter IN A 100.20.40.18

saturno IN A 100.20.40.55

; Servidor de correo

@ IN MX 10 correo.empresa.es.

11. Dado el siguiente fichero de zona, dibuja un esquema del dominio:



Responde también a las siguientes preguntas:

a) ¿Cada cuánto tiempo comprueba el DNS secundario si ha cambiado el fichero de zona del primario?

Consulta cada 43,200 segundos/12 horas.

b) ¿Cuánto tiempo permanecen los datos en la caché del servidor DNS?

Permanecen en la caché del servidor DNS durante 360,000 segundos, o 100 horas.

c) ¿Cuántos hosts tiene el dominio? ¿Cuántos nombres de host hay? ¿Y cuántas IP?

El dominio tiene 7 host y 7 nombres de host y 7 direcciones IP

12. Usando el comando nslookup, responde a las siguientes cuestiones:

a) ¿Cuál es la IP de www.mec.es?

Servidor: UnKnown

Address: 2a0c:5a80:0:2::1

Respuesta no autoritativa:

Nombre: www.mec.es

Address: 212.128.114.29

b) En el dominio elmundo.es, ¿cuáles son las IP y los nombres de los servidores de nombres del dominio?

```
C:\Users\victo>nslookup -type=NS elmundo.es
Servidor:  UnKnown
Address:  2a0c:5a80:0:2::1

Respuesta no autoritativa:
elmundo.es      nameserver = ns4-02.azure-dns.info
elmundo.es      nameserver = ns1-02.azure-dns.com
elmundo.es      nameserver = ns2-02.azure-dns.net
elmundo.es      nameserver = ns3-02.azure-dns.org

ns1-02.azure-dns.com    AAAA IPv6 address = 2603:1061:0:700::2
ns2-02.azure-dns.net    AAAA IPv6 address = 2620:1ec:8ec:700::2
ns3-02.azure-dns.org    AAAA IPv6 address = 2a01:111:4000:700::2
ns4-02.azure-dns.info   AAAA IPv6 address = 2620:1ec:bda:700::2
ns1-02.azure-dns.com    internet address = 13.107.236.2
ns2-02.azure-dns.net    internet address = 150.171.21.2
ns3-02.azure-dns.org    internet address = 204.14.183.2
ns4-02.azure-dns.info   internet address = 208.84.5.2
```

c) Respecto a los servidores del ejercicio anterior, ¿cuál es el servidor primario y cuáles los secundarios?

d) En el ejercicio anterior has obtenido el SOA del fichero de zona del servidor DNS del dominio elmundo.es preguntándoselo a tu servidor DNS habitual. Ahora has de obtenerlo preguntándoselo también a otro servidor DNS.

e) Si tuviéramos un problema con la resolución de nombres del dominio elmundo.es, ¿a qué dirección de correo electrónico mandaríamos un email informando del problema?

f) ¿Cuál es el nombre y la dirección IP de los servidores de correo de elmundo.es, utilizados cuando enviamos un correo a direcciones del tipo loquesea@elmundo.es?

g) ¿Cuánto tiempo almacena los datos en su caché local el servidor de nombres del dominio elpais.es?

h) ¿Cuándo fue la última vez que se modificó el fichero de zona del dominio elpais.es?

i) ¿Cuántos ordenadores hay como servidores de la web www.elpais.es?

j) ¿Cada cuánto tiempo se comprueba si el servidor de nombres primario de google.com ha modificado su información?

k) Dibuja el mapa del dominio google.com indicando todos sus servidores de correo, sus servidores DNS y los hosts www.google.com y groups.google.com. Indica también las IP para todos los equipos citados.

l) Escribe el contenido del fichero de zona del dominio google.com basándote en el ejercicio anterior.