

DNS (Bind & IOS)

Versión 2022, febrero 2022

Alumno(apellidos,nombre (DNI) : Juan José López Gómez

Alumno(apellidos,nombre (DNI) : Sergio Sánchez García

Fecha: 08/03/022

Duración estimada de la práctica: 2 sesiones de 2h.

1. Entorno de trabajo

- Software de emulación de redes: GNS3 (Analizador de red: wireshark)
- Cisco IOS
- Servidor DNS en Linux virtualizado (DebianAlumno): Bind10
- Órdenes de diagnóstico para interrogar al DNS: dig/host

2. Objetivos

- Aprender a configurar servidores DNS: Bind e IOS
 - Tipos de registros: SOA, NS, A, etc.
- Entender el funcionamiento de los servidores DNS en la jerarquía de servidores:
 - Como resuelven las preguntas (mensajes intercambiados entre los intervenientes (cliente-resolver y los diferentes DNSs de la jerarquía)
 - Como se gestionan las cachés

3. Escenario de trabajo

Para la realización de los siguientes ejercicios se trabajará sobre un escenario prediseñado en GNS3 llamado dns.zip. Descomprimir este fichero en el directorio GNS3/projects de tu unidad Z. Se generará un directorio llamado *dns* con los archivos del escenario. Abrirlo con GNS3 y se mostrará lo siguiente.

Árbol de dominios: El escenario de red definido en *dns* está formado por 4 routers y 9 equipos (ver Figura 1). Representan la jerarquía de servidores DNS de Internet existentes entre los dominios usal.es y cisco.com:

- Dominio **raíz** donde se encuentra la máquina *dnsraiz*.
- Dominio **.es** donde se encuentran los routers *r1* y *r2* y los equipos *dnses* y *pces*. Por lo tanto, sus nombres completos son *r1.es*, *r2.es*, *dnses.es* y *pces.es* respectivamente.
- Dominio **usal.es** donde se encuentran las máquinas *dnsusal*, *portal* y *roble*. Por lo tanto, sus nombres completos son *dnsusal.usal.es*, *portal.usal.es* (también www.usal.es) y *roble.usal.es* (también *diaweb.usal.es*) respectivamente.

- Dominio **.com** donde se encuentran los routers *r3* y *r4* y el equipo *dnscom*. Por lo tanto, sus nombres completos son *r3.com*, *r4.com* y *dnscom.com* respectivamente.
- Dominio **cisco.com** donde se encuentran los equipos *www1* y *www2*. El router *r4* o *dnscisco* actuará como DNS de este dominio. Por lo tanto, sus nombres completos son *r4.cisco.com* (*dnscisco.cisco.com*), *www1.cisco.com*, *www2.cisco.com* (ambos denominados *www.cisco.com*) respectivamente.

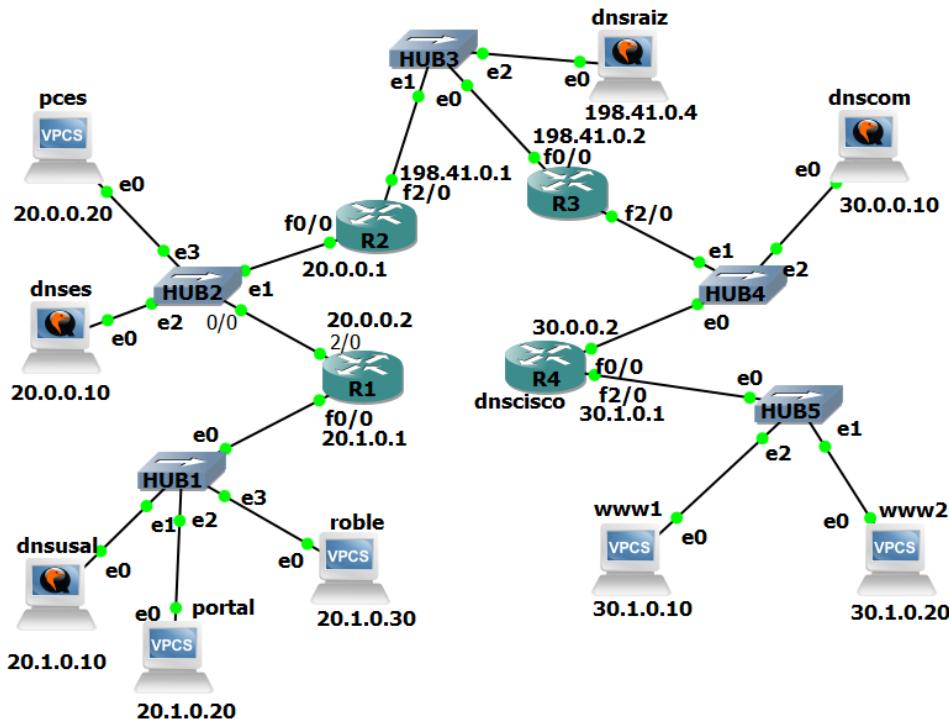


Figura 1: Escenario DNS

Todos los equipos están ya configurados excepto el DNS del router *r4* (o *dnscisco*) que será el responsable del dominio *cisco.com*.

4. El servidor DNS

Servidores DNS. Como servidor de DNS en los equipos Debian utilizaremos *bind9*. En las máquinas virtualizadas con QEmu (denominadas por defecto como Debian-X) ya se dispone de un servidor DNS instalado, pero en caso de necesitar instalarlo en un entorno diferente, la orden para Debian es:

```
apt-get install bind9
```

Los equipos denominados Debian en GNS3 virtualizan la máquina “Debian Alumno” siendo su usuario y clave las ya conocidas root/labii.

Arranca las máquinas del escenario de una en una (esta operación puede tardar unos minutos). Accede a su consola desde la interfaz de GNS3.

Los ficheros de configuración se encuentran en la ruta */etc/bind*. En los siguientes equipos se ha configurado *bind9* para que funcione como servidor de DNS como sigue:

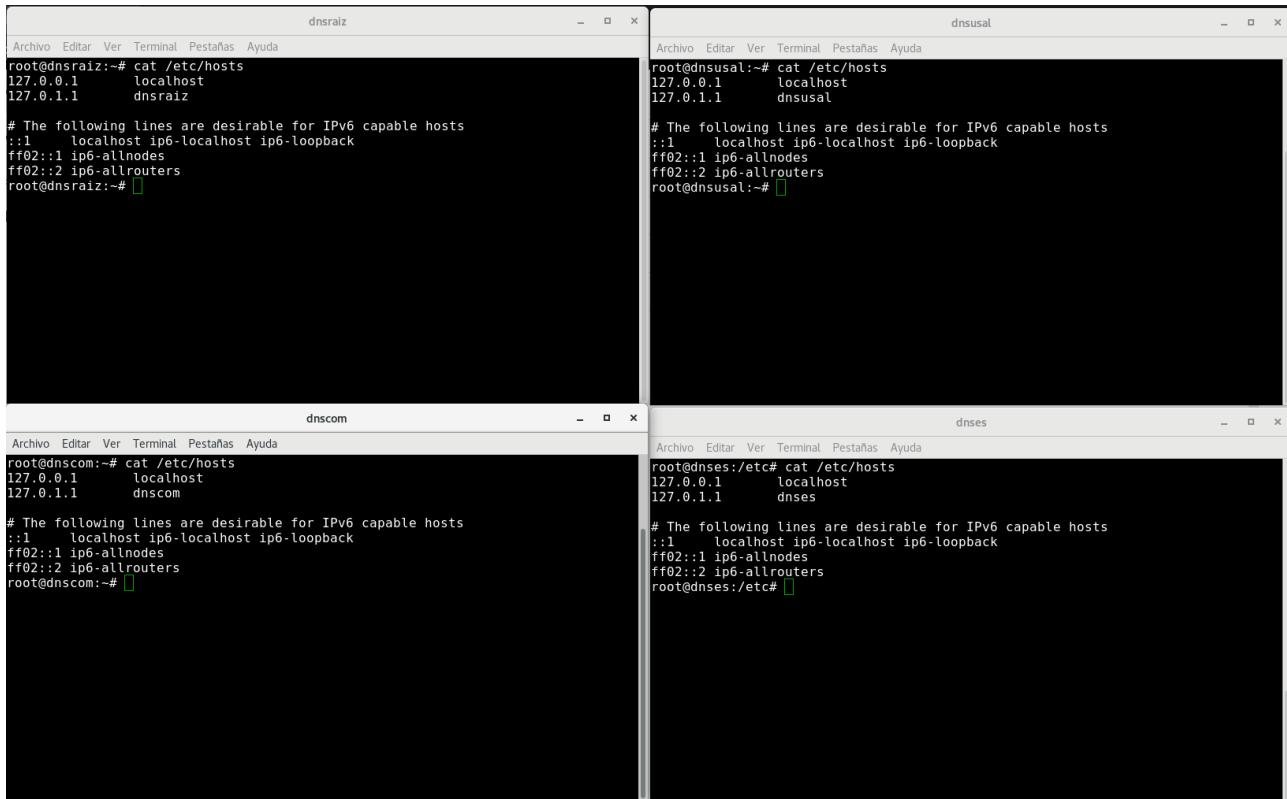
- **dnsraiz:** Servidor de nombres raíz (archivos */bind/named.conf.options*, */bind/named.conf.local*, */bind/db.root*, */bind/db.raiz* y */bind/db.0.41.198*).
- **dnscom:** Servidor de nombres del dominio com (archivos */bind/named.conf.options*, */bind/named.conf.local*, */bind/db.root*, */bind/db.com*, */bind/db.0.30* y */bind/db.1.30*).

- **dnses:** Servidor de nombres del dominio es (archivos `/bind/named.conf.options`, `/bind/named.conf.local`, `/bind/db.root`, `/bind/db.es`, `/bind/db.0.20` y `/bind/db.20`).
- **dnsusal:** Servidor de nombres del dominio usal.es (archivos `/bind/named.conf.options`, `/bind/named.conf.local`, `/bind/db.root`, `/bind/db.es.usal`, `/bind/db.0.1.20`, `/bind/db.0.2.20`).

Configuración de la resolución de nombres en los equipos: Todos los equipos del escenario, si necesitan una operación de resolución de nombres, primero consultarán su fichero local `/etc/hosts` y si no encuentran la respuesta, consultarán a su servidor de DNS.

- Revisa el fichero `resolv.conf` de los equipos Debian () e incluye en el informe el servidor DNS asignado.

Primeramente hemos iniciado sesión en cada uno de los terminales debian que existen en el escenario proporcionado y hemos mostrado el contenido del fichero `/etc/hosts` en el que se muestra las entradas de resolución de nombres que tiene ese terminal, se puede observar que tiene la entrada de localhost asignado a la IP 127.0.0.1 y en la IP local 127.0.1.1 está asignado el nombre que tiene la máquina.



```

dnsraiz                               dnsusal
Archivo Editar Ver Terminal Pestañas Ayuda
root@dnsraiz:~# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      dnsraiz

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
root@dnsraiz:~# 

dnsusal                               dnses
Archivo Editar Ver Terminal Pestañas Ayuda
root@dnsusal:~# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      dnsusal

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
root@dnsusal:~# 

dnscom                                dnses
Archivo Editar Ver Terminal Pestañas Ayuda
root@dnscom:~# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      dnscom

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
root@dnscom:~# 

dnses                                 dnses
Archivo Editar Ver Terminal Pestañas Ayuda
root@dnses:/etc# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      dnses

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
root@dnses:/etc# 

```

Resolviendo ya la pregunta planteada haciendo un `cat` del fichero `resolv.conf` que se encuentra en la ruta `/etc/resolv.conf`, esto tiene sentido ya que en este escenario cada terminal debian está configurado como un servidor de DNS que será responsable de una zona de dominio distinta. Una vez mostrado el contenido de ese fichero salen dos entradas por pantalla Domain y NameServer.

Domain: muestra el dominio del que es responsable este terminal

DNSraíz → “.”, DNSUsal → “usal.es”,
 DNScom → “com”, DNSes → “es”

NameServer: muestra la dirección a la que se tiene que hacer la consulta de DNS, en este caso todas son direcciones loopback ya que ellos mismos son servidores DNS.

The image shows four terminal windows side-by-side, each displaying the configuration of a DNS server (dnsmasq) on a Debian system. The terminals are arranged in a 2x2 grid.

- Top Left Terminal:** Shows the configuration of dnsmasq on the 'dnsraiz' interface. It includes a hosts file entry for 'localhost' and a resolv.conf entry pointing to 'dnscom'. The command 'cat /etc/hosts' is shown at the bottom.
- Top Right Terminal:** Shows the configuration of dnsmasq on the 'dnsusual' interface. It includes a hosts file entry for 'localhost' and a resolv.conf entry pointing to 'dnscom'. The command 'cat /etc/hosts' is shown at the bottom.
- Bottom Left Terminal:** Shows the configuration of dnsmasq on the 'dnscom' interface. It includes a hosts file entry for 'localhost' and a resolv.conf entry pointing to 'dnscom'. The command 'cat /etc/hosts' is shown at the bottom.
- Bottom Right Terminal:** Shows the configuration of dnsmasq on the 'dnses' interface. It includes a hosts file entry for 'localhost' and a resolv.conf entry pointing to 'dnscom'. The command 'cat /etc/hosts' is shown at the bottom.

In all terminals, the output of 'cat /etc/hosts' shows the following entries:

```
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

The resolv.conf outputs show the following entries:

```
domain com
nameserver 127.0.0.1
root@dnsraiz:~#
```

```
ultimo inicio de sesion:jue feb 24 20:45:37 CET 2022en ttyS0
Linux dnsusual 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@dnsraiz:~# cat /etc/resolv.conf
domain
nameserver 127.0.0.1
root@dnsraiz:~#
```

```
ultimo inicio de sesion:jue feb 24 19:16:33 CET 2022en ttyS0
Linux dnsusual 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@dnsraiz:~# cat /etc/resolv.conf
domain
nameserver 127.0.0.1
root@dnsraiz:~#
```

```
ultimo inicio de sesion:jue feb 24 18:37:13 CET 2022en ttyS0
Linux dnscom 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@dnscom:~# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      dnscom

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
root@dnscom:~# cat /etc/resolv.conf
domain com
nameserver 127.0.0.1
root@dnscom:~#
```

```
ultimo inicio de sesion:jue feb 24 20:45:37 CET 2022en ttyS0
Linux dnsusual 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@dnsusual:~# cat /etc/host
cat: /etc/host: No existe el fichero o el directorio
root@dnsusual:~# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      dnsusual

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
root@dnsusual:~# cat /etc/resolv.conf
domain es
nameserver 127.0.0.1
root@dnsusual:~#
```

```
ultimo inicio de sesion:jue feb 24 20:45:37 CET 2022en ttyS0
Linux dnses 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@dnses:~# cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      dnses

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
root@dnses:~# cat /etc/resolv.conf
domain es
nameserver 127.0.0.1
root@dnses:~#
```

- b) Consulta en los routers esta misma información. ¿Qué orden has utilizado?

Para poder consultar esta información primeramente tenemos que acceder a la consola de comandos de los routers, y al igual que en la herramienta CISCO PACKET TRACER poner la orden *enable* para poder acceder a la “pantalla interactiva” del router.

Una vez realizado estos pasos utilizamos la orden `show ip name-server` la cual nos va a proporcionar las direcciones IP de los servidores DNS a los que está asociado.

R1 → DNSes (20.0.0.10) y DNSusal (20.1.0.10)

R2 → DNSraíz (198.41.0.4) y DNSes (20.0.0.10)

R3 → DNSraíz (198.41.0.4), DNScom (30.0.0.10) y DNScisco (30.0.0.2)

R4 → Dirección broadcast (255.255.255.255) esto se debe a que el servidor DNS de este router no está configurado todavía

- c) Consulta en los VPCS esta misma información. ¿Qué orden has utilizado?

Para ver la configuración de los equipos hemos utilizado la orden *show ip* que muestra todo lo que nos interesa que en este caso es consultar el DNS predeterminado que tienen asociado.

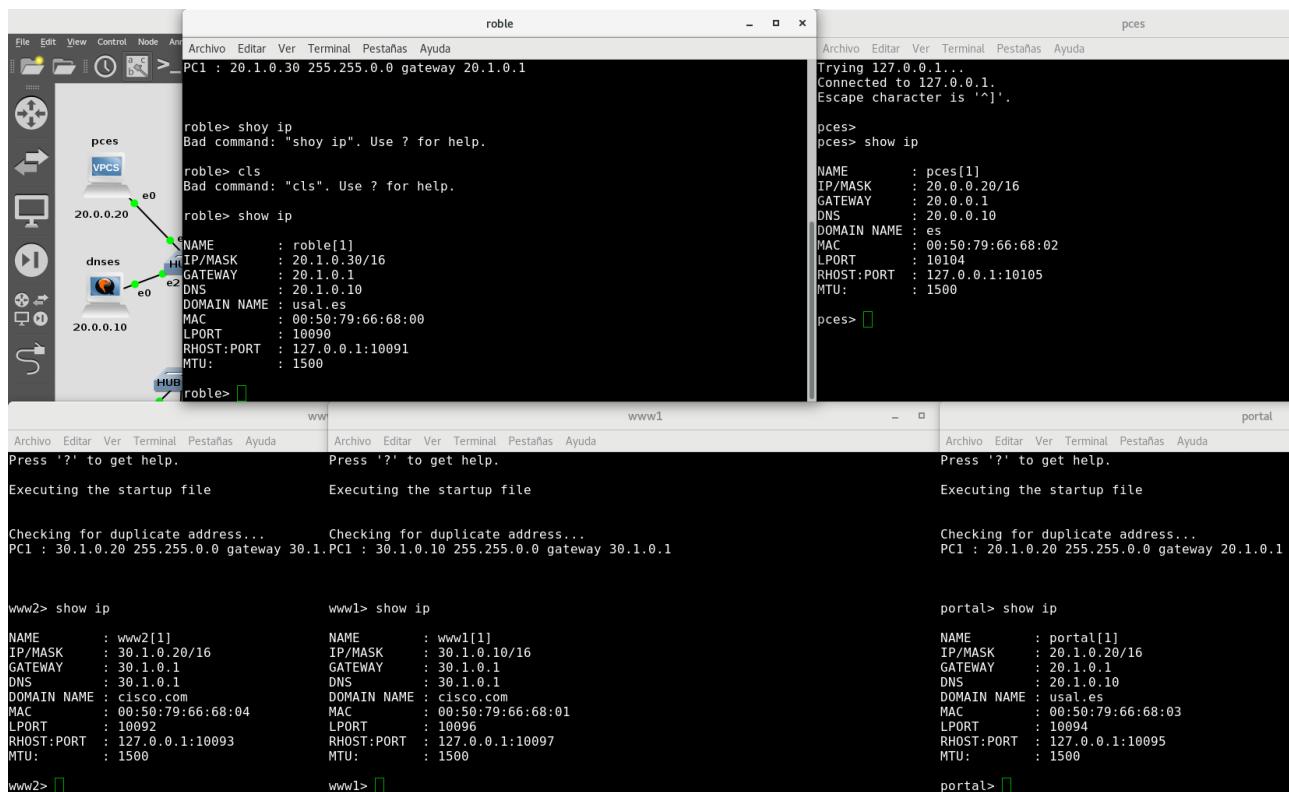
Roble → 20.1.0.10 (DNSusal) responsable del dominio usal.es

Pces → 20.0.0.10 (DNSes) responsable del dominio es

www1 → 30.1.0.1 (DNScom) responsable del dominio cisco.com

www2 → 30.1.0.1 (DNScom) responsable del dominio cisco.com

Portal → 20.1.0.10 (DNSusal) responsable del dominio usal.es



Revisión del escenario configurado

- d) Revisa y comenta brevemente los ficheros de configuración de todos los servidores de DNS del escenario (dnsraiz, dnscom, dnses y dnsusal). Solo hacer uno

Los ficheros de configuración de los servidores DNS se encuentran en la ruta /etc/bind.

Vamos a explicar cada uno de los ficheros que se encuentran en esa ruta para el servidor DNS dnses ya que de esta forma podremos ver cómo se enlaza con el servidor raíz y como delega en el servidor dnsusal.

Esta es la captura con los archivos:

```
i0961594@sundia04: ~
root@dnsses:/# cd /etc/bind
root@dnsses:/etc/bind# ls -l
total 80
-rw-r--r-- 1 root root 2761 oct 25 13:42 bind.keys
-rw-r--r-- 1 root root 237 ene 11 2017 db.0
-rw-r--r-- 1 root bind 695 feb 24 19:58 db.0.20
-rw-r--r-- 1 root root 271 ene 11 2017 db.127
-rw-r--r-- 1 root bind 563 feb 24 19:57 db.20
-rw-r--r-- 1 root root 237 ene 11 2017 db.255
-rw-r--r-- 1 root root 353 ene 11 2017 db.empty
-rw-r--r-- 1 root bind 955 feb 24 19:57 db.es
-rw-r--r-- 1 root root 270 ene 11 2017 db.local
-rw-r--r-- 1 root root 701 feb 24 18:59 db.root
-rw-r--r-- 1 root bind 3171 feb 24 18:56 db.root.original
-rw-r--r-- 1 root bind 463 ene 11 2017 named.conf
-rw-r--r-- 1 root bind 498 oct 25 13:42 named.conf.default-zones
-rw-r--r-- 1 root bind 400 feb 24 19:00 named.conf.local
-rw-r--r-- 1 root bind 165 feb 24 18:56 named.conf.local.original
-rw-r--r-- 1 root root 934 feb 24 19:02 named.conf.options
-rw-r--r-- 1 root bind 890 feb 13 2017 named.conf.options.dpkg-old
-rw-r--r-- 1 root bind 846 feb 24 18:56 named.conf.options.original
-rw-r----- 1 bind bind 77 feb 13 2017 rndc.key
-rw-r--r-- 1 root root 1317 ene 11 2017 zones.rfc1918
root@dnsses:/etc/bind#
```

```
i0961594@lvdia01: ~
GNU nano 3.2 bind.keys
[ 50 líneas leídas ]
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt^J Justificar^C Posición
^X Salir ^R Leer fich.^L Reemplazar^U Pegar txt ^T Ortografía^I Ir a línea
```

- bind.keys → archivo usado para hacer override al DNSSEC.

```
i0961594@lvdia01: ~
GNU nano 3.2 db.0
;
; BIND reverse data file for broadcast zone
;
$TTL    604800
@      IN      SOA     localhost. root.localhost. (
                      1           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )    ; Negative Cache TTL
;
@      IN      NS      localhost.
```

- db.0 → fichero mapa de dominio de resolución inversa para broadcast con dos registros, uno de tipo SOA y otro NS.

```
i0961594@lvdia01: ~
GNU nano 3.2 db.0.20
$TTL 1h ; ttl de permanencia en las cachEs
@      IN      SOA     dnses.es.      root.dnses.es. (
                      20220101 ; Numero de serie
                      28800    ; Refresco despues de 8 horas
                      7200     ; Reintentos despues de 2 horas
                     604800   ; Expiracion despues de 1 semana
                      1h       ; ttl de las respuestas negativas
)
;
; Configuracion de los servidores de nombres
      IN      NS      dnses.es.

; Configuracion de las maquinas
10.0      IN      PTR     dnses.es.
1.0       IN      PTR     r2.es.
2.0       IN      PTR     r1.es.
20.0      IN      PTR     pces.es.
```

- db.0.20 → fichero mapa de dominio con un registro de tipo SOA y otro NS para el servidor dnses.es. También varios PTR, utilizados para la resolución inversa de nombres de R2, R1 y pces. También se establece el TTL a una hora.

```
i0961594@lvdia01: ~
GNU nano 3.2 db.127
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@      IN      SOA     localhost. root.localhost. (
                      1           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )    ; Negative Cache TTL
;
@      IN      NS      localhost.
1.0.0   IN      PTR     localhost.
```

- db.127 → fichero mapa de dominio para la resolución inversa de .es. Cabe destacar el registro de tipo PTR para la resolución de nombres a partir de IPs.

```
i0961594@lvdia01: ~
GNU nano 3.2                               db.20
$TTL 1h ; ttl de permanencia en las cachEs
@      IN      SOA    dnses.es.      root.dnses.es. (
                      20220101 ; Numero de serie
                      28800   ; Refresco despues de 8 horas
                      7200    ; Reintentos despues de 2 horas
                      604800  ; Expiracion despues de 1 semana
                      1h       ; ttl de las respuestas negativas
)
; Configuracion de los servidores de nombres
      IN      NS      dnses.es.
1.20.in-addr.arpa.    IN NS dnsusal.usal.es.
```

- db.20 → fichero mapa de dominio para la resolución del servidor de nombres dnsusal que lo encamina a la subred 20.1.0.0. Se asigna una hora de TTL.

```
i0961594@lvdia01: ~
GNU nano 3.2                               db.255
;
; BIND reverse data file for broadcast zone
;
$TTL    604800
@      IN      SOA    localhost. root.localhost. (
                      1           ; Serial
                      604800     ; Refresh
                      86400      ; Retry
                      2419200   ; Expire
                      604800 )   ; Negative Cache TTL
;
@      IN      NS      localhost.
```

- db.255 → fichero mapa de dominio para la resolución inversa para broadcast con el mismo contenido que db.0.

```
i0961594@lvdia01: ~
GNU nano 3.2                               db.empty
;
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    86400
@      IN      SOA    localhost. root.localhost. (
                      1           ; Serial
                      604800     ; Refresh
                      86400      ; Retry
                      2419200   ; Expire
                      86400 )   ; Negative Cache TTL
;
@      IN      NS      localhost.
```

- db.empty → fichero usado como plantilla para la configuración del resto de ficheros db.

```
i0961594@lvdia01: ~                               dnses
GNU nano 3.2                                     db.es
$TTL 1h ; ttl de permanencia en las cachEs
@      IN      SOA      dnses.es.      root.dnses.es. (
                           20220101      ; Numero de serie
                           28800       ; Refresco despues de 8 horas
                           7200        ; Reintentos despues de 2 horas
                           604800      ; Expiracion despues de 1 semana
                           1h          ; ttl de las respuestas negativas
                           )

; Configuracion de los servidores de nombres del dominio es
      IN      NS      dnses.es.
dnses  IN      A       20.0.0.10

; Configuracion de los equipos
r2     IN      A       20.0.0.1
r1     IN      A       20.0.0.2
pces   IN      A       20.0.0.20

; Servidores de nombres del dominio usal.es
GNU nano 3.2                                     /etc/bind/db.es
      IN      NS      dnses.es.
dnses  IN      A       20.0.0.10

; Configuracion de los equipos
r2     IN      A       20.0.0.1
r1     IN      A       20.0.0.2
pces   IN      A       20.0.0.20

; Servidores de nombres del dominio usal.es
usal.es.           IN      NS      dnsusal.usal.es.
dnsusal.usal.es.  IN      A       20.1.0.10

; Para la resolucion inversa
1.20.in-addr.arpa. IN      NS      dnsusal.usal.es.

[ 24 líneas leídas ]
```

- db.es → encontramos un registro de tipo SOA y clase IN (Internet) para el servidor dnses.es. Después, tenemos un registro de tipo NS y otro de tipo A para configurar el servidor dnses. Por último encontramos tres registros de tipo A correspondientes a los equipos pces, f0/0 de R2 y f2/0 de R1.

```
i0961594@lvdia01: ~                               dnses
GNU nano 3.2                                     db.local
;
; BIND data file for local loopback interface
;
$TTL    604800
@      IN      SOA      localhost. root.localhost. (
                           2          ; Serial
                           604800     ; Refresh
                           86400      ; Retry
                           2419200    ; Expire
                           604800 )   ; Negative Cache TTL
;
@      IN      NS      localhost.
@      IN      A       127.0.0.1
@      IN      AAAA    ::1
```

- db.local → este fichero de zona permite resolver el nombre localhost a la dirección de loopback 127.0.0.1. Encontramos un registro de tipo A para IPv4 y otro de tipo AAAA para IPv6..

```
i0961594@lvdia01: ~                               ×      dnses
GNU nano 3.2          db.root
;
; This file holds the information on root name servers needed to
; initialize cache of Internet domain name servers
; (e.g. reference this file in the "cache . <file>" configuration
; file of BIND domain name servers).
;
; This file is made available by InterNIC
; under anonymous FTP as
;     file          /domain/named.cache
;     on server      FTP.INTERNIC.NET
; -OR-
;     file          /domain/named.cache
;     on server      RS.INTERNIC.NET
;
; last update:    February 17, 2016
; related version of root zone:   2016021701
;
; formerly NS.INTERNIC.NET
;
.           3600000      NS    dnsraiz.
dnsraiz.  3600000      A     198.41.0.4
; End of file
```

- db.root → fichero de zona que contiene la información de los servidores raíz para inicializar la caché de los DNSs. Cuando el bind se carga consulta este fichero para obtener los servidores raíz autoritarios. El NS indica quien es el servidor DNS para el dominio raíz, el punto. El registro A enlaza el nombre dnsraiz. con la IP 198.41.0.4.

```
i0961594@lvdia01: ~                               dnses
GNU nano 3.2          db.root.original

; This file holds the information on root name servers needed to
; initialize cache of Internet domain name servers
; (e.g. reference this file in the "cache . <file>" configuration
; file of BIND domain name servers).

; This file is made available by InterNIC
; under anonymous FTP as
;     file          /domain/named.cache
;     on server    FTP.INTERNIC.NET
; -OR-
;           RS.INTERNIC.NET
;
; last update: February 17, 2016
; related version of root zone: 2016021701

; formerly NS.INTERNIC.NET
;

.          3600000      NS   A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000      A    198.41.0.4
A.ROOT-SERVERS.NET. 3600000      AAAA 2001:503:ba3e::2:30
```

```
i0961594@lvdia01: ~                               dnses
GNU nano 3.2          db.root.original

.          3600000      NS   E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET. 3600000      A    192.203.230.10
;
; FORMERLY NS.ISC.ORG
;
.          3600000      NS   F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET. 3600000      A    192.5.5.241
F.ROOT-SERVERS.NET. 3600000      AAAA 2001:500:2f::f
;
; FORMERLY NS.NIC.DDN.MIL
;
.          3600000      NS   G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET. 3600000      A    192.112.36.4
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.          3600000      NS   H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET. 3600000      A    198.97.190.53
H.ROOT-SERVERS.NET. 3600000      AAAA 2001:500:1::53
```

```
i0961594@lvdia01: ~ x dnses
GNU nano 3.2 db.root.original

; FORMERLY NIC.NORDU.NET
;
. 3600000 NS I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET. 3600000 A 192.36.148.17
I.ROOT-SERVERS.NET. 3600000 AAAA 2001:7fe::53
;
; OPERATED BY VERISIGN, INC.
;
. 3600000 NS J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET. 3600000 A 192.58.128.30
J.ROOT-SERVERS.NET. 3600000 AAAA 2001:503:c27::2:30
;
; OPERATED BY RIPE NCC
;
. 3600000 NS K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET. 3600000 A 193.0.14.129
K.ROOT-SERVERS.NET. 3600000 AAAA 2001:7fd::1
;
; OPERATED BY ICANN

i0961594@lvdia01: ~ x dnses
GNU nano 3.2 db.root.original

. 3600000 NS L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET. 3600000 A 199.7.83.42
L.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:3::42
;
; OPERATED BY WIDE
;
. 3600000 NS M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET. 3600000 A 202.12.27.33
M.ROOT-SERVERS.NET. 3600000 AAAA 2001:dc3::35
; End of file
```

- db.root.original

```
i0961594@lvdia01: ~ x dnses
GNU nano 3.2 named.conf

// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

- named.conf → en este fichero se almacena una colección de declaraciones de tipo include que incluye los archivos que se ven en la imagen, de esta forma se colocan los datos de configuración confidenciales en diversos archivos con distintos permisos. El proceso named

escucha en el puerto 53 y cuando recibe una petición de dirección busca en este archivo. No debe tener errores para un correcto arranque del demonio named.

```
i0961594@lvdia01: ~
GNU nano 3.2          named.conf.default-zones
// prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/usr/share/dns/root.hints";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};
```

```
i0961594@lvdia01: ~
GNU nano 3.2          named.conf.default-zones
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
```

```
i0961594@lvdia01: ~
GNU nano 3.2          named.conf.default-zones
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
```

- named.conf.default-zones → encontramos las zonas, que sirven para ver a qué IP pertenece un nombre de dominio, y también tenemos las zonas inversas que permiten lo contrario.
 - zone “.” es de tipo hint y enlaza con /etc/bind/root que almacena los nombres y direcciones de servers root.
 - zone “localhost” es de tipo master, por lo que el servidor es autoritario sobre la zona, y permite reducir el tráfico.
 - zone “XXX.in-addr.arpa” son zonas inversas.

```
i0961594@lvdia01: ~                               dnses
GNU nano 3.2          named.conf.local

// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "es" {
    type master;
    file "/etc/bind/db.es";
};

zone "20.in-addr.arpa" {
    type master;
    file "/etc/bind/db.20";
};

zone "0.20.in-addr.arpa" {
    type master;
}

i0961594@lvdia01: ~                               dnses
GNU nano 3.2          named.conf.local

};

zone "20.in-addr.arpa" {
    type master;
    file "/etc/bind/db.20";
};

zone "0.20.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0.20";
};
```

- named.conf.local → contiene las zonas locales que podrá resolver el servidor DNS. Encontramos la zona para la resolución de “.es” para obtener su IP dado su nombre y dos zonas para resolución inversa “20” y “0.20”.

```
i0961594@lvdia01: ~
GNU nano 3.2          named.conf.local.original
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

- `named.conf.local.original` → fichero para configuraciones locales, como se puede observar en este caso no hay ninguna.

```
i0961594@lvdia01: ~
GNU nano 3.2          named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
```

```
i0961594@lvdia01: ~
GNU nano 3.2          named.conf.options
        // the all-0's placeholder.

        // forwarders {
        //     0.0.0.0;
        // };

        //=====
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys. See https://www.isc.org/bind-keys
        //=====
        // dnssec-validation auto;   I
        dnssec-enable no;
        dnssec-validation no;
        auth-nxdomain no;      # conform to RFC1035
        listen-on-v6 { any; };
};
```

- `named.conf.options` → en este fichero se define el directorio por defecto `/var/cache/bind`, se desactiva el DNSSEC y la validación.

El DNSSEC sirve para añadir mayor seguridad a los servidores DNS del dominio.

```
i0961594@lvdia01: ~
GNU nano 3.2          named.conf.options.dpkg-old
dnses

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
}

i0961594@lvdia01: ~
GNU nano 3.2          named.conf.options.dpkg-old
dnses

// the all-0's placeholder.

// forwarders {
//     0.0.0.0;
// };

//=====
// If BIND logs error messages about the root key being expired,
// you will need to update your keys. See https://www.isc.org/bind-keys
//=====
dnssec-validation auto;

auth-nxdomain no;      # conform to RFC1035
listen-on-v6 { any; };
};
```

- `named.conf.options.dpkg-old` → fichero de configuración en el que se define al directorio `/var/cache/bind` como directorio por defecto y se pone a modo auto la validación del DNSSEC.

```
i0961594@lvdia01: ~
GNU nano 3.2          named.conf.options.original
dnses

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
};

i0961594@lvdia01: ~
GNU nano 3.2          named.conf.options.original
dnses

// the all-0's placeholder.

// forwarders {
//     0.0.0.0;
// };

//=====
// If BIND logs error messages about the root key being expired,
// you will need to update your keys. See https://www.isc.org/bind-keys
//=====
dnssec-validation auto;

listen-on-v6 { any; };

};
```

- `named.conf.options.original` → fichero de configuración en el que se define al directorio `/var/cache/bind` como directorio por defecto y se pone a modo auto la validación del DNSSEC.

```
i0961594@lvdia01: ~
GNU nano 3.2          rndc.key
dnses

key "rndc-key" {
    algorithm hmac-md5;
    secret "g6F7XVJuxdF39NsILp0/Dg==";
};
```

- `rndc.key` → declaración para la key con nombre `rndc.key` en el que el valor `secret` usa el algoritmo `hmac.md5` para generar las llaves. Este fichero se usa para añadir seguridad y no tener declarada la key en `/etc/named.conf` ya que solo el root tendrá acceso a este.

```
i0961594@lvdia01: ~          dnses
GNU nano 3.2      zones.rfc1918

zone "10.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "16.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "17.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "18.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "19.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "20.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "21.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "22.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "23.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "24.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "25.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "26.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "27.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "28.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "29.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "30.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "31.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; }
```

```
i0961594@lvdia01: ~          dnses
GNU nano 3.2      zones.rfc1918

zone "24.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "25.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "26.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "27.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "28.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "29.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "30.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };
zone "31.172.in-addr.arpa" { type master; file "/etc/bind/db.empty"; };

zone "168.192.in-addr.arpa" { type master; file "/etc/bind/db.empty"; }
```

- zones.rfc1918 → incluye las zonas vacías que debe servir para los otros rangos.

Resolución de nombres: Por medio de las órdenes para preguntar al DNS host y *dig*, así como de *wireshark*, realiza los siguientes apartados.

5. Servidor DNS en IOS

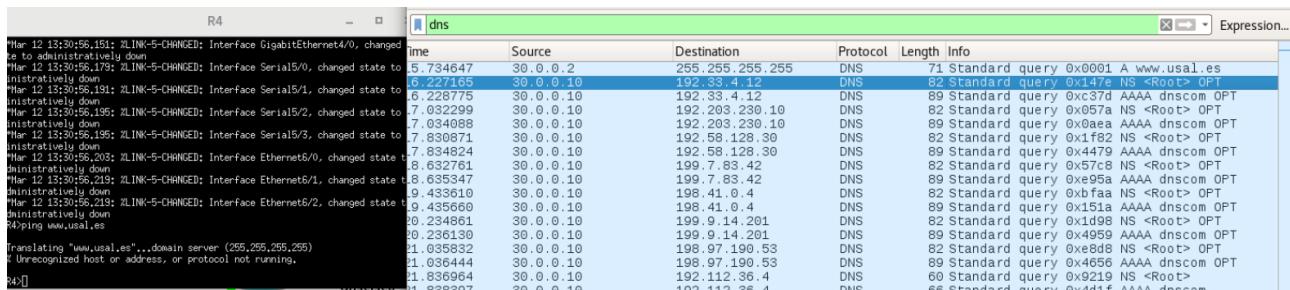
En los siguientes apartados podremos comprobar si los routers de Cisco habilitan o no un servidor DNS, configurar R4 como servidor DNS del dominio cisco.com y verificar su funcionamiento.

5.1. ¿Los routers son servidores DNS caché?

Los siguientes pasos permitirán observar si los routers de Cisco habilitan o no un servidor DNS caché.

- En el router R4 realiza un ping a www.usal.es. Captura el tráfico en sus dos interfaces para responder a las preguntas: ¿Qué ha ocurrido? ¿por qué? Incluye en el informe el tráfico implicado.

Para realizar el ping tenemos que acceder a la consola de comandos del router y utilizar la orden *ping www.usal.es*, previamente iniciamos el analizador de red wireshark en la interfaz 0/0 del router para poder capturar todo el tráfico que se genere por esa interfaz.

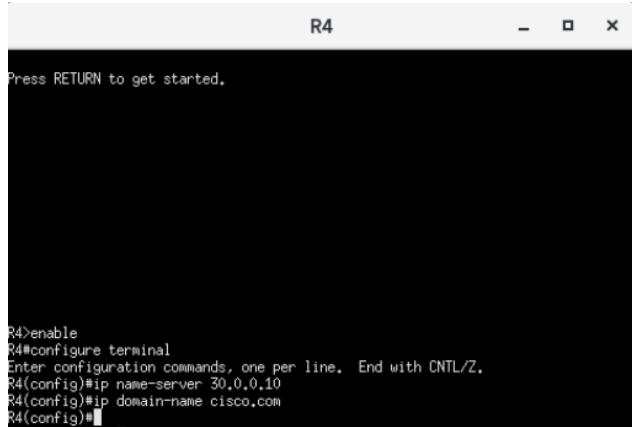


Cuando ejecutamos la orden el analizador empieza a capturar todo el tráfico, como ahora mismo solo nos interesa el tráfico DNS hemos filtrado solo por las tramas de este protocolo.

La primera que se observa es un DNS con dirección de destino al broadcast, esto ocurre cuando un terminal, en este caso el router R4 no tiene configurado ningún servidor DNS predeterminado, así que envía la petición por la red para que le llegue a todo el que pueda resolverla la petición, al único servidor que le llega es al DNScom que no tiene autoridad sobre ese campo así que sigue reenviando la trama, hasta que el tiempo de vida se agota y no se es capaz de resolver la petición del router

- Asigna a R4 un servidor de nombre (en nuestro caso dnscom – 30.0.0.10) y el dominio *cisco.com*. Incluye las órdenes utilizadas.

Para configurar al router R4 un servidor DNS se tiene que entrar en la consola del router y habilitar la configuración con *enable* y *configure terminal*, ahora ya estaremos en el modo configuración del router, para asignar la ip del DNS se utiliza *ip name-server <ip del DNS>* y para asignar el nombre del dominio se usa *ip domain-name <nombre de dominio>* con esto se habría configurado correctamente el servidor de DNS predeterminado para el router R4



```
R4
Press RETURN to get started.

R4>enable
R4#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R4(config)#ip name-server 30.0.0.10
R4(config)#ip domain-name cisco.com
R4(config)#[
```

- c) Realiza de nuevo un ping a www.usal.es ¿Qué ha ocurrido? ¿por qué? ¿Hay alguna entrada nueva en la caché de resolución de nombres? ¿Qué orden has utilizado para consultarla? ¿Cuánto tiempo permanecerán en la caché? ¿Dónde se configura este tiempo?

Una vez establecido el servidor DNS predeterminado para el router R4, volvemos a realizar el ping www.usal.es, se observa cómo ya no sale el mensaje de que se redirige a la dirección de broadcast el mensaje de DNS porque al haber configurado el DNS predeterminado ya tiene una ruta por la que preguntar la resolución de nombres. Completando de esta forma el ping.



```
R4>
R4>ping www.usal.es
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.1.0.20, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 68/326/1064 ms
R4>[
```

Para ver las entradas del ARP Caché se utiliza la orden *show hosts*:

```

R4>
R4>
R4>
R4>
R4>ping www.usal.es
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.1.0.20, timeout is 2 seconds:
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 68/326/1064 ms
R4>show hosts
Default domain is cisco.com
Name/address lookup uses domain service
Name servers are 30.0.0.10

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
      temp - temporary, perm - permanent
      NA - Not Applicable None - Not defined

Host          Port  Flags     Age Type  Address(es)
dnsusal.usal.es    None (temp, OK)  0   IP    20.1.0.10
portal.usal.es     None (temp, OK)  0   IP    20.1.0.20
www.usal.es       None (temp, OK)  0   IP    20.1.0.20
R4>

```

En la imagen de arriba se pueden ver como en efecto está configurado correctamente el servidor de nombres, en la parte de hosts aparecen dos entradas:

La primera almacena el responsable del dominio en este caso que es “dnsusal.usal.es”, junto con el estado en que se encuentra la entrada, ambas entradas son temporales y están activas, el tipo de la entrada y la ip a la que se refiere.

La segunda almacena la dirección de la máquina a la que se le está realizando el ping.

El tiempo de permanencia en la caché no es posible verlo desde la interfaz del router ya que no depende de él. Para acceder a este parámetro se tiene que ver en la configuración del servidor DNS responsable de este dominio que en este caso es DNSusal, más concretamente se tiene que obtener este valor desde el registro SOA del mismo, en el campo minimum TTL

5.2. Un router como responsable del dominio *cisco.com*.

Para configurar R4 (o dnscisco) como responsable del dominio cisco.com hemos de seguir los siguientes pasos:

- Habilitar DNS server
 - Añadir los recursos: SOA, NS y A
 - Añadir un balanceo de tráfico para www.cisco.com entre www1 y www2
 - Modificar los ficheros necesarios en dnscom para esta delegación
- a) Incluye las ordenes utilizadas, su ejecución en el router y los ficheros modificados en dnscom.

Para hacer este paso primero tenemos que habilitar la configuración del router con *enable* y *configure terminal*.

Una vez se está en el modo configuración, se utiliza la orden *ip dns server* para poder habilitar el servidor DNS:

```
R4(config)#ip dns server  
R4(config)#[REDACTED]
```

Ahora queda configurar los registros necesarios comenzando con el fichero SOA que es el que va a contener toda la información de la configuración del servidorDNS con la orden:

ip dns primary domain-name soa primary-server-name mailbox-name [refresh-interval [retry-interval[expire-ttl[minimum-ttl]]]];

```
*Mar 14 12:13:34.911: %SYS-5-CONFIG_I: Configured from console by console  
R4>enable  
R4#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R4(config)#ip dns pr  
R4(config)#ip dns primary  
R4(config)#ip dns primary ?  
WORD DNS domain name  
  
R4(config)#$com soa dnscisco.cisco.com root.cisco.com 28800 7200 604800 30  
R4(config)#ip dns primary cisco.com soa dnscisco.cisco.com root.cisco.com 28800$
```

Como nombre del dominio hemos puesto cisco.com a continuación la configuración del soa, lo siguiente es el nombre del servidor que es dnscisco.cisco.com y el mailbox name que no se utilizará pero hay que ponerlo, después hemos configurado los ttl:

Refresh-Interval → 28800 s, significando que cada pase este tiempo el servidor esclavo le va a pedir un refresco de las entradas al predeterminado.

Retry-Interval → 7200 s, el tiempo en el que el servidor esclavo ha de realizar un intento tras una solicitud fallida.

Expire-TTL → 604800 s, el tiempo a partir del cual un esclavo deja de dar información al exterior si el master sigue sin dar respuesta

Minimum-ttl → 30 s, el tiempo durante el cual la información puede ser almacenada en la memoria caché

Para configurar los registros NS y A, se utiliza la orden *ip host*, pero en el caso de que sea un registro NS se tiene que utilizar *ip host <dominio> ns <servidor del dominio>*

```
R4>enable  
R4#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R4(config)#ip host cisco.com ns ?  
WORD Target NS hostname  
  
R4(config)#ip host cisco.com ns dnscisco.cisco.com  
R4(config)#[REDACTED]
```

En la imagen de arriba se está creando el registro NS en el que se indica como primer parámetro el nombre del dominio y como segundo el nombre del servidor asociado a este registro.

```
R4(config)#ip host cisco.com ns dnscisco.cisco.com  
R4(config)#ip host www1.cisco.com 30.1.0.10  
R4(config)#ip host www2.cisco.com 30.1.0.20  
R4(config)#[REDACTED]
```

En la captura anterior estamos configurando los registros A para las dos máquinas del dominio asociando el nombre de la máquina junto con el dominio a la IP que tienen asignada

```
R4(config)#ip host cisco.com ns dnscisco.cisco.com
R4(config)#ip host www1.cisco.com 30.1.0.10
R4(config)#ip host www2.cisco.com 30.1.0.20
R4(config)#ip host www.cisco.com 30.1.0.10 30.1.0.20
R4(config)#[
```

Por último para el balanceo de www.cisco.com hemos añadido el registro A con ese nombre pero en vez de que se resuelva solamente con una IP, le hemos asignado las IPs de www1 y www2.

```
$TTL 2h ; ttl de permanencia en las cachEs
@ IN SOA dnscom.com. root.dnscom.com. (
    20220101 ; Numero de serie
    28800 ; Refresco despues de 8 horas
    7200 ; Reintentos despues de 2 horas
    604800 ; Expiracion despues de 1 semana
    2h ; ttl de las respuestas negativas
)

; Configuracion de los servidores de nombres del dominio com
IN NS dnscom.com.
dnscom IN A 30.0.0.10

dnscisco IN NS cisco.com
dnscisco IN A 30.0.0.2

; Configuracion de los equipos
r3 IN A 30.0.0.1
r4 IN A 30.0.0.2
pccom IN A 30.0.0.20
[ 22 líneas escritas ]
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt^J Justificar^C Posición
^X Salir ^R Leer fich.^V Reemplazar^U Pegar txt ^T Ortografía^_ Ir a línea
```

En el terminal DNScom, en el fichero db.com hemos añadido las referencias al dominio cisco.com, un registro NS para que sepa el nombre del dominio y el registro A para que pueda resolver el dominio indicando la ip del router R4 o dnscisco.

- b) Comprueba tu configuración desde los equipos www1 y www2 resolviendo nombres del dominio .com y usal.es. ¿Qué órdenes has utilizado? Muestra y comenta las salidas obtenidas. Consulta la caché del DNS de R4. ¿Qué orden has utilizado? ¿Justifica las entradas encontradas?

Para poder resolver correctamente hemos hecho dos pings distintos, desde www1 hemos realizado un ping al dominio usal.es mientras que con www2 lo hemos hecho al dominio .com.

En www1 la orden a utilizar es *ping robles.usal.es*

Mientras que en www2 es *ping www1.cisco.com*

```
www1
Press '?' to get help.
Executing the startup file

Checking for duplicate address...
PC1 : 30.1.0.10 255.255.0.0 gateway 30.1.0.1

www1> ping robles.usal.es
Cannot resolve robles.usal.es

www1> ping www1.cisco.com
www1.cisco.com resolved to 20.1.0.30
robles.usal.es icmp seq=1 timeout
robles.usal.es icmp seq=2 timeout
84 bytes from 20.1.0.30 icmp seq=3 ttl=60 time=49.534 ms
84 bytes from 20.1.0.30 icmp seq=4 ttl=60 time=44.542 ms
84 bytes from 20.1.0.30 icmp seq=5 ttl=60 time=44.235 ms

www2> ping www1.cisco.com
www1.cisco.com resolved to 30.1.0.10
84 bytes from 30.1.0.10 icmp seq=1 ttl=64 time=0.084 ms
84 bytes from 30.1.0.10 icmp seq=2 ttl=64 time=0.137 ms
84 bytes from 30.1.0.10 icmp seq=3 ttl=64 time=0.102 ms
84 bytes from 30.1.0.10 icmp seq=4 ttl=64 time=0.123 ms
84 bytes from 30.1.0.10 icmp seq=5 ttl=64 time=0.107 ms

www2>
```

Al realizar el primer ping en ambos casos no se puede resolver porque se sobrepasa el tiempo máximo de espera, ya que al tener que resolver los dominios y los nombres es más lento. Pero una vez ya están cacheados al realizar de nuevo el ping se completa exitosamente.

```

R4>
R4>
R4>
R4>show hosts
Default domain is cisco.com
Name/address lookup uses domain service
Name servers are 30.0.0.10

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
      temp - temporary, perm - permanent
      NA - Not Applicable None - Not defined

Host          Port  Flags    Age Type   Address(es)
dnsusal.usal.es  None  (temp, OK)  0   IP    20.1.0.10
roble.usal.es   None  (temp, OK)  0   IP    20.1.0.30
cisco.com       NA    (perm, OK)  0   NS    dnscisco.cisco.com
                           SOA   dnscisco.com root.cisco.com
                           0   28800 7200 604800 28800
www1.cisco.com  None  (perm, OK)  0   IP    30.1.0.10
www2.cisco.com  None  (perm, OK)  0   IP    30.1.0.20
www.cisco.com   None  (perm, OK)  0   IP    30.1.0.10
                           30.1.0.20

R4>

```

Para ver las tabla de caché del router se utiliza la orden `show hosts` en el R4, en la pantalla se observa como ha cacheado el servidor que provee el dominio usal.es, y también la dirección del máquina roble.usal.es, mientras que para la otra petición no ha tenido que hacer nada ya que es responsable de esa parte del dominio.

6. Entendiendo las consultas a la jerarquía y las cachés

Antes de comenzar este apartado asegurate que las cachés de todos los DNS estén vacías. Puedes borrar la caché de un servidor de DNS reiniciando el servidor con la orden: `service bind9 restart` o bien con las órdenes:

```

rndc flush
rndc reload

```

- a) Desde la máquina *roble* (del dominio usal.es) ejecuta `ping www.cisco.com`. Realiza las capturas del tráfico que consideres necesarias para obtener los mensajes de DNS que se generan entre todas las máquinas del escenario. Explica, apoyándote en las capturas realizadas, el proceso de obtención de respuestas en un sistema de DNS.

Presta especial atención al campo *Recursion desired* que especifica el tipo de pregunta realizada: recursiva (activado) o iterativa (desactivado). Observa también en las capturas realizadas el valor del campo TTL (*Time To Live*) del mensaje de DNS de la respuesta obtenida en *roble* (no confundir con el campo TTL de la cabecera de los datagramas IP). ¿Qué significa este valor y de donde se obtiene? Ten en cuenta que la primera vez que realices el ejercicio todas las cachés de los servidores DNS estarán vacías. Recuerda que, si realizas más de una consulta a un servidor de DNS, éste almacena información en su caché. Para consultarla puedes utilizar las órdenes

```

rndc dumpdb -cache
cat /var/cache/bind/named_dump.db

```

The image shows four terminal windows from a Linux desktop environment. The windows are titled 'dnsraiz', 'dnsusal', 'R4', and 'dnscom'. The 'dnsraiz' and 'dnsusal' windows show the configuration of a DNS server on R4, with commands like 'rndc flush' and 'rndc reload' being run. The 'R4' window shows the output of the 'show hosts' command, listing entries for 'www1.cisco.com', 'www2.cisco.com', and 'www.cisco.com' with their respective IP addresses. The 'dnscom' window shows the configuration of a DNS client on another host, with commands like 'rndc flush' and 'rndc reload' being run.

```

dnsraiz login: root
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Debian GNU/Linux 10 dnsraiz ttyS0
dnssusal login: root
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Debian GNU/Linux 10 dnssusal ttyS0
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@dnsraiz:~# rndc flush
root@dnsraiz:~# rndc reload
server reload successful
root@dnsraiz:~# 

R4
Archivo Editar Ver Terminal Pestañas Ayuda
30.1.0.20
34#rndc flush
^
! Invalid input detected at `^` marker.
34#show hosts
default domain is cisco.com
name/address lookup uses domain service
name servers are 30.0.0.10
codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
      temp - temporary, perm - permanent
      NA - Not Applicable None - Not defined
host          Port Flags   Age Type  Address(es)
cisco.com     MA (perm, OK) 0  NS      dns@cisco.cisco.com
              SOA      dns@cisco.com root.cisco
.com
              0 28800 7200 604800 28800
www1.cisco.com  None (perm, OK) 0  IP    30.1.0.10
www2.cisco.com  None (perm, OK) 0  IP    30.1.0.10
www.cisco.com   None (perm, OK) 0  IP    30.1.0.10
              30.1.0.20

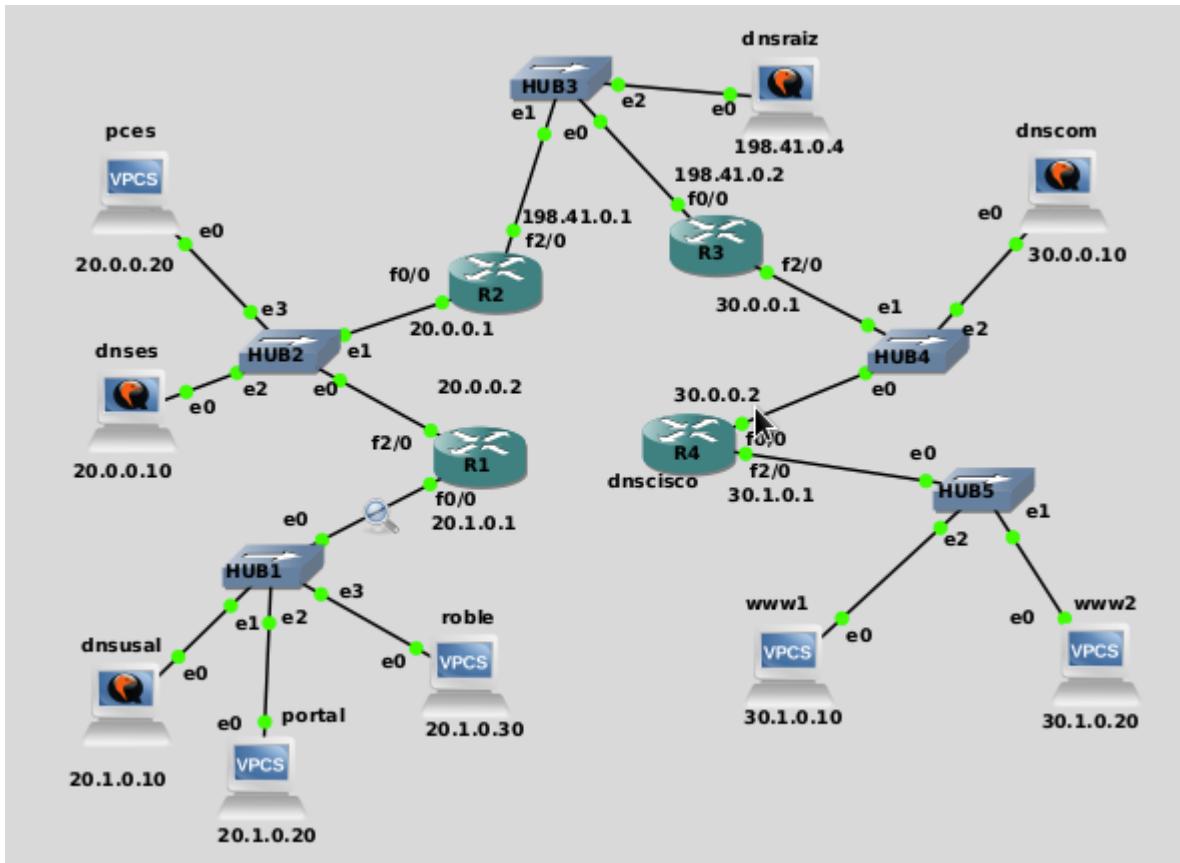
dnscom login: root
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
Debian GNU/Linux 10 dnsses tt
root@dnscom:~# rndc flush
root@dnscom:~# rndc reload
server reload successful
root@dnscom:~# 
dnsses login: root
Contraseña:
Ultimo inicio de sesion:mar mar  8 17:37:52 CET 2022en ttyS0
Linux dnsses 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@dnscom:~# rndc flush
root@dnscom:~# rndc reload
server reload successful
root@dnscom:~# 

```

Para comprobar que los dns están vacíos hemos utilizado en las órdenes dadas para los terminales y la show hosts para el R4

Para observar correctamente las tramas hemos capturado con wireshark en el enlace entre HUB1 y R1:



Hemos elegido este enlace debido a que los HUB van a retransmitir la trama por todas sus interfaces por lo que el punto donde observar no es único, se podría hacer la escucha en otros enlaces.

```
roble
Archivo Editar Ver Terminal Pestañas Ayuda
dnsraiz dnscom dnses dnsusal roble

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC1 : 20.1.0.30 255.255.0.0 gateway 20.1.0.1

roble> ping www.cisco.com
www.cisco.com resolved to 30.1.0.20
www.cisco.com icmp_seq=1 timeout
www.cisco.com icmp_seq=2 timeout
84 bytes from 30.1.0.20 icmp_seq=3 ttl=60 time=67.628 ms
84 bytes from 30.1.0.20 icmp_seq=4 ttl=60 time=43.872 ms
84 bytes from 30.1.0.20 icmp_seq=5 ttl=60 time=59.438 ms

roble>
```

*Standard input [HUB1 Ethernet0 to R1 FastEthernet0/0]

File Edit View Go Capture Analyze Statistics Telephone Wireless Tools Help

dns Expression... +

No.	Time	Source	Destination	Protocol	Length	Info
5	66.720095	20.1.0.30	20.1.0.10	DNS	73	Standard query 0x4cbd A www.cisco.com
6	66.733458	20.1.0.30	20.1.0.10	DNS	73	Standard query 0x4cbd A www.cisco.com
7	66.741990	20.1.0.30	198.44.0.4	DNS	112	Standard query 0x7c7c A www.cisco.com OPT

► Frame 5: 73 bytes on wire (594 bits), 73 bytes captured (594 bits) on interface 0
► Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: ca:01:06:c5:00:00 (ca:01:06:c5:00:00)
► Internet Protocol Version 4, Src: 20.1.0.30, Dst: 20.1.0.10
► User Datagram Protocol, Src Port: 58591, Dst Port: 53
► Domain Name System (query)
 Transaction ID: 0x4cbd
 Flags: 0x0100 Standard query
 0... = Response: Message is a query
 .000 0.... = Opcode: Standard query (0)
 0.... = Truncated: Message is not truncated
 1.... = Recursion desired: Do query recursively
 0.... = Z: reserved (0)
 0.... = Non-authenticated data: Unacceptable
 Questions : 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
► Queries
[Response In: 19]

Tras ejecutar la orden ping www.cisco.com el equipo roble genera una mensaje DNS con destino dnsusal. Como se puede observar el campo Recursion desired está activado por lo tanto se trata de una pregunta recursiva con el objetivos de que el servidor DNS por defecto (dnsusal) se encargue de realizar todas las consultas y el equipo roble sólo reciba la dirección IP de su solicitud.

*Standard input [HUB1 Ethernet0 to R1 FastEthernet0/0]						
No.	Time	Source	Destination	Protocol	Length	Info
7	66.741990	20.1.0.10	198.41.0.4	DNS	112	Standard query 0x7c7c A www.cisco.com OPT
8	66.773838	198.41.0.4	20.1.0.10	DNS	149	Standard query response 0x7c7c A www.cisco.com NS dnscom.com A 30.0.0.10 OPT
9	66.778591	20.1.0.10	30.0.0.10	DNS	96	Standard query 0x3d3e A www.cisco.com OPT
▶	Frame 7: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0					
▶	Ethernet II, Src: 0c:77:5d:6b:be:00 (0c:77:5d:6b:be:00), Dst: ca:01:06:c5:00:00 (ca:01:06:c5:00:00)					
▶	Internet Protocol Version 4, Src: 20.1.0.10, Dst: 198.41.0.4					
▶	User Datagram Protocol, Src Port: 33788, Dst Port: 53					
▶	Domain Name System (query)					
	Transaction ID: 0x7c7c					
▼	Flags: 0x0010 Standard query					
	0... = Response: Message is a query					
	.000 0... = Opcode: Standard query (0)					
 0... = Truncated: Message is not truncated					
0.... = Recursion desired: Don't do query recursively					
0.... = Z: reserved (0)					
1.... = Non-authenticated data: Acceptable					
	Questions: 1					
	Answer RRs: 0					
	Authority RRs: 0					
	Additional RRs: 1					
▶	Queries					
▶	Additional records					
	[Response In: 8]					

Debido a lo explicado previamente, dnsusal envía un mensaje de tipo DNS con destino dnsraiz, a diferencia del mensaje anterior, en este el campo Recursion desired está desactivado por lo que se trata de una pregunta iterativa para que si dnsraiz no conoce la resolución de nombre de www.cisco.com le devuelva la dirección de un servidor DNS donde se puede encontrar..

*Standard input [HUB1 Ethernet0 to R1 FastEthernet0/0]						
No.	Time	Source	Destination	Protocol	Length	Info
7	66.741990	20.1.0.10	198.41.0.4	DNS	112	Standard query 0x7c7c A www.cisco.com OPT
8	66.773838	198.41.0.4	20.1.0.10	DNS	149	Standard query response 0x7c7c A www.cisco.com NS dnscom.com A 30.0.0.10 OPT
9	66.778591	20.1.0.10	30.0.0.10	DNS	96	Standard query 0x3d3e A www.cisco.com OPT
▶	Frame 8: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0					
▶	Ethernet II, Src: ca:01:06:c5:00:00 (ca:01:06:c5:00:00), Dst: 0c:77:5d:6b:be:00 (0c:77:5d:6b:be:00)					
▶	Internet Protocol Version 4, Src: 20.1.0.10, Dst: 198.41.0.4					
▶	User Datagram Protocol, Src Port: 53, Dst Port: 33788					
▶	Domain Name System (response)					
	Transaction ID: 0x7c7c					
▼	Flags: 0x0000 Standard query response, No error					
	1.... = Response: Message is a response					
	.000 0... = Opcode: Standard query (0)					
 1... = Authoritative: Server is not an authority for domain					
0.... = Truncated: Message is not truncated					
0.... = Recursion desired: Don't do query recursively					
0.... = Recursion available: Server can't do recursive queries					
0.... = Z: reserved (0)					
0.... = Answer authenticated: Answer/authority portion was not authenticated by the server					
0.... = Non-authenticated data: Unacceptable					
 0000 = Reply code: No error (0)					
	Questions: 1					
	Answer RRs: 0					
	Authority RRs: 1					
	Additional RRs: 2					
▶	Queries					
▶	Authoritative nameservers					
▶	Additional records					

Dnsraiz no conoce la resolución de www.cisco.com pero le responde con la IP de dnscom (30.0.0.10) ya que es el encargado del dominio com para que le pregunte a él. Esta respuesta es de tipo iterativa.

*Standard input [HUB1 Ethernet0 to R1 FastEthernet0/0]						
No.	Time	Source	Destination	Protocol	Length	Info
9	66.778591	20.1.0.10	30.0.0.10	DNS	96	Standard query 0x3d3e A www.cisco.com OPT
10	66.814213	30.0.0.10	20.1.0.10	DNS	151	Standard query response 0x3d3e A www.cisco.com NS dnsCisco.cisco.com A 30.0.0.2 OPT
11	66.827341	20.1.0.10	30.0.0.2	DNS	96	Standard query 0x5eac A www.cisco.com OPT
▶	Frame 9: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0					
▶	Ethernet II, Src: 0c:77:5d:6b:be:00 (0c:77:5d:6b:be:00), Dst: ca:01:06:c5:00:00 (ca:01:06:c5:00:00)					
▶	Internet Protocol Version 4, Src: 20.1.0.10, Dst: 30.0.0.10					
▶	User Datagram Protocol, Src Port: 35559, Dst Port: 53					
▶	Domain Name System (query)					
	Transaction ID: 0x3d3e					
▼	Flags: 0x0010 Standard query					
	0... = Response: Message is a query					
	.000 0... = Opcode: Standard query (0)					
 0... = Truncated: Message is not truncated					
0.... = Recursion desired: Don't do query recursively					
0.... = Z: reserved (0)					
1.... = Non-authenticated data: Acceptable					
	Questions: 4					
	Answer RRs: 0					
	Authority RRs: 0					
	Additional RRs: 1					
▶	Queries					
▶	Additional records					
	[Response In: 10]					

Posteriormente, dnsusal enviará un mensaje a dnscom preguntando de forma iterativa (Recursion desired desactivado) por www.cisco.com.

*Standard input [HUB1 Ethernet0 to R1 FastEthernet0/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
9	66.778691	20.1.0.10	30.0.0.10	DNS	96	Standard query 0x3d3e A www.cisco.com OPT
10	66.814213	30.0.0.10	20.1.0.10	DNS	151	Standard query response 0x3d3e A www.cisco.com NS dnscisco.cisco.com A 30.0.0.2 OPT
11	66.827341	20.1.0.10	30.0.0.2	DNS	96	Standard query 0x5eac A www.cisco.com OPT

► Frame 10: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface 0
 ► Ethernet II, Src: ca:01:06:c5:00:00 (ca:01:06:c5:00:00), Dst: 0c:77:5d:6b:be:00 (0c:77:5d:6b:be:00)
 ► Internet Protocol Version 4, Src: 30.0.0.10, Dst: 20.1.0.10
 ► User Datagram Protocol, Src Port: 53, Dst Port: 35559
 ▾ Domain Name System (response)

Transaction ID: 0x3d3e

Flags: 0x8000 Standard query response, No error

- 1... = Response: Message is a response
- .000 0.... = Opcode: Standard query (0)
- 0.... = Authoritative: Server is not an authority for domain
- 0.... = Truncated: Message is not truncated
- 0.... = Recursion desired: Don't do query recursively
- 0.... = Recursion available: Server can't do recursive queries
- 0.... = Z: reserved (0)
- 0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
- 0.... = Non-authenticated data: Unacceptable
- 0000 = Reply code: No error (0)

Questions: 1
 Answer RRs: 0
 Authority RRs: 1
 Additional RRs: 2

► Queries
 ► Authoritative nameservers
 ► Additional records

Dnscom no conoce la resolución de www.cisco.com pero le responde de forma iterativa con la IP de dnscisco (30.0.0.2), que es el encargado del dominio cisco.com.

*Standard input [HUB1 Ethernet0 to R1 FastEthernet0/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
10	66.814213	30.0.0.10	20.1.0.10	DNS	151	Standard query response 0x3d3e A www.cisco.com NS dnscisco.cisco.com A 30.0.0.2 OPT
11	66.827341	20.1.0.10	30.0.0.2	DNS	96	Standard query 0x5eac A www.cisco.com OPT
12	67.630330	20.1.0.10	30.0.0.2	DNS	96	Standard query 0x0c00 A www.cisco.com OPT

► Frame 11: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0
 ► Ethernet II, Src: 0c:77:5d:6b:be:00 (0c:77:5d:6b:be:00), Dst: ca:01:06:c5:00:00 (ca:01:06:c5:00:00)
 ► Internet Protocol Version 4, Src: 20.1.0.10, Dst: 30.0.0.2
 ► User Datagram Protocol, Src Port: 39070, Dst Port: 53
 ▾ Domain Name System (query)

Transaction ID: 0x5eac

Flags: 0x0010 Standard query

- 0... = Response: Message is a query
- .000 0.... = Opcode: Standard query (0)
- 0.... = Truncated: Message is not truncated
- 0.... = Recursion desired: Don't do query recursively
- 0.... = Z: reserved (0)
- 1.... = Non-authenticated data: Acceptable

Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 1
 ► Queries
 ► Additional records

Dnsusal realiza la misma consulta iterativa a dnscisco.

*Standard input [HUB1 Ethernet0 to R1 FastEthernet0/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
16	67.676872	30.0.0.2	20.1.0.10	DNS	105	Standard query response 0x0c00 A www.cisco.com A 30.1.0.10 A 30.1.0.20
19	67.678644	20.1.0.10	20.1.0.30	DNS	144	Standard query response 0x4cbd A www.cisco.com A 30.1.0.20 A 30.1.0.10 NS dnscisco.cisco.com A ...
22	68.442361	20.1.0.10	193.0.14.129	DNS	101	Standard query 0x816c AAAA dnscisco.cisco.com OPT

► Frame 16: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0
 ► Ethernet II, Src: ca:01:06:c5:00:00 (ca:01:06:c5:00:00), Dst: 0c:77:5d:6b:be:00 (0c:77:5d:6b:be:00)
 ► Internet Protocol Version 4, Src: 30.0.0.2, Dst: 20.1.0.10
 ► User Datagram Protocol, Src Port: 53, Dst Port: 54118
 ▾ Domain Name System (response)

Transaction ID: 0x0c00

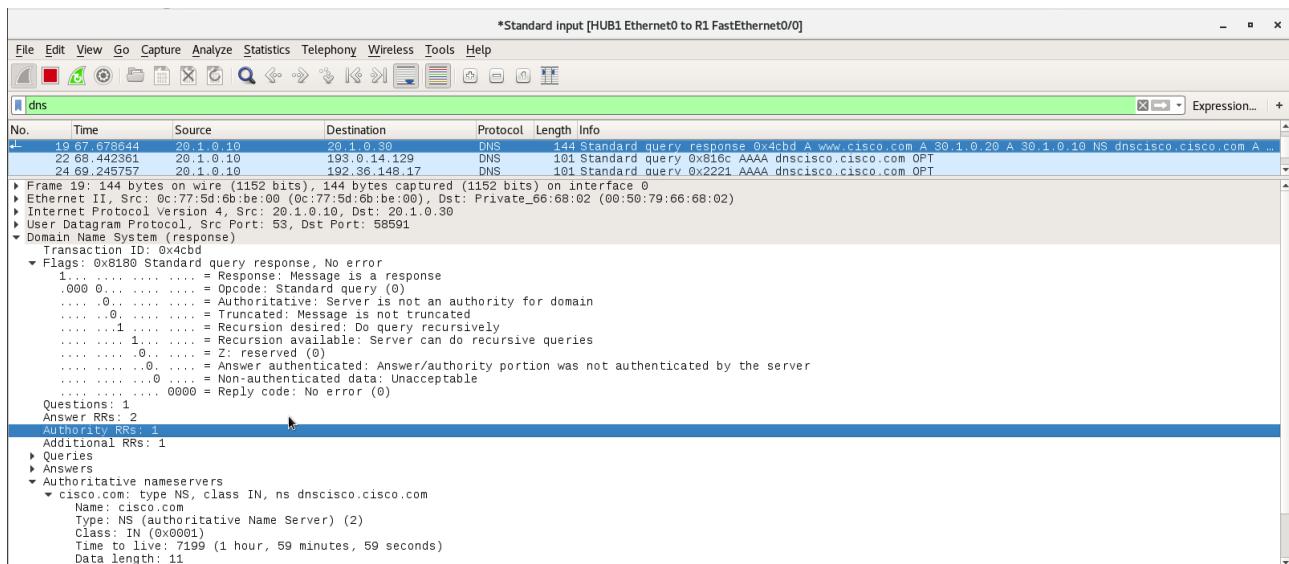
Flags: 0x0580 Standard query response, No error

- 1... = Response: Message is a response
- .000 0.... = Opcode: Standard query (0)
- 1.... = Authoritative: Server is an authority for domain
- 0.... = Truncated: Message is not truncated
- 1.... = Recursion desired: Do query recursively
- 1.... = Recursion available: Server can do recursive queries
- 0.... = Z: reserved (0)
- 0.... = Answer authenticated: Answer/authority portion was not authenticated by the server
- 0.... = Non-authenticated data: Unacceptable
- 0000 = Reply code: No error (0)

Questions: 1
 Answer RRs: 2
 Authority RRs: 0
 Additional RRs: 0

► Queries
 ► Answers
 [Request In: 121]

En este caso dnscisco si conoce la resolución por lo que envía a dnsusal las direcciones IP de www.cisco.com que tiene almacenadas en sus registros, es decir, la de www1 (30.1.0.10) y www2 (30.1.0.20). El campo Recursion desired está activado.



Finalmente, dnsusal responde a la solicitud realizada por roble con las direcciones IP de www.cisco.com. El campo Recursion desired está activado.

Como se puede observar el campo TTL indica cuanto tiempo tiene que cachear una consulta antes de que solicite una nueva. Este campo esta especificado en el fichero db, en nuestro caso como el mensaje tiene de origen a dnsusal estará localizado en en db.es.usal

```

dnsraiz      x      dnscom      x      dnses      x      dnsusal      x      roble      x
GNU nano 3.2                         db.es.usal

$TTL 3h ; ttl de permanencia en las cachEs
@       IN      SOA    dnsusal.usal.es.      root.dnsusal.usal.es.  (
                           20220101 ; Numero de serie
                           28800   ; Refresco despues de 8 horas
                           7200    ; Reintentto despues de 2 horas
                           604800  ; Expiracion despues de 1 semana
                           3h      ; ttl de las respuestas negativas
                           )

; Configuracion de los servidores de nombres
IN      NS      dnsusal.usal.es.
dnsusal IN      A      20.1.0.10

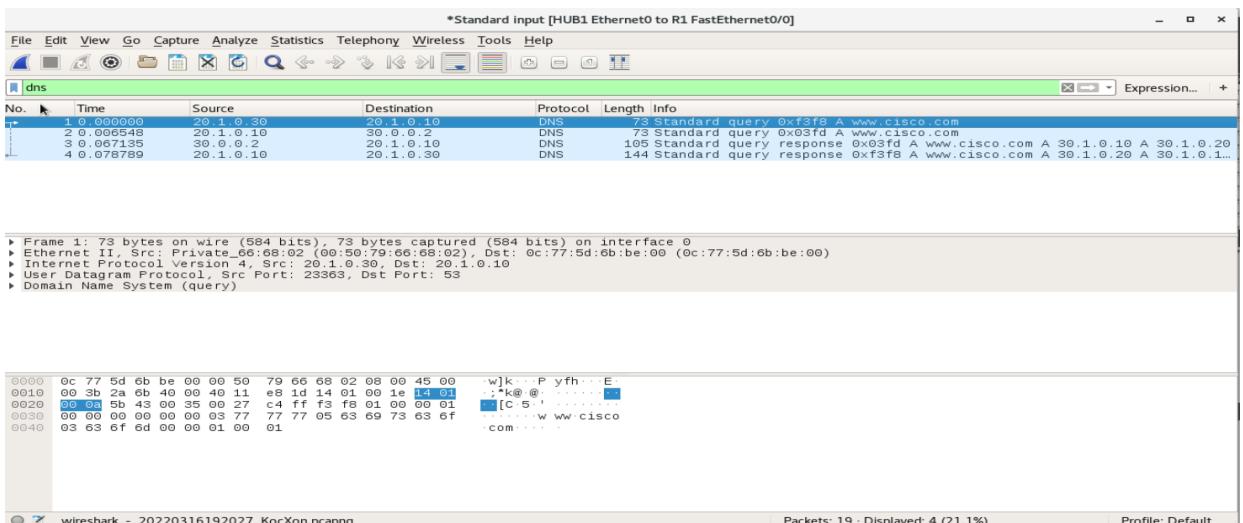
; Configuracion de las maquinas
r1      IN      A      20.1.0.1
portal  IN      A      20.1.0.20
roble   IN      A      20.1.0.30
www     IN      CNAME  portal
diaweb  IN      CNAME  roble

```

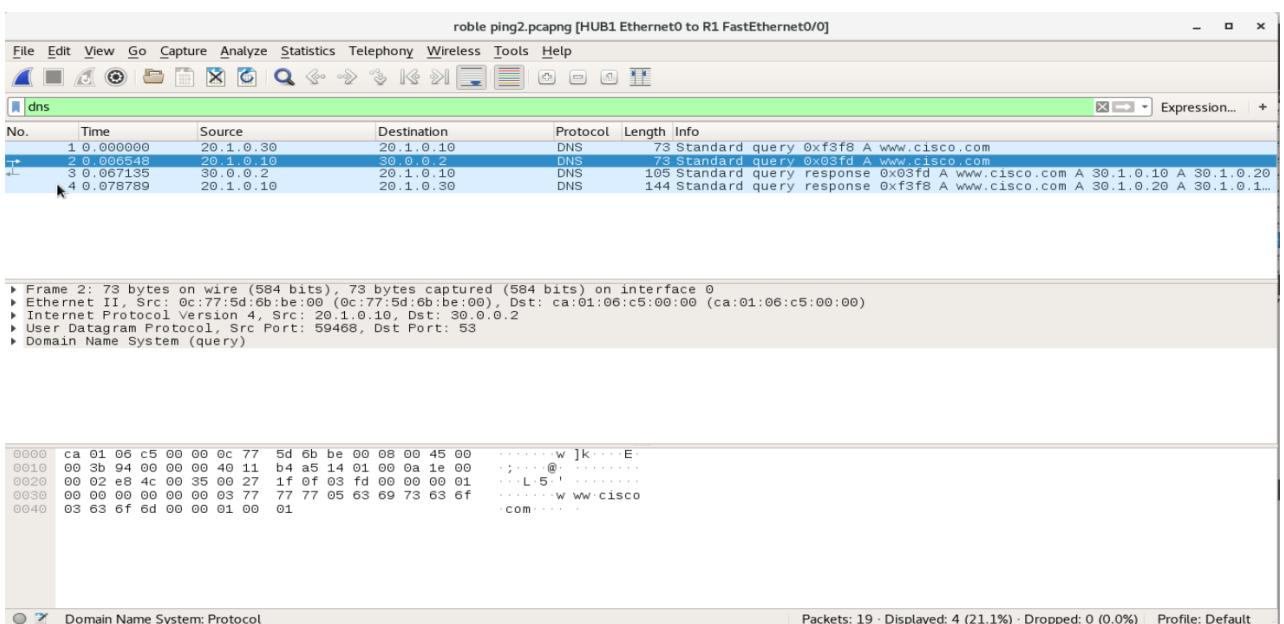
- b) Desde la máquina roble (del dominio usal.es), ejecuta de nuevo ping www.cisco.com. ¿Qué mensajes DNS se han generado esta vez? ¿Por qué? Explica el valor del campo TTL del mensaje de DNS de la respuesta obtenida en roble y compáralo con el de la pregunta anterior.

Una vez vuelto a realizar el `ping www.cisco.com` se observa que se genera únicamente cuatro mensajes del protocolo DNS, ya que el servidor DNSusal tiene cacheado cual es el servidor responsable del dominio .cisco.com. Los mensajes que se generan son los siguientes:

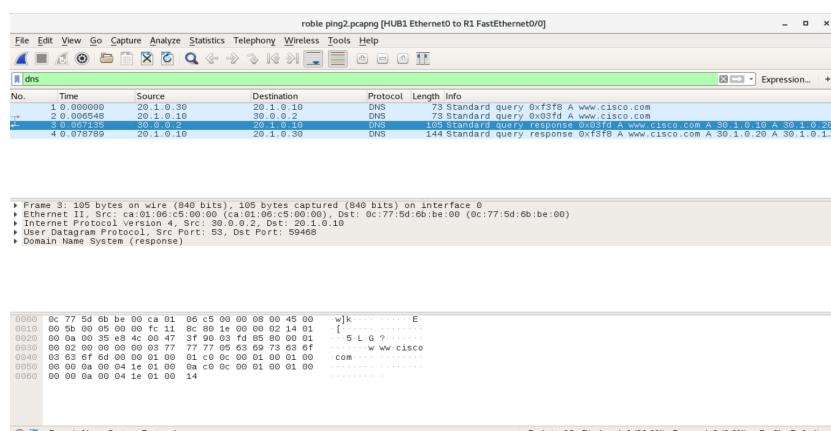
1 → El terminal roble le lanza la pregunta a su servidor DNS, en este caso DNSusal



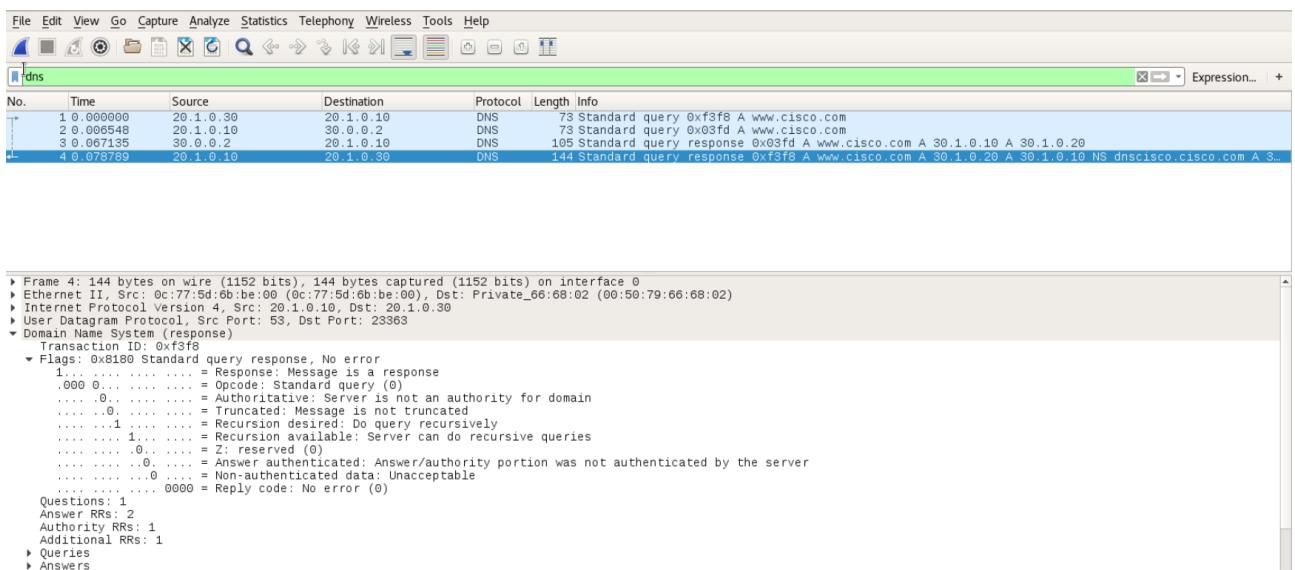
2 → Despues el servidor DNSusal le pregunta al servidor responsable del dominio, que es DNScisco.



3 → DNScisco resuelve la petición que le ha realizado DNSusal, enviando la correspondencia de las ip asociadas al nombre “www.cisco.com”



4 → Por último DNSusal le envía la respuesta obtenida de DNScisco, a roble terminando así la petición DNS



- c) Desde la máquina dnsusal (del dominio usal.es) consulta la caché del DNS. A continuación, ejecuta las órdenes (recuerda lanzar wireshark en el lugar adecuado para capturar el tráfico generado):

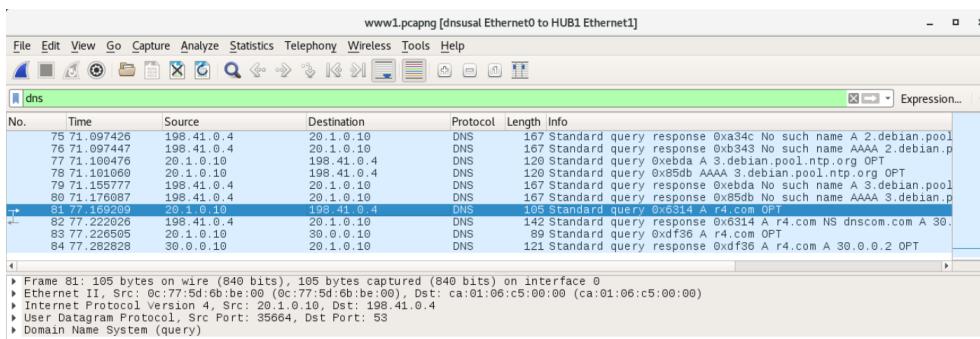
```
dig r4.com > www1.log
dig r4.com > www2.log
dig dnscom.com > r4_1.log
dig dnscom.com > r4_2.log
```

Vuelve a consultar la cache de nuevo.

La orden dig permite obtener entre otros detalles de la resolución de nombre el tiempo de respuesta. ¿Qué mensajes DNS se han generado? ¿Por qué? Muestra y analiza cada mensaje con la ayuda de wireshark y los ficheros log obtenidos (incluyelos en el informe). ¿Ha mejorado el tiempo de respuesta entre la primera pregunta y su repetición? ¿Por qué?

Para este apartado no podemos mirar la caché del servidor DNSusal porque no tiene creado el archivo correspondiente y al consultarla con la orden `cat /var/cache/bind named_dump.db` da error, pero aún así vamos a hacer una deducción de lo que sucedería.

`dig r4.com > www1.log`



En este primer caso se generan cuatro mensajes recorriendo, el primero el DNSusal le pregunta al servidor raíz si sabe cual es responsable del dominio .com

81 77.169209	20.1.0.10	198.41.0.4	DNS	105 Standard query 0x6314 A r4.com OPT
82 77.222026	198.41.0.4	20.1.0.10	DNS	142 Standard query response 0x6314 A r4.com NS dnscom.com A 30.0.0.10 OPT
83 77.226505	20.1.0.10	30.0.0.10	DNS	89 Standard query 0xdf36 A r4.com OPT
84 77.282828	30.0.0.10	20.1.0.10	DNS	121 Standard query response 0xdf36 A r4.com A 30.0.0.2 OPT
Frame 81: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0 Ethernet II, Src: 0c:77:5d:6b:be:00 (0c:77:5d:6b:be:00), Dst: ca:01:06:c5:00:00 (ca:01:06:c5:00:00) Internet Protocol Version 4, Src: 20.1.0.10, Dst: 198.41.0.4 User Datagram Protocol, Src Port: 35664, Dst Port: 53 Domain Name System (query)				
Transaction ID: 0x6314 Flags: 0x0010 Standard query 0... = Response: Message is a query .000 0... = Opcode: Standard query (0)0. = Truncated: Message is not truncated0. = Recursion desired: Don't do query recursively0. = Z: reserved (0)1 = Non-authenticated data: Acceptable Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 1 Queries ► r4.com: type A, class IN Additional records				

El segundo mensaje es la respuesta del servidor raíz enviándole la información del servidor responsable que en este caso es DNScom

81 77.169209	20.1.0.10	198.41.0.4	DNS	105 Standard query 0x6314 A r4.com OPT
82 77.222026	198.41.0.4	20.1.0.10	DNS	142 Standard query response 0x6314 A r4.com NS dnscom.com A 30.0.0.10 OPT
83 77.226505	20.1.0.10	30.0.0.10	DNS	89 Standard query 0xdf36 A r4.com OPT
84 77.282828	30.0.0.10	20.1.0.10	DNS	121 Standard query response 0xdf36 A r4.com A 30.0.0.2 OPT
Frame 81: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0 Ethernet II, Src: 0c:77:5d:6b:be:00 (0c:77:5d:6b:be:00), Dst: ca:01:06:c5:00:00 (ca:01:06:c5:00:00) Internet Protocol Version 4, Src: 20.1.0.10, Dst: 198.41.0.4 User Datagram Protocol, Src Port: 35664, Dst Port: 53 Domain Name System (query)				
Transaction ID: 0x6314 Flags: 0x0010 Standard query .000 0... = Opcode: Standard query (0)0. = Authoritative: Server is not an authority for domain0. = Truncated: Message is not truncated0. = Recursion available: Don't do query recursively0. = Z: reserved (0)0. = Answer authenticated: Answer/authority portion was not authenticated by the server0. = Non-authenticated data: Unacceptable Questions: 1 Answer RRs: 0 Authority RRs: 1 Additional RRs: 2 Queries ► Authoritative nameservers ► com: type NS, class IN, ns dnscom.com Name: com Type: NS (Authoritative Name Server) (2) Class: IN (0x0001) Time to live: 14400 (4 hours) Data length: 9 Name Server: dnscom.com				

El tercero es el traslado de la petición al nuevo servidor DNS que le ha llegado del mensaje anterior

81 77.169209	20.1.0.10	198.41.0.4	DNS	105 Standard query 0x6314 A r4.com OPT
82 77.222026	198.41.0.4	20.1.0.10	DNS	142 Standard query response 0x6314 A r4.com NS dnscom.com A 30.0.0.10 OPT
83 77.226505	20.1.0.10	30.0.0.10	DNS	89 Standard query 0xdf36 A r4.com OPT
84 77.282828	30.0.0.10	20.1.0.10	DNS	121 Standard query response 0xdf36 A r4.com A 30.0.0.2 OPT
Frame 83: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0 Ethernet II, Src: 0c:77:5d:6b:be:00 (0c:77:5d:6b:be:00), Dst: ca:01:06:c5:00:00 (ca:01:06:c5:00:00) Internet Protocol Version 4, Src: 20.1.0.10, Dst: 30.0.0.10 User Datagram Protocol, Src Port: 50824, Dst Port: 53 Domain Name System (query)				
Transaction ID: 0xdf36 Flags: 0x0010 Standard query 0... = Response: Message is a query .000 0... = Opcode: Standard query (0)0. = Truncated: Message is not truncated0. = Recursion desired: Don't do query recursively0. = Z: reserved (0)1 = Non-authenticated data: Acceptable Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 1 Queries ► r4.com: type A, class IN Answers				

Y el último es la respuesta de vuelta del servidor DNScom con la información referente a la consulta r4.com

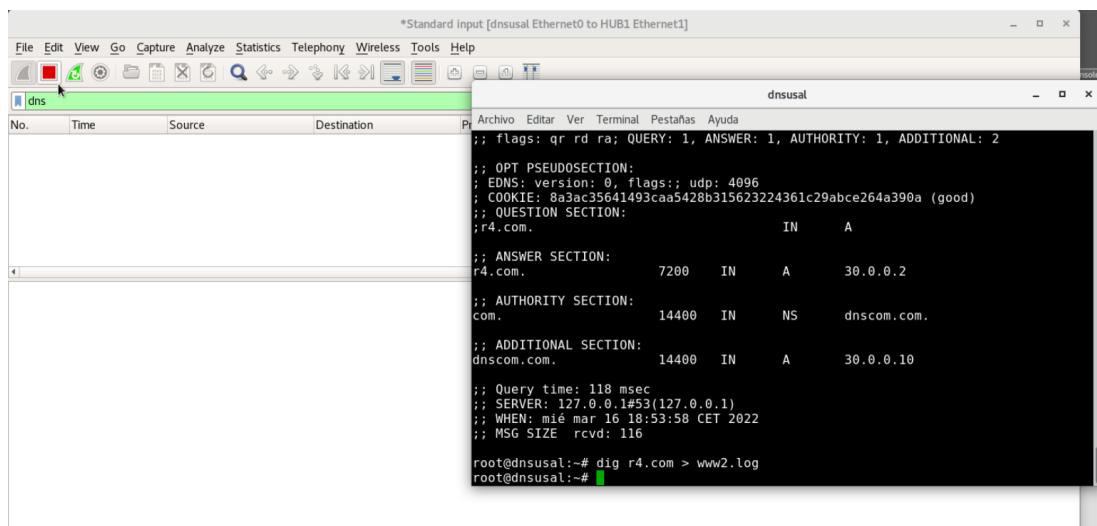
81 77.169209	20.1.0.10	198.41.0.4	DNS	105 Standard query 0x6314 A r4.com OPT
82 77.222026	198.41.0.4	20.1.0.10	DNS	142 Standard query response 0x6314 A r4.com NS dnscom.com A 30.0.0.10 OPT
83 77.226505	20.1.0.10	30.0.0.10	DNS	89 Standard query 0xdf36 A r4.com OPT
84 77.282828	30.0.0.10	20.1.0.10	DNS	121 Standard query response 0xdf36 A r4.com A 30.0.0.2 OPT
Frame 83: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0 Ethernet II, Src: 0c:77:5d:6b:be:00 (0c:77:5d:6b:be:00), Dst: ca:01:06:c5:00:00 (ca:01:06:c5:00:00) Internet Protocol Version 4, Src: 20.1.0.10, Dst: 30.0.0.10 User Datagram Protocol, Src Port: 50824, Dst Port: 53 Domain Name System (query)				
Transaction ID: 0xdf36 Flags: 0x0010 Standard query0. = Z: reserved (0)0. = Answer authenticated: Answer/authority portion was not authenticated by the server0. = Non-authenticated data: Unacceptable0000 = Reply code: No error (0) Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 1 Queries ► r4.com: type A, class IN Answers ► r4.com: type A, class IN, addr 30.0.0.2 Name: r4.com Type: A (Host Address) (1) Class: IN (0x0001) Time to live: 7200 (2 hours) Data length: 4 Address: 30.0.0.2 Additional records ► <Root>: type OPT				

Lo que se conseguiría con todo esto es que en la caché del servidor DNSusal haya una entrada que contenga un registro A con la correspondencia de r4.com y su IP (30.0.0.2). El archivo log generado por el dig es el siguiente:

```
root@dnsusal:~# cat www1.log
; <>> DiG 9.11.5-P4-5.1+deb10u6-Debian <>> r4.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23896
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 8a3ac35641493caa5428b315623224361c29abce264a390a (good)
;; QUESTION SECTION:
;r4.com.           IN      A
;;
;; ANSWER SECTION:
r4.com.        7200    IN      A      30.0.0.2
;;
;; AUTHORITY SECTION:
com.          14400   IN      NS     dnscom.com.
;;
;; ADDITIONAL SECTION:
dnscom.com.    14400   IN      A      30.0.0.10
;;
;; Query time: 118 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: mié mar 16 18:53:58 CET 2022
;; MSG SIZE  rcvd: 116
root@dnsusal:~#
```

En él se observa lo que se ha tardado en resolver la petición (118 ms) y aparte el registro A que se incluirá en su caché, como hemos dicho anteriormente.

```
dig r4.com > www2.log
```



Como se observa en la imagen anterior si volvemos a ejecutar la sentencia y capturamos en el mismo punto con el whireskash, a este no le da tiempo a capturar ningún mensaje de tipo DNS ya que la respuesta de la orden es prácticamente inmediata como vemos en el log generado

```
root@dnsususal:~# cat www2.log

; <>> DiG 9.11.5-P4-5.1+deb10u6-Debian <>> r4.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30942
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: 019c46f559fa34a80cf9a96d62322a037ffff7bb6292cae34 (good)
;; QUESTION SECTION:
;r4.com.           IN      A

;; ANSWER SECTION:
r4.com.          5715    IN      A      30.0.0.2

;; AUTHORITY SECTION:
com.             12915   IN      NS     dnscom.com.

;; ADDITIONAL SECTION:
dnscom.com.      12915   IN      A      30.0.0.10

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: mié mar 16 19:18:43 CET 2022
;; MSG SIZE rcvd: 116

root@dnsususal:~#
```

Se ve que la respuesta es de 2ms prácticamente imposible de ser capturada. Ya que la dirección por la que se estaba preguntando ya estaba cacheada en la máquina.

```
dig dnscom.com > r4_1.log
```

2 10 043700	20.1.0.10	30.0.0.10	DNS	93 Standard query 0x0106 A dnscom.com OPT
3 10 097412	30.0.0.10	20.1.0.10	DNS	125 Standard query response 0x0106 A dnscom.com A 30.0.0.10 OPT

Al ejecutar la orden se generan los dos mensajes de arriba, el de pregunta al servidor del dominio y la respuesta del mismo.

2 10 043700	20.1.0.10	30.0.0.10	DNS	93 Standard query 0x0106 A dnscom.com OPT
3 10 097412	30.0.0.10	20.1.0.10	DNS	125 Standard query response 0x0106 A dnscom.com A 30.0.0.10 OPT

Frame 2: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
Ethernet II, Src: 0c:77:5d:6b:be:00 (0c:77:5d:6b:be:00), Dst: ca:01:06:c5:00:00 (ca:01:06:c5:00:00)
Internet Protocol Version 4, Src: 20.1.0.10, Dst: 30.0.0.10
User Datagram Protocol, Src Port: 34935, Dst Port: 53
Domain Name System (query)

Transaction ID: 0x0106
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
dnscom.com: type A, class IN

El primer mensaje tiene como destinatario el servidor DNScom, que es el responsable del dominio .com.

2 10 043700	20.1.0.10	30.0.0.10	DNS	93 Standard query 0x0106 A dnscom.com OPT
3 10 097412	30.0.0.10	20.1.0.10	DNS	125 Standard query response 0x0106 A dnscom.com A 30.0.0.10 OPT

Frame 3: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface 0
Ethernet II, Src: ca:01:06:c5:00:00 (ca:01:06:c5:00:00), Dst: 0c:77:5d:6b:be:00 (0c:77:5d:6b:be:00)
Internet Protocol Version 4, Src: 30.0.0.10, Dst: 20.1.0.10
User Datagram Protocol, Src Port: 53, Dst Port: 34935
Domain Name System (response)
Transaction ID: 0x0106
Flags: 0x8400 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1
Queries
dnscom.com: type A, class IN
Answers
dnscom.com: type A, class IN, addr 30.0.0.10
Additional records
[Request In: 2]
[Time: 0.053712000 seconds]

El segundo es la respuesta del servidor DNScom a DNSusal, con la información de la petición que la había pedido que en este caso son los propios datos.

En el archivo log podemos ver lo siguiente, que en la caché se va a añadir el registro A con la correspondencia dnscom.com. 30.0.0.10 y el tiempo que ha tardado en realizarse la consulta que son 66 ms.

```
root@dnsusal:~# cat r4_1.log
; <>> DiG 9.11.5-P4-5.1+deb10u6-Debian <>> dnscom.com
; global options: +cmd
; Got answer:
; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 45047
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

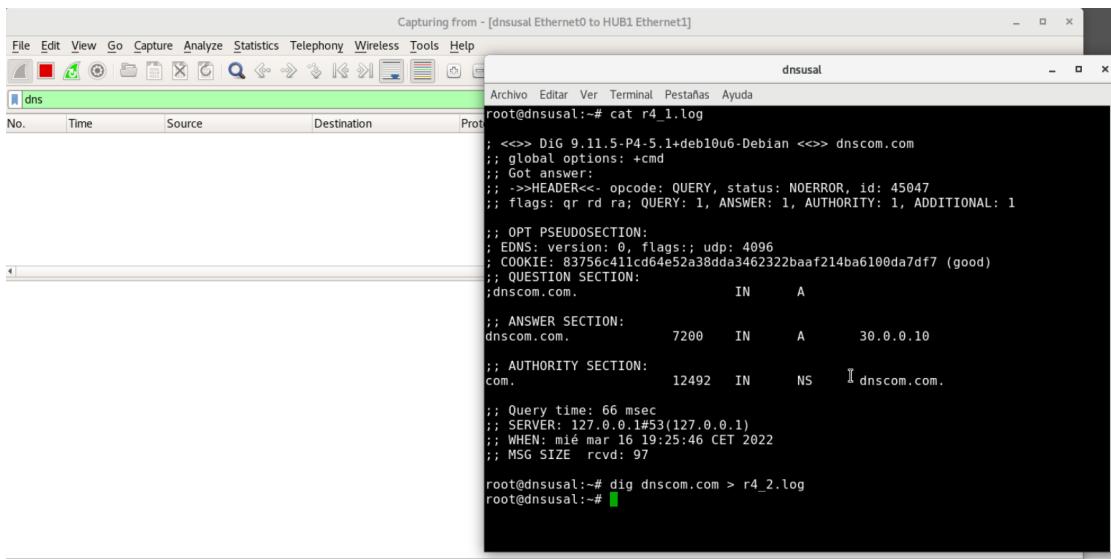
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 83756c411cd64e52a38dda346232baaf214ba6100da7df7 (good)
; QUESTION SECTION:
;dnscom.com.           IN      A

; ANSWER SECTION:
dnscom.com.        7200    IN      A      30.0.0.10

; AUTHORITY SECTION:
com.                12492   IN      NS     dnscom.com.

; Query time: 66 msec
; SERVER: 127.0.0.1#53(127.0.0.1)
; WHEN: mié mar 16 19:25:46 CET 2022
; MSG SIZE rcvd: 97
root@dnsusal:~#
```

dig dnscisco.com > r4_2.log



Al igual que en la otra ocasión al tener cacheado ya la correspondencia la resolución del nombre es inmediata, por lo que el analizador de red no es capaz de captar ningún mensaje del tipo DNS

```
root@dnsusal:~# cat r4_2.log
; <>> DiG 9.11.5-P4-5.1+deb10u6-Debian <>> dnscom.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64368
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: ad5e0b413d2ba94358e9b83462322dc9fe881e32b66b4d57 (good)
; QUESTION SECTION:
;dnscom.com.           IN      A

;; ANSWER SECTION:
dnscom.com.       6657    IN      A      30.0.0.10

;; AUTHORITY SECTION:
com.            11949   IN      NS     dnscom.com.

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: mié mar 16 19:34:49 CET 2022
;; MSG SIZE  rcvd: 97

root@dnsusal:~#
```

Y el archivo generado es este, en el que se observa que efectivamente el tiempo son dos milisegundos. Y que el registro que se va a almacenar en caché será el registro A que hemos mencionado anteriormente.

7. Servidores DNS locales

Se desea instalar un servidor DNS privado con un dominio ficticio, por ejemplo “redes.usal.es”, para nombrar a los equipos del laboratorio. Todos los PCs de nuestra red pertenecerán a dicho dominio. El nombre completo de los PCs terminará con “redes.usal.es”, por ejemplo: pc1.redes.usal.es. El diagrama resultante del montaje se aproximará al de la Figura 2.

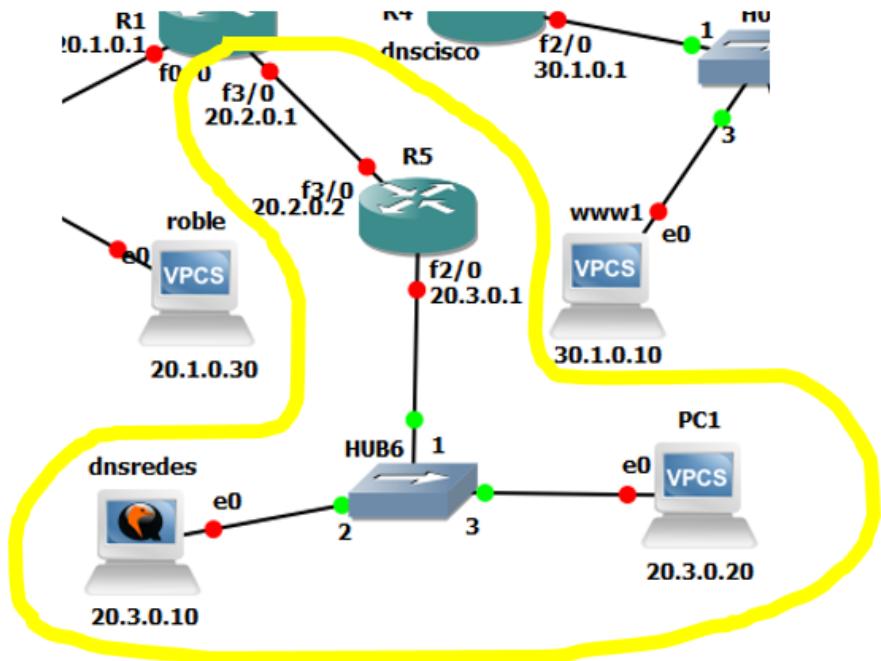


Figura 2: Dominio redes.usal.es

Se pide:

- a) Añadir al esquema de red los elementos necesarios (router, hub y equipos) y configurarlos para que puedan comunicarse en la red. Asignar direcciones IP de la subred 20.3.0.0/16. Incluir el fichero de configuración */etc/network/interfaces* del equipo *dnsreduces*, y las órdenes de configuración en PC1 y R5. Recuerda que para dar conectividad total a esta nueva subred tendremos que modificar adecuadamente las tablas de rutas de nuestro escenario. Indica estos cambios y donde los has realizado. Antes de continuar comprueba que has configurado correctamente todos los elementos. ¿Qué pruebas has realizado?

NOTA:

- Para configurar *dnsreduces* consultar la sintaxis de las órdenes en el anexo de órdenes de redes en Linux disponible en Diaweb (Material práctico Resumen de Órdenes). Especialmente: */etc/network/interfaces*, */etc/resolv.conf* y las relacionadas con *bind*.
- Para configurar PC1 y los routers consultar las órdenes IOS en el manual de Órdenes IOS disponible en Diaweb (Material práctico Resumen de Órdenes).

Configuración de PC1:

```

PC1> set pcname PC1

PC1> ip 20.3.0.20/16 20.3.0.1
Checking for duplicate address...
PC1 : 20.3.0.20 255.255.0.0 gateway 20.3.0.1

PC1> ip domain redes.usal.es

PC1> ip dns 20.3.0.10

PC1>

```

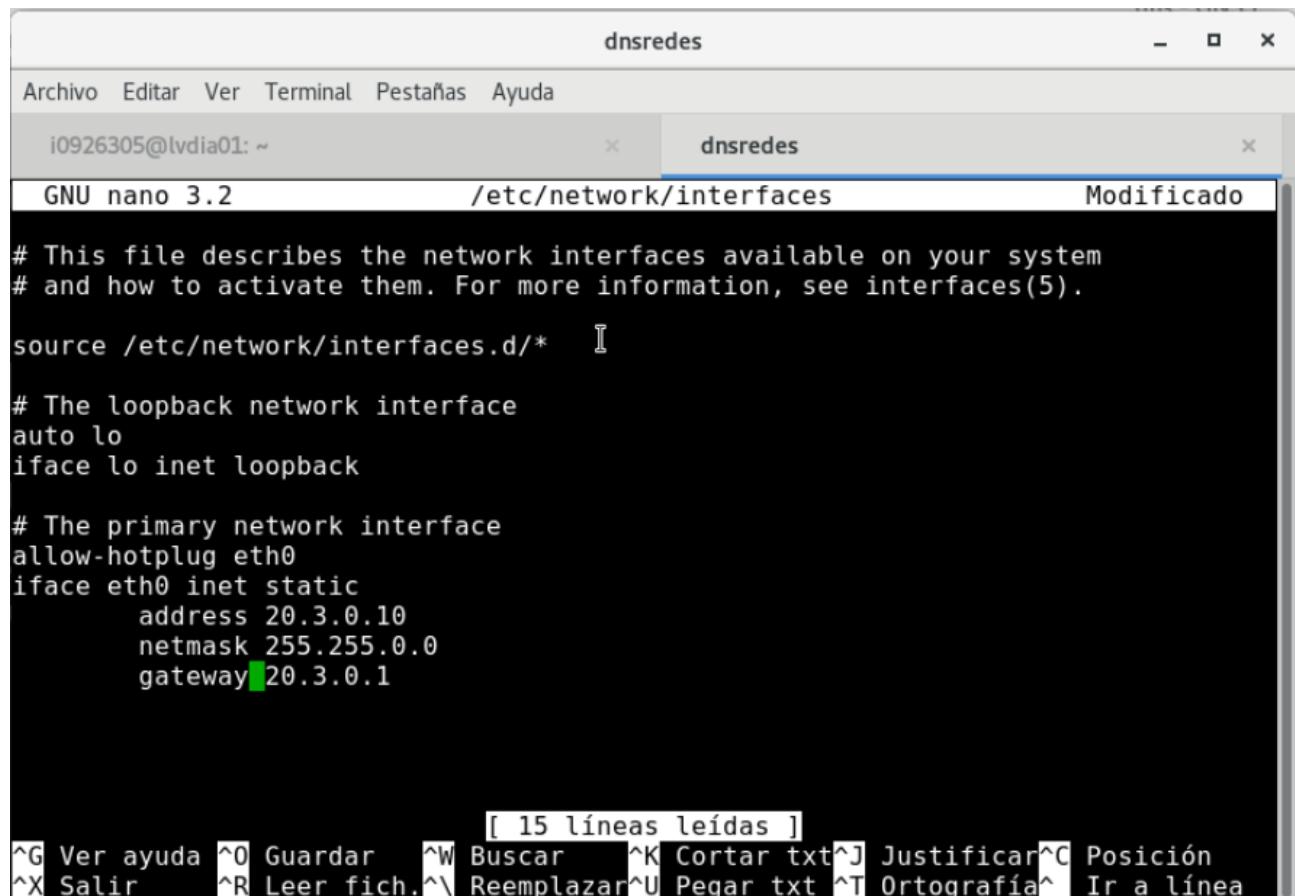
Configuración de PC1 para asignarle el nombre 'PC1', su IP (20.3.0.20), la puerta de enlace predeterminada (20.3.0.1), al dominio que pertenece (redes.usal.es) y la IP del DNS predeterminado (20.3.0.10)

```
PC1> show ip

NAME      : PC1[1]
IP/MASK   : 20.3.0.20/16
GATEWAY   : 20.3.0.1
DNS       : 20.3.0.10
DOMAIN NAME: redes.usal.es
MAC       : 00:50:79:66:68:05
LPORT     : 10124
RHOST:PORT: 127.0.0.1:10125
MTU:      : 1500
```

En esta imagen vemos como PC1 está configurado correctamente.

Configuración de dnsredes:



```
dnsredes
Archivo Editar Ver Terminal Pestañas Ayuda
i0926305@lvdia01: ~          dnsredes
GNU nano 3.2           /etc/network/interfaces           Modificado

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
    address 20.3.0.10
    netmask 255.255.0.0
    gateway 20.3.0.1

[ 15 líneas leídas ]
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt^J Justificar^C Posición
^X Salir    ^R Leer fich.^V Reemplazar^U Pegar txt ^T Ortografía^I Ir a línea
```

Configuramos DNSredes mediante la modificación del archivo “/etc/network/interfaces”, establecemos su IP estática que es 20.3.0.10, la máscara y la puerta de enlace predeterminada que corresponde con el puerto f2/0 de R5 (20.3.0.1).

Configuración de R5:

```

Archivo Editar Ver Terminal Pestañas Ayuda
dnses PC1 R5
R5(config)#interface FastEthernet2/0
R5(config-if)#ip address 20.3.0.1 255.255.0.0
R5(config-if)#no shutdown
R5(config-if)#
*Mar 17 17:02:40.919: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
R5(config-if)#
*Mar 17 17:02:40.919: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa2/0 Physical Port Administrative State Down
*Mar 17 17:02:41.919: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to up
R5(config-if)#

```

Configuramos la interfaz f2/0 con la IP 20.3.0.1 y la máscara de subred predeterminada para IPs de la clase B y la activamos con el comando ‘no shutdown’.

```

Archivo Editar Ver Terminal Pestañas Ayuda
dnses PC1 R5
R5(config)#interface FastEthernet0/0
R5(config-if)#ip address 20.2.0.2 255.255.0.0
R5(config-if)#no shutdown
R5(config-if)#esit
*Mar 17 17:06:11.375: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
R5(config-if)#esit
*Mar 17 17:06:11.375: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa0/0 Physical Port Administrative State Down
*Mar 17 17:06:12.375: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R5(config-if)#

```

Configuramos la interfaz f0/0 con la IP 20.2.0.2 con la misma máscara de subred que la interfaz anterior y la activamos con el comando ‘no shutdown’.

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	20.2.0.2	YES	manual	up	up
FastEthernet1/0	unassigned	YES	unset	administratively down	down
FastEthernet1/1	unassigned	YES	unset	administratively down	down
FastEthernet2/0	20.3.0.1	YES	manual	up	up
FastEthernet2/1	unassigned	YES	unset	administratively down	down
GigabitEthernet3/0	unassigned	YES	unset	administratively down	down
GigabitEthernet4/0	unassigned	YES	unset	administratively down	down
Serial5/0	unassigned	YES	unset	administratively down	down
Serial5/1	unassigned	YES	unset	administratively down	down
Serial5/2	unassigned	YES	unset	administratively down	down
Serial5/3	unassigned	YES	unset	administratively down	down

En esta imagen vemos como FastEthernet2/0 y FastEthernet0/0 se han configurado correctamente.

```

Archivo Editar Ver Terminal Pestañas Ayuda
i0961594@lvdia01: ~ R5
R5(config)#ip route 0.0.0.0 0.0.0.0 20.2.0.1

```

Por último establecemos la ruta por defecto que debe usar R5 para que si no tiene entrega directa para el paquete lo envía hacia R1, es decir, a la dirección IP 20.1.0.1.

```
R5#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route
Gateway of last resort is 20.2.0.1 to network 0.0.0.0

      20.0.0.0/16 is subnetted, 2 subnets
C        20.2.0.0 is directly connected, FastEthernet0/0
C        20.3.0.0 is directly connected, FastEthernet2/0
S*   0.0.0.0/0 [1/0] via 20.2.0.1
```

En esta imagen vemos como la entrada se ha añadido correctamente.

Por último, debemos configurar la R1 para establecer el enlace entre ambos routers.

```
R1
Archivo Editar Ver Terminal Pestañas Ayuda
i0961594@lvdia01: ~ × R5 × R1 ×
R1(config-if)#no shutdown
R1(config-if)#
*Mar 17 16:33:43.407: %LINK-3-UPDOWN: Interface FastEthernet3/0, changed state to up
R1(config-if)#
R1(config-if)#
*Mar 17 16:33:43.407: %ENTITY_ALARM-6-INFO: CLEAR INFO Fa3/0 Physical Port Adminis
trative State Down
*Mar 17 16:33:44.407: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet3/0, changed state to up
R1(config-if)#
R1(config-if)#

```

Configuraremos la interfaz f0/0 con la IP 20.2.0.2 y la activaremos con el comando 'no shutdown'.

R1

Archivo Editar Ver Terminal Pestañas Ayuda

i0961594@lvdia01: ~ R5 R1

```
R1#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 20.1.0.1 YES NVRAM up up
ATM1/0 unassigned YES unset administratively down down
FastEthernet2/0 20.0.0.2 YES NVRAM up up
FastEthernet3/0 20.2.0.1 YES manual up up
FastEthernet3/1 unassigned YES NVRAM administratively down down
GigabitEthernet4/0 unassigned YES NVRAM administratively down down
Serial5/0 unassigned YES NVRAM administratively down down
Serial5/1 unassigned YES NVRAM administratively down down
Serial5/2 unassigned YES NVRAM administratively down down
Serial5/3 unassigned YES NVRAM administratively down down
Ethernet6/0 unassigned YES NVRAM administratively down down

R1#
```

En esta imagen vemos como FastEthernet2/0 y FastEthernet0/0 se han configurado correctamente.

R1

Archivo Editar Ver Terminal Pestañas Ayuda

i0961594@lvdia01: ~ R5 R1

```
R1(config)#ip route 20.3.0.0 255.255.0.0 20.2.0.2
```

Usamos la orden ip route para que R1 sepa encaminar los mensajes que van hacia el nuevo dominio y los envíe por la interfaz f0/0 de R5, es decir, la dirección IP 20.2.0.2.

R1

Archivo Editar Ver Terminal Pestañas Ayuda

i0961594@lvdia01: ~ R5 R1

```
R1>show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

Gateway of last resort is 20.0.0.1 to network 0.0.0.0

      20.0.0.0/16 is subnetted, 4 subnets
C        20.0.0.0 is directly connected, FastEthernet2/0
C        20.1.0.0 is directly connected, FastEthernet0/0
C        20.2.0.0 is directly connected, FastEthernet3/0
S*      20.3.0.0 [1/0] via 20.2.0.2
S*      0.0.0.0/0 [1/0] via 20.0.0.1
```

En esta imagen vemos como la entrada se ha añadido correctamente.

Para comprobar que todo está configurado correctamente basta con realizar un par de pings desde una máquina localizada en el nuevo dominio y otra localizada, por ejemplo, en el dominio “usal.es”.

```

roble> ping 20.3.0.20
20.3.0.20 icmp_seq=1 timeout
20.3.0.20 icmp_seq=2 timeout
84 bytes from 20.3.0.20 icmp_seq=3 ttl=62 time=37.426 ms
84 bytes from 20.3.0.20 icmp_seq=4 ttl=62 time=21.931 ms
84 bytes from 20.3.0.20 icmp_seq=5 ttl=62 time=27.281 ms

roble>

```

Ping desde roble a PC1.

```

PC1> ping 20.1.0.30
84 bytes from 20.1.0.30 icmp_seq=1 ttl=62 time=28.677 ms
84 bytes from 20.1.0.30 icmp_seq=2 ttl=62 time=39.769 ms
84 bytes from 20.1.0.30 icmp_seq=3 ttl=62 time=28.459 ms
84 bytes from 20.1.0.30 icmp_seq=4 ttl=62 time=32.035 ms
84 bytes from 20.1.0.30 icmp_seq=5 ttl=62 time=37.515 ms

PC1>

```

Ping desde PC1 a roble.

- b) Configurar un servidor DNS que sea maestro del dominio “redes.usal.es” en la máquina *dnsredes* de tal forma que sea capaz de responder peticiones internas tanto de forma directa como inversa.

- i. En el fichero /etc/bind/named.conf.options deshabilitar las opciones de seguridad. Cambiar:

```

dnssec-validation auto; por
// dnssec-validation auto;
// dnssec-enable no;
// dnssec-validation no;
root@lipcUR:~# cat /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    =====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    =====
    //dnssec-validation auto;
    dnssec-enable no;
    dnssec-validation no;

    listen-on-v6 { any; };
}
root@lipcUR:~#

```

- ii. Añade en el archivo /etc/bind/named.conf.local la especificación de maestro para el dominio en cuestión y para la resolución inversa como sigue:

```

// Archivo para búsquedas directas
zone "redes.usal.es" {
    type master;
    file "/etc/bind/db.es.usal.redes";

```

```

};

// Archivo para búsquedas inversas
zone "0.3.20.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0.3.20";
};

GNU nano 3.2          /etc/bind/named.conf.local          Modificado

//


// Do any local configuration here
//


// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

// Archivo para la búsqueda directa
zone "redes.usal.es"{
    type master;
    file "/etc/bind/db.es.usal.redes";
};

// Archivo para las búsquedas inversas
zone "0.3.20.in-addr.arpa"{
    type master;
    file "/etc/bind/db.0.3.20";
};

```

iii. Crea el archivo de zona de resolución directa */etc/bind/db.es.usal.redes* como sigue:

```

$TTL 1d; ttl de permanencia en las cachEs
@ IN SOA dnsredes.redes.usal.es. root.redes.usal.es. (
    20170201; número de serie actualizar en cada cambio
    ; redirix recomienda poner la fecha
    604800 ; Refresco 1 semana (servidores secundarios)
    86400 ; Reintentto tras 1 día
    2419200 ; Expira después de 4 semanas
    1d) ; ttl de las respuestas negativas

    IN NS dnsredes.redes.usal.es.
dnsredes IN      A      20.3.0.10

r5      IN      A      20.3.0.1
pcl     IN      A      20.3.0.20
www     IN      CNAME  pcl
correo  IN      CNAME  pcl

```

```

GNU nano 3.2          /etc/bind/db.es.usal.redes          Modificado

$TTL 1d; ttl de permanencia en las caches
@ IN SOA dnsredes.redes.usal.es root.redes.usal.es (
    20170201; numero de serie
    ; redirix recomienda poner la fecha
    604800; Refresco 1 semana (Servidores secundarios)
    86400; Reintentto tras 1 dia
    2419200; Expira despues de 4 semanas
    1d) ; ttl de las respuestas negativas

; Configuracion de los servidores de nombres

    IN      NS      dnsredes.redes.usal.es.
dnsredes IN      A      20.3.0.10

; Configuracion de las maquinas
r5      IN      A      20.3.0.1
pcl     IN      A      20.3.0.20
www     IN      CNAME  pcl
correo  IN      CNAME  pcl

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt^J Justificar^C Posición
^X Salir   ^R Leer fich.^X Reemplazar^U Pegar txt ^T Ortografía^I Ir a línea

```

iv. Crea el archivo de zona de resolución inversa */etc/bind/db.0.3.20* como sigue:

```

$TTL 1d; ttl de permanencia en las cachEs
@ IN SOA dnsredes.redes.usal.es. root.redes.usal.es. (
    20170201; número de serie actualizar en cada cambio

```

```

; rediris recomienda poner la fecha
604800 ; Refresco 1 semana (servidores secundarios)
86400 ; Reintentos tras 1 día
2419200 ; Expira después de 4 semanas
1d) ; ttl de las respuestas negativas

IN NS dnsredes.redes.usal.es.

1 IN PTR r5.redes.usal.es.
20 IN PTR pc1.redes.usal.es.
10 IN PTR dnsredes.redes.usal.es.

GNU nano 3.2                               /etc/bind/db.0.3.20                         Modificado

$TTL 1d; ttl de permanencia en las caches
@ IN SOA dnsredes.redes.usal.es root.redes.usal.es (
    20170201; numero de serie
    ; rediris recomienda poner la fecha
    604800; Refresco 1 semana (Servidores secundarios)
    86400; Reintentos tras 1 dia
    2419200; Expira despues de 4 semanas
    1d) ; ttl de las respuestas negativas

; Configuración de los servidores de nombres

IN      NS      dnsredes.redes.usal.es.

; Configuración de las máquinas
1      IN      PTR      r5.redes.usal.es
20     IN      PTR      pc1.redes.usal.es.
10    IN      PTR      dnsredes.redes.usal.es.

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt^J Justificar^C Posición
^X Salir   ^R Leer^fich.^V Reemplazar^U Pegar txt ^T Ortografía^L Ir a línea

```

- v. Una vez configurado el servidor DNS, debemos indicarle que él mismo es su servidor DNS, lo cual se especifica en el archivo */etc/resolv.conf* como sigue:

```

domain redes.usal.es
nameserver 127.0.0.1

```

```

i0926305@lvdia01: ~          dnsredes           dnscom
GNU nano 3.2                               /etc/resolv.conf                         Modificado

domain redes.usal.es
nameserver 127.0.0.1

```

```

PC1> show ip

NAME      : PC1[1]
IP/MASK   : 20.3.0.20/16
GATEWAY   : 20.3.0.1
DNS       : 20.3.0.10
DOMAIN NAME : redes.usal.es
MAC       : 00:50:79:66:68:05
LPORT     : 10124
RHOST:PORT : 127.0.0.1:10125
MTU:      : 1500

```

Aquí se ve la configuración del PC1 con el dns predeterminado y el dominio correctamente puestos

En el resto de PCs de la red (*pc1, pc2, etc.*) indicaremos que el servidor DNS es el que acabamos de instalar (p. ej.: 20.3.0.10).

- vi. Configura adecuadamente nuestro servidor local para que alcance los DNS raíces. Incluye en el informe los ficheros de configuración.

```
root@lipcUR:~# cat /etc/bind/db.root
;
; This file holds the information on root name servers needed to
; initialize cache of Internet domain name servers
; (e.g. reference this file in the "cache . <file>" configuration
; file of BIND domain name servers).
;
; This file is made available by InterNIC
; under anonymous FTP as
;   file          /domain/named.cache
;   on server    FTP.INTERNIC.NET
; -OR-
;   file          RS.INTERNIC.NET
;
; last update: February 17, 2016
; related version of root zone: 2016021701
;
; formerly NS.INTERNIC.NET
; Establecimiento del dns raiz de la jerarquia
; dnsraiz          3600000      NS      dnsraiz.
; dnsraiz          3600000      A       198.41.0.4
; End of file
root@lipcUR:~#
```

Para ello tenemos que editar el fichero `/etc/bind/db.root` añadiendo en el mismo dos registros un NS con el nombre de `dnsraiz`. y el correspondiente A para la resolución del nombre

- vii. Ante de poner en marcha el servidor verifica que los ficheros de configuración son correctos con la orden: `named-checkconf`. Incluye la salida obtenida.

```
root@lipcUR:~# named-checkconf
root@lipcUR:~# echo $?
0
root@lipcUR:~#
```

La respuesta del comando `named-checkconf` no es ninguna por lo que no ha habido error pero para asegurarnos, si volcamos el contenido de la variable de entorno `$?` por pantalla obtenemos el valor 0 por lo que efectivamente sí que se ejecutado sin ningún error y por lo tanto no ha habido ningún error en la configuración.

- viii. Por último pon en marcha nuestro servidor de nombres ejecutando la siguiente orden: `service bind9 restart` o `/etc/init.d/bind9 restart`

```
root@lipcUR:~# service bind9 restart
root@lipcUR:~#
```

Comprueba que se ha arrancado correctamente con alguna de estas órdenes:

```
service bind9 status
systemctl status bind9.service
journalctl -xe
```

Incluye la salida de la orden utilizada.

```

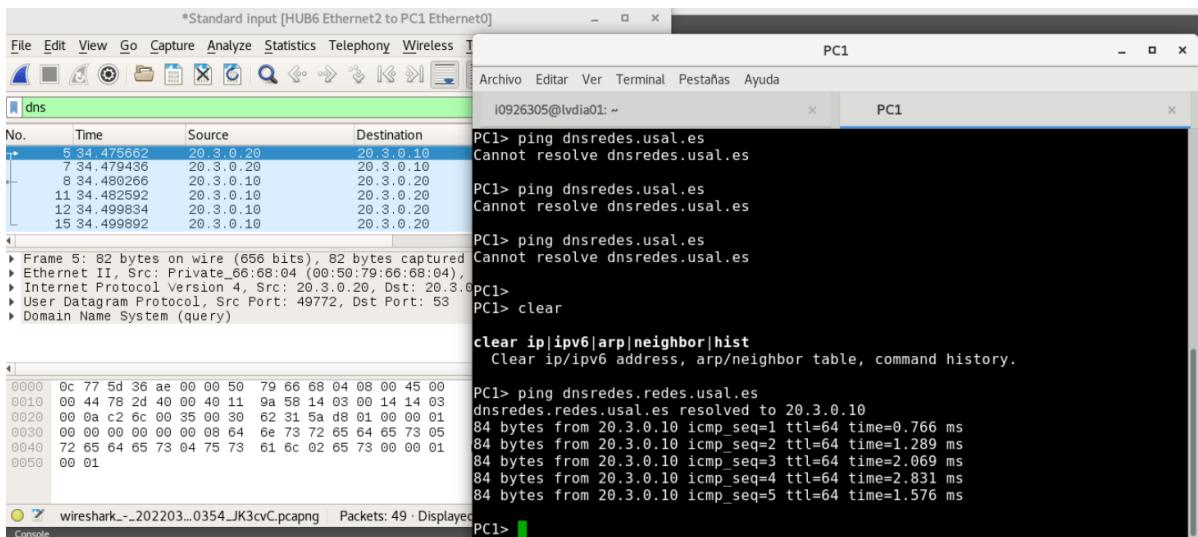
root@lipcUR:~# systemctl status bind9.service
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: en
   Active: active (running) since Thu 2022-03-17 17:55:30 CET; 1min 59s ago
     Docs: man:named(8)
 Process: 765 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS
 Main PID: 766 (named)
   Tasks: 4 (limit: 242)
  Memory: 13.5M
    CGroup: /system.slice/bind9.service
            └─766 /usr/sbin/named -u bind

mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
mar 17 17:57:25 lipcUR named[766]: network unreachable resolving '3.debian.pool.
lines 1-21/21 (END)

```

Hemos utilizado la orden `systemctl status bind9.service` con la que se muestra la imagen anterior en la que se puede ver con el servicio está cargado, habilitado y corriendo correctamente.

- c) Desde pc1 intenta resolver el nombre `dnsredes.redes.usal.es`. Especifica la orden que has utilizado y realiza las capturas de tráfico que consideres necesarias para obtener los mensajes de DNS que se generan en todo el esquema.



Se consigue resolver correctamente el nombre de “dnsredes.redes.usal.es” sin la perdida de paquetes en el transcurso del ping. Los mensajes DNS generados son los siguientes

```

7 34.479436 20.3.0.20 20.3.0.10 DNS 82 Standard query 0x5ad8 A dnsredes.redes.usal.es
8 34.480266 20.3.0.10 20.3.0.20 DNS 112 Standard query response 0x5ad8 A dnsredes.redes.usal.es A 20.3...
11 34.482592 20.3.0.10 20.3.0.20 DNS 112 Standard query response 0x5ad8 A dnsredes.redes.usal.es A 20.3...
12 34.499834 20.3.0.10 20.3.0.20 DNS 112 Standard query response 0x5ad8 A dnsredes.redes.usal.es A 20.3...
15 34.499892 20.3.0.10 20.3.0.20 DNS 112 Standard query response 0x5ad8 A dnsredes.redes.usal.es A 20.3...

Frame 7: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
Ethernet II, Src: ca:05:10:9a:00:38 (ca:05:10:9a:00:38), Dst: 0c:77:5d:36:ae:00 (0c:77:5d:36:ae:00)
Internet Protocol Version 4, Src: 20.3.0.20, Dst: 20.3.0.10
User Datagram Protocol, Src Port: 49772, Dst Port: 53
Domain Name System (query)
  Transaction ID: 0x5ad8
  Flags: 0x0100 Standard query
  Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  Queries
    dnsredes.redes.usal.es: type A, class IN
      Name: dnsredes.redes.usal.es
      [Name Length: 22]
      [Label Count: 4]
      Type: A (Host Address) (1)
      Class: IN (0x0001)

```

El mensaje que genera el terminal PC1 es un mensaje DNS preguntando por la IP del nombre “dnsredes.redes.usal.es” con destino a la IP 20.3.0.10 que es la del servidor DNS predeterminado que le hemos configurado anteriormente.

```

8 34.480266 20.3.0.10 20.3.0.20 DNS 112 Standard query response 0x5ad8 A dnsredes.redes.usal.es A 20.3...
11 34.482592 20.3.0.10 20.3.0.20 DNS 112 Standard query response 0x5ad8 A dnsredes.redes.usal.es A 20.3...
12 34.499834 20.3.0.10 20.3.0.20 DNS 112 Standard query response 0x5ad8 A dnsredes.redes.usal.es A 20.3...
15 34.499892 20.3.0.10 20.3.0.20 DNS 112 Standard query response 0x5ad8 A dnsredes.redes.usal.es A 20.3...

Ethernet II, Src: 0c:77:5d:36:ae:00 (0c:77:5d:36:ae:00), Dst: Private_66:68:04 (00:50:79:66:68:04)
Internet Protocol Version 4, Src: 20.3.0.10, Dst: 20.3.0.20
User Datagram Protocol, Src Port: 49772, Dst Port: 53
Domain Name System (response)
  Transaction ID: 0x5ad8
  Flags: 0x8580 Standard query response, No error
  Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  Queries
    dnsredes.redes.usal.es: type A, class IN
  Answers
    dnsredes.redes.usal.es: type A, class IN, addr 20.3.0.10

```

La respuesta del servidor DNS es un mensaje de DNS response con destino a la máquina PC1 en el que se especifica la resolución de la petición que en este caso era sí mismo por lo que no ha tenido que preguntar a nadie más para poder resolver la petición.

- d) Desde *dnsredes* intenta resolver la dirección IP obtenida en el apartado anterior. Especifica la orden que has utilizado y realiza las capturas de tráfico que consideres necesarias para obtener los mensajes de DNS que se generan en todo el esquema.

Como DNSredes es un servidor DNS y la ip que se pide resolver es en este caso la de la propia máquina no se genera ningún tráfico de mensajes DNS hacia la subred por lo que lanzando el analizador de red no se obtendría nada.

```

root@lipcUR:/var/cache/bind# ping 20.3.0.10
PING 20.3.0.10 (20.3.0.10) 56(84) bytes of data.
64 bytes from 20.3.0.10: icmp_seq=1 ttl=64 time=0.251 ms
64 bytes from 20.3.0.10: icmp_seq=2 ttl=64 time=0.328 ms
64 bytes from 20.3.0.10: icmp_seq=3 ttl=64 time=0.566 ms
64 bytes from 20.3.0.10: icmp_seq=4 ttl=64 time=0.729 ms
64 bytes from 20.3.0.10: icmp_seq=5 ttl=64 time=0.529 ms
64 bytes from 20.3.0.10: icmp_seq=6 ttl=64 time=0.818 ms
64 bytes from 20.3.0.10: icmp_seq=7 ttl=64 time=0.445 ms
64 bytes from 20.3.0.10: icmp_seq=8 ttl=64 time=0.649 ms
64 bytes from 20.3.0.10: icmp_seq=9 ttl=64 time=0.539 ms
^C
--- 20.3.0.10 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 21ms
rtt min/avg/max/mdev = 0.251/0.539/0.818/0.172 ms
root@lipcUR:/var/cache/bind#

```

Para obtener la resolución inversa de la ip tras realizar el ping se tiene que utilizar la orden *host 20.3.0.10*, con ella se muestra la información de la resolución inversa de esa IP

```

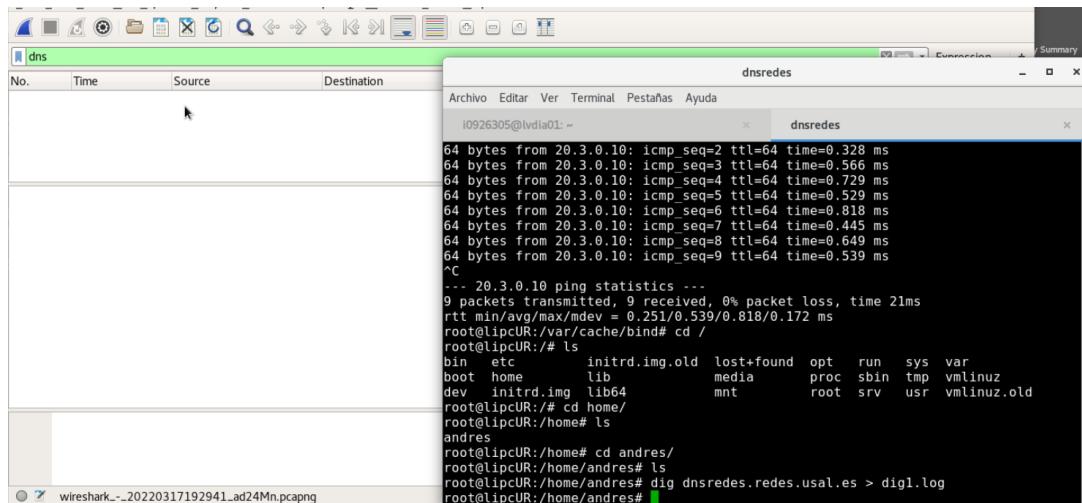
root@lipcUR:/var/cache/bind# host 20.3.0.10
10.0.3.20.in-addr.arpa domain name pointer dnsredes.redes.usal.es.
root@lipcUR:/var/cache/bind#

```

- e) Desde la máquina *dnsredes* ejecuta las órdenes (recuerda lanzar wireshark en el lugar adecuado para capturar el tráfico generado):

```
dig dnsredes.redes.usal.es (anota el tiempo de respuesta)
dig dnsredes.redes.usal.es (anota el tiempo de respuesta)
```

¿Qué mensajes DNS se han generado? ¿Por qué? Muestra y analiza cada mensaje con la ayuda de wireshark. ¿Ha mejorado el tiempo de respuesta entre la primera pregunta y su repetición? ¿Por qué?



Tras realizar el primer dig se observa que no se ha generado ningún mensaje DNS que haya podido captar el analizador de red situado en el enlace desde DNSredes hasta el hub

```
; <>>> DiG 9.11.5-P4-5.1+deb10u6-Debian <>>> dnsredes.redes.usal.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 27214
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7b8f7477aff8526df3e221156233702aea07ad3563637970 (good)
;; QUESTION SECTION:
;dnsredes.redes.usal.es.           IN      A

;; ANSWER SECTION:
dnsredes.redes.usal.es. 86400   IN      A      20.3.0.10

;; AUTHORITY SECTION:
redes.usal.es.          86400   IN      NS     dnsredes.redes.usal.es.

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: jue mar 17 18:30:18 CET 2022
;; MSG SIZE  rcvd: 109
```

El log generado por el dig muestra que en efecto no se ha podido detectar nada porque el tiempo de ejecución ha sido de 1 msec por lo que no ha dado tiempo a que se pueda recoger nada desde el wireshark.

```

dns
No. Time Source Destination
1 17:30:18.000000000 +0000 dnsredes
Archivo Editar Ver Terminal Pestañas Ayuda
i0926305@lvdia01: ~ dnsredes
:; global options: +cmd
:; Got answer:
:; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 27214
:; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
:; OPT PSEUDOSECTION:
: EDNS: version: 0, flags: udp: 4096
: COOKIE: 7b8f7477aff8526df3e221156233702aea07ad3563637970 (good)
: QUESTION SECTION:
:dnsredes.redes.usal.es. IN A
:; ANSWER SECTION:
dnsredes.redes.usal.es. 86400 IN A 20.3.0.10
:; AUTHORITY SECTION:
redes.usal.es. 86400 IN NS dnsredes.redes.usal.es.
:; Query time: 1 msec
:; SERVER: 127.0.0.1#53(127.0.0.1)
:; WHEN: jue mar 17 18:30:18 CET 2022
:; MSG SIZE rcvd: 109
root@lipcUR:/home/andres# dig dnsredes.redes.usal.es > dig2.log
root@lipcUR:/home/andres#

```

Al igual que en el caso anterior no se ha detectado ningún mensaje de DNS

```

i0926305@lvdia01: ~ dnsredes
:; <>> DiG 9.11.5-P4-5.1+deb10u6-Debian <>> dnsredes.redes.usal.es
:; global options: +cmd
:; Got answer:
:; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 46965
:; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
:; OPT PSEUDOSECTION:
: EDNS: version: 0, flags: udp: 4096
: COOKIE: 6cca5783bd1a0db73c73ef816233712ffe08c738a829b587 (good)
:; QUESTION SECTION:
:dnsredes.redes.usal.es. IN A
:; ANSWER SECTION:
dnsredes.redes.usal.es. 86400 IN A 20.3.0.10
:; AUTHORITY SECTION:
redes.usal.es. 86400 IN NS dnsredes.redes.usal.es.
:; Query time: 2 msec
:; SERVER: 127.0.0.1#53(127.0.0.1)
:; WHEN: jue mar 17 18:34:39 CET 2022
:; MSG SIZE rcvd: 109
root@lipcUR:/home/andres#

```

Y en el log generado no se observa mejora en el tiempo de respuesta porque aunque haya aumentado un milisegundo la respuesta es prácticamente inmediata

- f) Modifica los ficheros necesarios en los servidores de dns para que desde cualquier equipo se puedan resolver nombres del dominio redes.usal.es (resolución directa e inversa). Incluye los ficheros nuevos y modificados necesarios. Realiza y documenta las pruebas necesarias para verificar el correcto funcionamiento.

```

root@dnsusal:~# cat /etc/bind/db.es.usal
$TTL 3h ; ttl de permanencia en las cachEs
@ IN SOA dnsusal.usal.es. root.dnsusal.usal.es. (
    20220101 ; Numero de serie
    28800    ; Refresco despues de 8 horas
    7200     ; Reintentos despues de 2 horas
    604800   ; Expiracion despues de 1 semana
    3h       ; ttl de las respuestas negativas
)

; Configuracion de los servidores de nombres
IN NS dnsusal.usal.es.
dnsusal IN A 20.1.0.10

; Configuracion de las maquinas
r1 IN A 20.1.0.1
portal IN A 20.1.0.20
roble IN A 20.1.0.30
www IN CNAME portal
diaweb IN CNAME roble
informatica IN CNAME roble

; Configuracion del dominio redes.usal.es
redes.usal.es. IN NS dnsredes.redes.usal.es.
dnsredes.redes.usal.es IN A 20.3.0.10

; Configuracion del dominio redes.usal.es mediante resolucion inversa
3.20.in-addr.arpa. IN NS dnsredes.redes.usal.es.
root@dnsusal:~#

```

Para que se pueda resolver el problema hay que incorporar el nuevo dominio a la jerarquía y como redes.usal.es es un subdominio de usal.es, el servidor dns responsable de que se pueda llegar a ello es el servidor DNSusal por lo que hay que modificar su fichero “db.usal.es” añadiendo las líneas que aparecen en la imagen de arriba, para la resolución directa del dominio se necesitan dos registro, un NS para asociar el dominio redes.usal.es al servidor responsable del mismo y el registro A que es el que realiza la correspondencia del nombre con la IP que en este caso es dnsredes.redes.usal.es → 20.3.0.10.

Y para la resolución inversa solo se necesita el registro NS que resuelva la IP inversa de IPv4 con el nombre del servidor del dominio dnsredes.redes.usal.es

Para comprobar el correcto funcionamiento de la resolución de nombres vamos a realizar dos pings uno desde la subred hacia fuera y otro desde fuera hacia la subred, y con wireshark vamos a analizar los mensajes DNS que se han generado.

Antes de realizar el ping haremos un ‘service bind9 restart’ en todos los DNS para asegurarnos de restaurar su caché y así asegurarnos de que no usaran alguna correspondencia almacenada previamente.

PC1

Archivo Editar Ver Terminal Pestañas Ayuda

PC1 dnsredes dnsusal dnses

```

PC1> ping www.cisco.com
www.cisco.com resolved to 30.1.0.20
www.cisco.com icmp_seq=1 timeout
www.cisco.com icmp_seq=2 timeout
84 bytes from 30.1.0.20 icmp_seq=3 ttl=59 time=85.285 ms
84 bytes from 30.1.0.20 icmp_seq=4 ttl=59 time=68.968 ms
84 bytes from 30.1.0.20 icmp_seq=5 ttl=59 time=93.092 ms

PC1>

```

Desde PC1 → *ping www.cisco.com*

Para ello vamos a lanzar el analizador de red en el enlace que une el HUB 6 con R5, en este caso daría igual lanzarlo en cualquiera de los enlaces del hub porque este reenvía todos las tramas que le llegan menos por la que le ha llegado, este procedimiento cambiaría si en vez de un hub tuviésemos un switch.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	20.3.0.20	20.3.0.10	DNS	73	Standard query 0x4dd6 A www.cisco.com
2	0.003196	20.3.0.10	198.41.0.4	DNS	112	Standard query 0x6d8c A www.cisco.com OPT
4	0.009940	20.3.0.20	20.3.0.10	DNS	73	Standard query 0x4dd6 A www.cisco.com

Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
 ▶ Ethernet II, Src: Private_66:68:04 (00:50:79:66:68:04), Dst: 0c:77:5d:36:ae:00 (0c:77:5d:36:ae:00)
 ▶ Internet Protocol Version 4, Src: 20.3.0.20, Dst: 20.3.0.10
 ▶ User Datagram Protocol, Src Port: 35708, Dst Port: 53
 ▶ Domain Name System (query)
 Transaction ID: 0x4dd6
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 ▶ Queries
 ▼ www.cisco.com: type A, class IN
 Name: www.cisco.com
 [Name Length: 13]
 [Label Count: 3]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 [Response In: 10]

El terminal PC1 con IP (20.3.0.10) pregunta a su servidor DNS predeterminado el parámetro especificado en una DNS Query.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	20.3.0.20	20.3.0.10	DNS	73	Standard query 0x4dd6 A www.cisco.com
2	0.003196	20.3.0.10	198.41.0.4	DNS	112	Standard query 0x6d8c A www.cisco.com OPT
3	4.009940	20.3.0.20	20.3.0.10	DNS	73	Standard query 0x4dd6 A www.cisco.com
Frame 2: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface 0						
Ethernet II, Src: 0c:77:5d:36:ae:00 (0c:77:5d:36:ae:00), Dst: ca:05:10:9a:00:38 (ca:05:10:9a:00:38)						
Internet Protocol Version 4, Src: 20.3.0.10, Dst: 198.41.0.4						
User Datagram Protocol, Src Port: 56837, Dst Port: 53						
Domain Name System (query)						
Transaction ID: 0x6d8c						
Flags: 0x0010 Standard query						
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						
Additional RRs: 1						
Queries						
www.cisco.com: type A, class IN						
Name: www.cisco.com						
[Name Length: 13]						
[Label Count: 3]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Additional records						
<Root>: type OPT						
Name: <Root>						
Type: OPT (41)						
UDP payload size: 4096						
Higher bits in extended RCODE: 0x00						
EDNS0 version: 0						
Z: 0x8000						
1..... = DO bit: Accepts DNSSEC security RRs						
000 0000 0000 0000 = Reserved: 0x0000						
Data length: 28						
Option: COOKIE						
[Response In: 5]						

Seguidamente como DNSredes no es el responsable del dominio tiene que preguntar a su DNS raíz (198.41.0.4) sobre el servidor que es el responsable del dominio "cisco.com"

No.	Time	Source	Destination	Protocol	Length	Info
1	5.091047	198.41.0.4	20.3.0.10	DNS	149	Standard query response 0x6d8c A www.cisco.com NS dnscom.com A 30.0.0.10...
2	6.096629	20.3.0.10	30.0.0.10	DNS	96	Standard query 0x4b52 A www.cisco.com OPT
3	7.0174921	30.0.0.10	20.3.0.10	DNS	151	Standard query response 0x4b52 A www.cisco.com NS dnscisco.cisco.com A 3...
Frame 5: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0						
Ethernet II, Src: ca:05:10:9a:00:38 (ca:05:10:9a:00:38), Dst: 0c:77:5d:36:ae:00 (0c:77:5d:36:ae:00)						
Internet Protocol Version 4, Src: 05:10:9a:00:38, Dst: 198.41.0.4						
User Datagram Protocol, Src Port: 56837, Dst Port: 53						
Domain Name System (response)						
Transaction ID: 0x6d8c						
Flags: 0x8000 Standard query response, No error						
Questions: 1						
Answer RRs: 0						
Authority RRs: 1						
Additional RRs: 2						
Queries						
www.cisco.com: type A, class IN						
Name: www.cisco.com						
[Name Length: 13]						
[Label Count: 3]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Authoritative nameservers						
com: type NS, class IN, ns dnscom.com						
Name: com						
Type: NS (authoritative Name Server) (2)						
Class: IN (0x0001)						
Time to live: 14400 (4 hours)						
Data length: 9						
Name Server: dnscom.com						
Additional records						
dnscom.com: type A, class IN, addr 30.0.0.10						
Name: dnscom.com						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Time to live: 14400 (4 hours)						
Data length: 4						
Address: 30.0.0.10						
<Root>: type OPT						
Name: <Root>						
Type: OPT (41)						
UDP payload size: 4096						
Higher bits in extended RCODE: 0x00						
EDNS0 version: 0						
Z: 0x0000						
0..... = DO bit: Cannot handle DNSSEC security RRs						
000 0000 0000 0000 = Reserved: 0x0000						
Data length: 28						
Option: COOKIE						
[Request In: 2]						

El DNSraíz tampoco es el responsable del dominio en cuestión, pero al ser el servidor raíz de la jerarquía conoce todos los servidores DNS que están un nivel por debajo en la jerarquía haciendo posible en este caso el encaminamiento hacia el DNScom, enviando en el DNS query response el registro A asociado a ese servidor que incluye el nombre del servidor y la IP del mismo en este caso es 30.0.0.10.

No.	Time	Source	Destination	Protocol	Length	Info
5	0.091047	198.41.0.4	20.3.0.10	DNS	149	Standard query response 0x6d8c A www.cisco.com NS dnscom.com A 30.0.0.10...
6	0.096629	20.3.0.10	30.0.0.10	DNS	96	Standard query 0x4b52 A www.cisco.com OPT
Frame 6: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0						
Ethernet II, Src: 0c:77:5d:36:ae:00 (0c:77:5d:36:ae:00), Dst: ca:05:10:9a:00:38 (ca:05:10:9a:00:38)						
Internet Protocol Version 4, Src: 20.3.0.10, Dst: 30.0.0.10						
User Datagram Protocol, Src Port: 46422, Dst Port: 53						
Domain Name System (query)						
Transaction ID: 0x4b52						
Flags: 0x0010 Standard query						
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						
Additional RRs: 1						
Queries						
www.cisco.com: type A, class IN						
Name: www.cisco.com						
[Name Length: 13]						
[Label Count: 3]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Additional records						
<Root>: type OPT						
Name: <Root>						
Type: OPT (41)						
UDP payload size: 512						
Higher bits in extended RCODE: 0x00						
EDNS version: 0						
Z: 0x8000						
1..... = DO bit: Accepts DNSSEC security RRs						
000 0000 0000 0000 = Reserved: 0x0000						
Data length: 12						
Option: COOKIE						
[Response In: 7]						

El siguiente mensaje generado es el DNS query hacia el servidor nuevo desde DNSusal, preguntando por “www.cisco.com”

No.	Time	Source	Destination	Protocol	Length	Info
7	0.174921	30.0.0.10	20.3.0.10	DNS	151	Standard query response 0x4b52 A www.cisco.com NS dnsCisco.cisco.com A 3...
8	0.179911	20.3.0.10	30.0.0.2	DNS	96	Standard query 0x9713 A www.cisco.com OPT
9	0.255662	30.0.0.2	20.3.0.10	DNS	105	Standard query response 0x9713 A www.cisco.com A 30.1.0.10 A 30.1.0.20
Frame 7: 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits) on interface 0						
Ethernet II, Src: 0c:77:5d:36:ae:00 (0c:77:5d:36:ae:00), Dst: 0c:77:5d:36:ae:00 (0c:77:5d:36:ae:00)						
Internet Protocol Version 4, Src: 30.0.0.10, Dst: 20.3.0.10						
User Datagram Protocol, Src Port: 46422, Dst Port: 53						
Domain Name System (response)						
Transaction ID: 0x4b52						
Flags: 0x0000 Standard query response, No error						
Questions: 1						
Answer RRs: 0						
Authority RRs: 1						
Additional RRs: 2						
Queries						
www.cisco.com: type A, class IN						
Name: www.cisco.com						
[Name Length: 13]						
[Label Count: 3]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Authoritative nameservers						
cisco.com: type NS, class IN, ns dnsCisco.cisco.com						
Name: cisco.com						
Type: NS (authoritative Name Server) (2)						
Class: IN (0x0001)						
Time to live: 7200 (2 hours)						
Data length: 11						
Name Server: dnsCisco.cisco.com						
Additional records						
dnsCisco.cisco.com: type A, class IN, addr 30.0.0.2						
Name: dnsCisco.cisco.com						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Time to live: 7200 (2 hours)						
Data length: 4						
Address: 30.0.0.2						
<Root>: type OPT						
Name: <Root>						
Type: OPT (41)						
UDP payload size: 4096						
Higher bits in extended RCODE: 0x00						
EDNS version: 0						
Z: 0x0000						
0.... = DO bit: Cannot handle DNSSEC security RRs						
000 0000 0000 0000 = Reserved: 0x0000						
Data length: 28						
Option: COOKIE						
[Request In: 6]						

DNScom tampoco es el responsable del dominio en cuestión, pero tiene un servidor DNS en sus registros que es responsable de esa parte del dominio. Por lo que en el DNS query response le va a enviar la correspondiente información de DNScisco (IP: 30.0.0.2)

No.	Time	Source	Destination	Protocol	Length	Info
7	0.174921	30.0.0.10	20.3.0.10	DNS	151	Standard query response 0x4b52 A www.cisco.com NS dnsCisco.cisco.com A 3...
8	0.179011	20.3.0.10	30.0.0.2	DNS	96	Standard query 0x9713 A www.cisco.com OPT
9	0.255662	30.0.0.2	20.3.0.10	DNS	105	Standard query response 0x9713 A www.cisco.com A 30.1.0.10 A 30.1.0.20
Frame 8: 96 bytes on wire (768 bits), 96 bytes captured (768 bits) on interface 0						
Ethernet II, Src: 0c:77:5d:36:ae:00 (0c:77:5d:36:ae:00), Dst: ca:05:10:9a:00:38 (ca:05:10:9a:00:38)						
Internet Protocol Version 4, Src: 20.3.0.10, Dst: 30.0.0.2						
User Datagram Protocol, Src Port: 41349, Dst Port: 53						
Domain Name System (query)						
Transaction ID: 0x9713						
Flags: 0x0010 Standard query						
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						
Additional RRs: 1						
Queries						
www.cisco.com: type A, class IN						
Name: www.cisco.com						
[Name Length: 13]						
[Label Count: 3]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Additional records						
<Root>: type OPT						
Name: <Root>						
Type: OPT (41)						
UDF payload size: 512						
Higher bits in extended RCODE: 0x00						
EDNS version: 0						
Z: 0x8000						
1.... = DO bit: Accepts DNSSEC security RRs						
000 0000 0000 0000 = Reserved: 0x0000						
Data length: 12						
Option: COOKIE						
[Response In: 9]						

El siguiente mensaje generado es el DNS query hacia el servidor nuevo desde DNScisco, preguntando por “www.cisco.com”

No.	Time	Source	Destination	Protocol	Length	Info
9	0.255662	30.0.0.2	20.3.0.10	DNS	105	Standard query response 0x9713 A www.cisco.com A 30.1.0.10 A 30.1.0.20
10	0.257533	20.3.0.10	20.3.0.20	DNS	144	Standard query response 0x4dd6 A www.cisco.com A 30.1.0.20 A 30.1.0.10 N...
12	0.265770	20.3.0.10	20.3.0.20	DNS	144	Standard query response 0x4dd6 A www.cisco.com A 30.1.0.20 A 30.1.0.10 N...
Frame 9: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0						
Ethernet II, Src: ca:05:10:9a:00:38 (ca:05:10:9a:00:38), Dst: 0c:77:5d:36:ae:00 (0c:77:5d:36:ae:00)						
Internet Protocol Version 4, Src: 20.3.0.10, Dst: 30.0.0.2						
User Datagram Protocol, Src Port: 41349, Dst Port: 53						
Domain Name System (response)						
Transaction ID: 0x9713						
Flags: 0x08580 Standard query response, No error						
Questions: 1						
Answer RRs: 2						
Authority RRs: 0						
Additional RRs: 0						
Queries						
www.cisco.com: type A, class IN						
Name: www.cisco.com						
[Name Length: 13]						
[Label Count: 3]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Answers						
www.cisco.com: type A, class IN, addr 30.1.0.10						
Name: www.cisco.com						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Time to live: 10 (10 seconds)						
Data length: 4						
Address: 30.1.0.10						
www.cisco.com: type A, class IN, addr 30.1.0.20						
Name: www.cisco.com						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Time to live: 10 (10 seconds)						
Data length: 4						
Address: 30.1.0.20						
[Request In: 8]						
[Time: 0.075751000 seconds]						

Finalmente DNScisco es el responsable del dominio “cisco.com” por lo que tiene la capacidad para resolver el nombre pedido desde el principio, como en la configuración de DNScisco introducimos un balanceo hacia el nombre “[www.cisco.com](#)”, DNScisco le envía los nombres y las IPs asociadas cuando se configuró el servidor

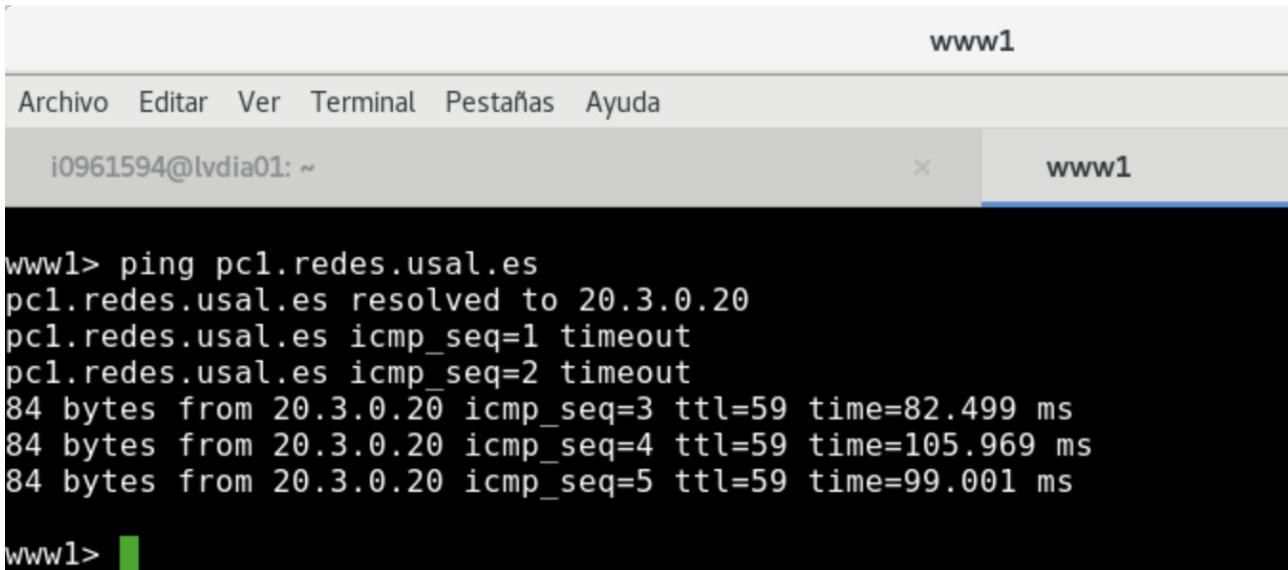
No.	Time	Source	Destination	Protocol	Length	Info
8	0.179911	20.3.0.10	30.0.0.2	DNS	96	Standard query 0x9713 A www.cisco.com OPT
9	0.255662	30.0.0.2	20.3.0.10	DNS	105	Standard query response 0x9713 A www.cisco.com A 30.1.0.10 A 30.1.0.20
10	0.257538	20.3.0.10	20.3.0.20	DNS	144	Standard query response 0x4dd6 A www.cisco.com A 30.1.0.20 A 30.1.0.10 N...
► Frame 10: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0						
► Ethernet II, Src: PC1 (0c:77:5d:36:ae:00) (0c:77:5d:36:ae:00), Dst: Private_66:68:04 (00:50:79:66:68:04)						
► Internet Protocol Version 4, Src: 20.3.0.10, Dst: 20.3.0.20						
► User Datagram Protocol, Src Port: 53, Dst Port: 35708						
► Domain Name System (response)						
Transaction ID: 0x4dd6						
Flags: 0x8180 Standard query response, No error						
Questions: 1						
Answer RRs: 2						
Authority RRs: 1						
Additional RRs: 1						
Queries						
www.cisco.com: type A, class IN						
Name: www.cisco.com						
[Name Length: 13]						
[Label Count: 3]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Time to live: 10 (10 seconds)						
Data length: 4						
Address: 30.1.0.20						
www.cisco.com: type A, class IN, addr 30.1.0.20						
Name: www.cisco.com						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Time to live: 10 (10 seconds)						
Data length: 4						
Address: 30.1.0.10						
Authoritative nameservers						
cisco.com: type NS, class IN, ns dnsCisco.cisco.com						
Name: cisco.com						
Type: NS (authoritative Name Server) (2)						
Class: IN (0x0001)						
Time to live: 7200 (2 hours)						
Data length: 11						
Name Server: dnsCisco.cisco.com						
Additional records						
dnsCisco.cisco.com: type A, class IN, addr 30.0.0.2						
Name: dnsCisco.cisco.com						
Type: A (Host Address) (1)						
Class: IN (0x0001)						

Una vez que se ha obtenido la información el DNSusal, le envía la información a PC1 completando así la resolución de los nombres y posteriormente pudiendo completar el ping realizando la secuencia de mensajes ICMP

Volvemos a borrar las cachés de todos los DNSs, para que se tengan que volver a hacer todas las correspondencias y apreciar debidamente todos los mensajes generados.

Desde www1 → ping pc1.redes.usal.es

Para ello vamos a lanzar el analizador de red 1 en el enlace que une el HUB5 con R4 y el analizador de red 2 en el enlace entre HUB4 con R4.



```
i0961594@lvdia01: ~
```

```
www1> ping pc1.redes.usal.es
pc1.redes.usal.es resolved to 20.3.0.20
pc1.redes.usal.es icmp_seq=1 timeout
pc1.redes.usal.es icmp_seq=2 timeout
84 bytes from 20.3.0.20 icmp_seq=3 ttl=59 time=82.499 ms
84 bytes from 20.3.0.20 icmp_seq=4 ttl=59 time=105.969 ms
84 bytes from 20.3.0.20 icmp_seq=5 ttl=59 time=99.001 ms
```

```
www1>
```

No.	Time	Source	Destination	Protocol	Length	Info
68	24.743130	30.0.0.2	30.0.0.10	DNS	77	Standard query 0x8aeb A pc1.redes.usal.es
69	24.748706	30.0.0.10	198.41.0.4	DNS	116	Standard query 0xf4cf A pc1.redes.usal.es OPT
70	24.763319	198.41.0.4	30.0.0.10	DNS	152	Standard query response 0xf4cf A pc1.redes.usal.es NS dnses.es A 20.0.0.10 OPT

Frame 68: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
Ethernet II, Src: ca:04:07:04:00:00 (ca:04:07:04:00:00), Dst: 0c:77:5d:0e:02:00 (0c:77:5d:0e:02:00)
Internet Protocol Version 4, Src: 30.0.0.2, Dst: 30.0.0.10
User Datagram Protocol, Src Port: 53, Dst Port: 53
Domain Name System (query)
 Transaction ID: 0x8aeb
 Flags: 0x0100 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 0
 Queries
 pc1.redes.usal.es: type A, class IN
[Response In: 77]

El terminal www1 (IP: 30.0.0.2) pregunta a su servidor DNS predeterminado el parámetro especificado en una DNS Query.

No.	Time	Source	Destination	Protocol	Length	Info
68	24.743130	30.0.0.2	30.0.0.10	DNS	77	Standard query 0x8aeb A pc1.redes.usal.es
69	24.748706	30.0.0.10	198.41.0.4	DNS	116	Standard query 0xf4cf A pc1.redes.usal.es OPT
70	24.763319	198.41.0.4	30.0.0.10	DNS	152	Standard query response 0xf4cf A pc1.redes.usal.es NS dnses.es A 20.0.0.10 OPT

Frame 69: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface 0
Ethernet II, Src: 0c:77:5d:0e:02:00 (0c:77:5d:0e:02:00), Dst: ca:03:06:f4:00:38 (ca:03:06:f4:00:38)
Internet Protocol Version 4, Src: 30.0.0.10, Dst: 198.41.0.4
User Datagram Protocol, Src Port: 57964, Dst Port: 53
Domain Name System (query)
 Transaction ID: 0xf4cf
 Flags: 0x0010 Standard query
 Questions: 1
 Answer RRs: 0
 Authority RRs: 0
 Additional RRs: 1
 Queries
 pc1.redes.usal.es: type A, class IN
 Name: pc1.redes.usal.es
 [Name Length: 17]
 [Label Count: 4]
 Type: A (Host Address) (1)
 Class: IN (0x0001)
 Additional records
 <Root>: type OPT
[Response In: 70]

Seguidamente como DNScisco no es el responsable del dominio tiene que preguntar a su DNS raíz (198.41.0.4) sobre el servidor que es el responsable del dominio "redes.usal.es"

No.	Time	Source	Destination	Protocol	Length	Info
68	24.743130	30.0.0.2	30.0.0.10	DNS	77	Standard query 0x8aeb A pc1.redes.usal.es
69	24.748706	30.0.0.10	198.41.0.4	DNS	116	Standard query 0xf4cf A pc1.redes.usal.es OPT
70	24.763519	198.41.0.4	30.0.0.10	DNS	152	Standard query response 0xf4cf A pc1.redes.usal.es NS dnses.es A 20.0.0.10 OPT
<p>► Frame 70: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface 0 ► Ethernet II, Src: ca:03:06:f4:00:38 (ca:03:06:f4:00:38), Dst: 0c:77:5d:0e:02:00 (0c:77:5d:0e:02:00) ► Internet Protocol Version 4, Src: 198.41.0.4, Dst: 30.0.0.10 ► User Datagram Protocol, Src Port: 53, Dst Port: 57964 ▾ Domain Name System (response) Transaction ID: 0xf4cf ► Flags: 0x8000 Standard query response, No error Questions: 1 Answer RRs: 0 Authority RRs: 1 Additional RRs: 2 ▾ Queries ► pc1.redes.usal.es: type A, class IN Name: pc1.redes.usal.es [Name Length: 17] [Label Count: 4] Type: A (Host Address) (1) Class: IN (0x0001) ▾ Authoritative nameservers ► es: type NS, class IN, ns dnses.es Name: es Type: NS (authoritative Name Server) (2) Class: IN (0x0001) Time to live: 14400 (4 hours) Data length: 8 Name Server: dnses.es ▾ Additional records ► dnses.es: type A, class IN, addr 20.0.0.10 Name: dnses.es Type: A (Host Address) (1) Class: IN (0x0001) Time to live: 14400 (4 hours) Data length: 4 Address: 20.0.0.10 ► <Root>: type OPT [Request In: 69] [Time: 0.014613000 seconds]</p>						

El DNSraíz tampoco es el responsable del dominio en cuestión, pero al ser el servidor raíz de la jerarquía conoce todos los servidores DNS que están un nivel por debajo en la jerarquía haciendo posible en este caso el encaminamiento hacia el DNScom, enviando en el DNS query response el registro A asociado a ese servidor que incluye el nombre del servidor y la IP del mismo en este caso es 20.0.0.10.

No.	Time	Source	Destination	Protocol	Length	Info
71	24.769121	30.0.0.10	20.0.0.10	DNS	100	Standard query 0x33f8 A pc1.redes.usal.es OPT
72	24.803647	20.0.0.10	30.0.0.10	DNS	154	Standard query response 0x33f8 A pc1.redes.usal.es NS dnsusal.usal.es A 20.1.0...
73	24.810147	30.0.0.10	20.1.0.10	DNS	100	Standard query 0x0f89 A pc1.redes.usal.es OPT
<p>► Frame 71: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0 ► Ethernet II, Src: 0c:77:5d:0e:02:00 (0c:77:5d:0e:02:00), Dst: ca:03:06:f4:00:38 (ca:03:06:f4:00:38) ► Internet Protocol Version 4, Src: 30.0.0.10, Dst: 20.0.0.10 ► User Datagram Protocol, Src Port: 34612, Dst Port: 53 ▾ Domain Name System (query) Transaction ID: 0x33f8 ► Flags: 0x0010 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 1 ▾ Queries ► pc1.redes.usal.es: type A, class IN Name: pc1.redes.usal.es [Name Length: 17] [Label Count: 4] Type: A (Host Address) (1) Class: IN (0x0001) ▾ Additional records ► <Root>: type OPT [Response In: 72]</p>						

El siguiente mensaje generado es el DNS query hacia el servidor nuevo desde DNScom, preguntando por “pc1.redes.usal.es”

No.	Time	Source	Destination	Protocol	Length	Info
71	24.769121	30.0.0.10	20.0.0.10	DNS	100	Standard query 0x33f8 A pc1.redes.usal.es OPT
72	24.803647	20.0.0.10	30.0.0.10	DNS	154	Standard query response 0x33f8 A pc1.redes.usal.es NS dnsusal.usal.es A 20.1.0...
73	24.810147	30.0.0.10	20.1.0.10	DNS	100	Standard query 0x0f89 A pc1.redes.usal.es OPT
▶ Frame 72: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits) on interface 0 ▶ Ethernet II, Src: ca:03:06:f4:00:38 (ca:03:06:f4:00:38), Dst: 0c:77:5d:0e:02:00 (0c:77:5d:0e:02:00) ▶ Internet Protocol Version 4, Src: 20.0.0.10, Dst: 30.0.0.10 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 34612 ▶ Domain Name System (response) Transaction ID: 0x33f8 Flags: 0x8000 Standard query response, No error Questions: 1 Answer RRs: 0 Authority RRs: 1 Additional RRs: 2 Queries pc1.redes.usal.es: type A, class IN Name: pc1.redes.usal.es [Name Length: 17] [Label Count: 4] Type: A (Host Address) (1) Class: IN (0x0001) Authoritative nameservers usal.es: type NS, class IN, ns dnsusal.usal.es Name: usal.es Type: NS (authoritative Name Server) (2) Class: IN (0x0001) Time to live: 3600 (1 hour) Data length: 10 Name Server: dnsusal.usal.es Additional records dnsusal.usal.es: type A, class IN, addr 20.1.0.10 Name: dnsusal.usal.es Type: A (Host Address) (1) Class: IN (0x0001) Time to live: 3600 (1 hour) Data length: 4 Address: 20.1.0.10 <Root>: type OPT [Request In: 71] [Time: 0.034526000 seconds]						

DNSes tampoco es el responsable del dominio en cuestión, pero tiene un servidor DNS en sus registros que es responsable de esa parte del dominio. Por lo que en el DNS query response le va a enviar la correspondiente información de DNSusal (IP: 20.1.0.10)

No.	Time	Source	Destination	Protocol	Length	Info
71	24.769121	30.0.0.10	20.0.0.10	DNS	100	Standard query 0x33f8 A pc1.redes.usal.es OPT
72	24.803647	20.0.0.10	30.0.0.10	DNS	154	Standard query response 0x33f8 A pc1.redes.usal.es NS dnsusal.usal.es A 20.1.0...
73	24.810147	30.0.0.10	20.1.0.10	DNS	100	Standard query 0x0f89 A pc1.redes.usal.es OPT
▶ Frame 73: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0 ▶ Ethernet II, Src: 0c:77:5d:0e:02:00 (0c:77:5d:0e:02:00), Dst: ca:03:06:f4:00:38 (ca:03:06:f4:00:38) ▶ Internet Protocol Version 4, Src: 30.0.0.10, Dst: 20.1.0.10 ▶ User Datagram Protocol, Src Port: 32882, Dst Port: 53 ▶ Domain Name System (query) Transaction ID: 0x0f89 Flags: 0x0010 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 1 Queries pc1.redes.usal.es: type A, class IN Name: pc1.redes.usal.es [Name Length: 17] [Label Count: 4] Type: A (Host Address) (1) Class: IN (0x0001) Additional records <Root>: type OPT Name: <Root> Type: OPT (41) UDP payload size: 512 Higher bits in extended RCODE: 0x00 EDNS0 version: 0 Z: 0x8000 1... = DO bit: Accepts DNSSEC security RRs 0 = Reserved: 0x0000 Data length: 12 > Option: COOKIE [Response In: 74]						

El siguiente mensaje generado es el DNS query hacia el servidor nuevo desde DNScom, preguntando por “pc1.redes.usal.es”

No.	Time	Source	Destination	Protocol	Length	Info
74	24.864105	20.1.0.10	30.0.0.10	DNS	155	Standard query response 0x0f89 A pc1.redes.usal.es NS dnsredes.redes.usal.es A ...
75	24.868765	30.0.0.10	20.3.0.10	DNS	100	Standard query 0x6664 A pc1.redes.usal.es OPT
76	24.934863	20.3.0.10	30.0.0.10	DNS	132	Standard query response 0x6664 A pc1.redes.usal.es A 20.3.0.20 OPT
▶ Frame 74: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits) on interface 0						
▶ Ethernet II, Src: ca:03:06:f4:00:38 (ca:03:06:f4:00:38), Dst: 0c:77:5d:0e:02:00 (0c:77:5d:0e:02:00)						
▶ Internet Protocol Version 4, Src: 20.1.0.10, Dst: 30.0.0.10						
▶ User Datagram Protocol, Src Port: 53, Dst Port: 32882						
▶ Domain Name System (response)						
Transaction ID: 0x0f89						
Flags: 0x8000 Standard query response, No error						
Questions: 1						
Answer RRs: 0						
Authority RRs: 1						
Additional RRs: 2						
Queries						
pc1.redes.usal.es: type A, class IN						
Name: pc1.redes.usal.es						
[Name Length: 17]						
[Label Count: 4]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Authoritative nameservers						
redes.usal.es: type NS, class IN, ns dnsredes.redes.usal.es						
Name: redes.usal.es						
Type: NS (authoritative Name Server) (2)						
Class: IN (0x0001)						
Time to live: 108000 (3 hours)						
Data length: 11						
Name Server: dnsredes.redes.usal.es						
Additional records						
dnsredes.redes.usal.es: type A, class IN, addr 20.3.0.10						
Name: dnsredes.redes.usal.es						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Time to live: 108000 (3 hours)						
Data length: 4						
Address: 20.3.0.10						
<Root>: type OPT						
Name: <Root>						
Type: OPT (41)						
UDP payload size: 4096						
Higher bits in extended RCODE: 0x00						
EDNS0 version: 0						
Z: 0x0000						
0..... = DO bit: Cannot handle DNSSEC security RRs						
.000 0000 0000 0000 = Reserved: 0x0000						
Data length: 28						
Option: COOKIE						

DNSusal tampoco es el responsable del dominio en cuestión, pero tiene un servidor DNS en sus registros que es responsable de esa parte del dominio. Por lo que en el DNS query response le va a enviar la correspondiente información de DNSredes (IP: 20.3.0.10)

No.	Time	Source	Destination	Protocol	Length	Info
74	24.864105	20.1.0.10	30.0.0.10	DNS	155	Standard query response 0x0f89 A pc1.redes.usal.es NS dnsredes.redes.usal.es A ...
75	24.868765	30.0.0.10	20.3.0.10	DNS	100	Standard query 0x6664 A pc1.redes.usal.es OPT
76	24.934863	20.3.0.10	30.0.0.10	DNS	132	Standard query response 0x6664 A pc1.redes.usal.es A 20.3.0.20 OPT
▶ Frame 75: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0						
▶ Ethernet II, Src: 0c:77:5d:0e:02:00 (0c:77:5d:0e:02:00), Dst: ca:03:06:f4:00:38 (ca:03:06:f4:00:38)						
▶ Internet Protocol Version 4, Src: 20.1.0.10, Dst: 30.0.0.10						
▶ User Datagram Protocol, Src Port: 53, Dst Port: 32882						
▶ Domain Name System (query)						
Transaction ID: 0x6664						
Flags: 0x0010 Standard query						
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						
Additional RRs: 1						
Queries						
pc1.redes.usal.es: type A, class IN						
Name: pc1.redes.usal.es						
[Name Length: 17]						
[Label Count: 4]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Authoritative nameservers						
redes.usal.es: type NS, class IN, ns dnsredes.redes.usal.es						
Name: redes.usal.es						
Type: NS (authoritative Name Server) (2)						
Class: IN (0x0001)						
Time to live: 108000 (3 hours)						
Data length: 11						
Name Server: dnsredes.redes.usal.es						
Additional records						
dnsredes.redes.usal.es: type A, class IN, addr 20.3.0.10						
Name: dnsredes.redes.usal.es						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
Time to live: 108000 (3 hours)						
Data length: 4						
Address: 20.3.0.10						
<Root>: type OPT						
Name: <Root>						
Type: OPT (41)						
UDP payload size: 512						
Higher bits in extended RCODE: 0x00						
EDNS0 version: 0						
Z: 0x8000						
1..... = DO bit: Accepts DNSSEC security RRs						
.000 0000 0000 0000 = Reserved: 0x0000						
Data length: 12						
Option: COOKIE						
[Response In: 76]						

El siguiente mensaje generado es el DNS query hacia el servidor nuevo desde DNScom, preguntando por "pc1.redes.usal.es"

No.	Time	Source	Destination	Protocol	Length	Info
74	24.864105	20.1.0.10	30.0.0.10	DNS	155	Standard query response 0x0f89 A pc1.redes.usal.es NS dnsredes.redes.usal.es A ...
75	24.868765	30.0.0.10	20.3.0.10	DNS	100	Standard query 0x6664 A pc1.redes.usal.es OPT
76	24.934863	20.3.0.10	30.0.0.10	DNS	132	Standard query response 0x6664 A pc1.redes.usal.es A 20.3.0.20 OPT
Frame 76: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0 Ethernet II, Src: ca:03:06:f4:00:38 (ca:03:06:f4:00:38), Dst: 0c:77:5d:0e:02:00 (0c:77:5d:0e:02:00) Internet Protocol Version 4, Src: 20.3.0.10, Dst: 30.0.0.10 User Datagram Protocol, Src Port: 53, Dst Port: 35399 Domain Name System (response) Transaction ID: 0x6664 Flags: 0x8400 Standard query response, No error Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 1 Queries pc1.redes.usal.es: type A, class IN Name: pc1.redes.usal.es [Name Length: 17] [Label Count: 4] Type: A (Host Address) (1) Class: IN (0x0001) Answers pc1.redes.usal.es: type A, class IN, addr 20.3.0.20 Name: pc1.redes.usal.es Type: A (Host Address) (1) Class: IN (0x0001) Time to live: 86400 (1 day) Data length: 4 Address: 20.3.0.20 Additional records <Root>: type OPT Name: <Root> Type: OPT (41) UDP payload size: 4096 Higher bits in extended RCODE: 0x00 EDNS0 version: 0 Z: 0x0000 0..... = DO bit: Cannot handle DNSSEC security RRs .000 0000 0000 0000 = Reserved: 0x0000 Data length: 28 > Option: COOKIE [Request In: 75] [Time: 0.066098000 seconds]						

Finalmente DNSredes es el responsable del dominio “redes.usal.es” por lo que tiene la capacidad para resolver el nombre pedido desde el principio, por lo que en la respuesta del DNS le enviará la correspondencia de IP-Nombre de pc1.redes.usal.es → 20.3.0.20. Esta información le llega a DNScom

No.	Time	Source	Destination	Protocol	Length	Info
75	24.868765	30.0.0.10	20.3.0.10	DNS	100	Standard query 0x6664 A pc1.redes.usal.es OPT
76	24.934863	20.3.0.10	30.0.0.10	DNS	132	Standard query response 0x6664 A pc1.redes.usal.es A 20.3.0.20 OPT
77	24.940217	30.0.0.10	30.0.0.2	DNS	132	Standard query response 0x8aeb A pc1.redes.usal.es A 20.3.0.20 NS dnsredes.redes.usal.es
Frame 77: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface 0 Ethernet II, Src: 0c:77:5d:0e:02:00 (0c:77:5d:0e:02:00), Dst: ca:04:07:04:00:00 (ca:04:07:04:00:00) Internet Protocol Version 4, Src: 30.0.0.10, Dst: 30.0.0.2 User Datagram Protocol, Src Port: 53, Dst Port: 53 Domain Name System (response) Transaction ID: 0x8aeb Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 1 Authority RRs: 1 Additional RRs: 1 Queries pc1.redes.usal.es: type A, class IN Name: pc1.redes.usal.es [Name Length: 17] [Label Count: 4] Type: A (Host Address) (1) Class: IN (0x0001) Answers pc1.redes.usal.es: type A, class IN, addr 20.3.0.20 Name: pc1.redes.usal.es Type: A (Host Address) (1) Class: IN (0x0001) Time to live: 86400 (1 day) Data length: 4 Address: 20.3.0.20 Authoritative nameservers redes.usal.es: type NS, class IN, ns dnsredes.redes.usal.es Name: redes.usal.es Type: NS (authoritative Name Server) (2) Class: IN (0x0001) Time to live: 10800 (3 hours) Data length: 11 Name Server: dnsredes.redes.usal.es Additional records dnsredes.redes.usal.es: type IN, class IN, addr 20.3.0.10 Name: dnsredes.redes.usal.es Type: A (Host Address) (1) Class: IN (0x0001) Time to live: 10800 (3 hours) Data length: 4 Address: 20.3.0.10 [Request In: 68] [Time: 0.197087000 seconds]						

Una vez resuelto se tiene que volver a enviar la información al terminal www1, para ello desde DNScom tiene que enviarle la información recibida desde DNSredes, se envía primeramente a DNScisco que es el DNS predeterminado del terminal www1

Una vez que le llega la información a DNScisco éste la reenvía hacia www1 habiendo resuelto el nombre correctamente y pudiendo realizar la secuencia de mensajes ICMP como se debe.