DNS (Bind & IOS)

Versión febrero 2023

**Alumno (apellidos, nombre (DNI) : Tundidor Calvo, Domingo (71045732C)**

**Alumno (apellidos, nombre (DNI) : Vicente Sánchez, Natalia (70918190J)**

**Fecha: 7-3-2023**

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

# Entorno de trabajo

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

# 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 intervinientes (cliente-resolver y los diferentes DNSs de la jerarquía)
* Como se gestionan las cachés

# 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*](http://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 (o dnscisco.cisco.com), www1.cisco.com, www2.cisco.com* (ambos denominados w*ww.cisco.com*) respectivamente.

Imagen que contiene Diagrama

Descripción generada automáticamente

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*.

# 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.

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

RESPUESTA

La orden utilizada es cat /etc/resolv.conf

127.0.0.1 se refiere a sí mismo luego el servidor dns asignado son ellos mismos. Es decir para el equipo dnses es dnses, dnscom es dnscom, dnsraiz es dnsraiz y dnsusal es dnsusal.





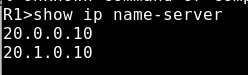




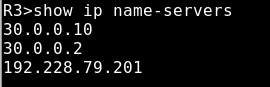
1. Consulta en los routers esta misma información. ¿Qué orden has utilizado?

RESPUESTA

Se ha utilizado show ip name-server









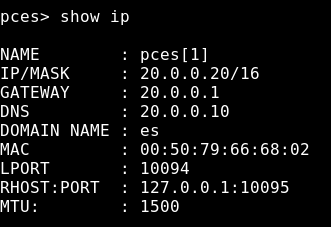
1. Consulta en los VPCS esta misma información. ¿Qué orden has utilizado?

RESPUESTA

Se ha utilizado la orden show ip.

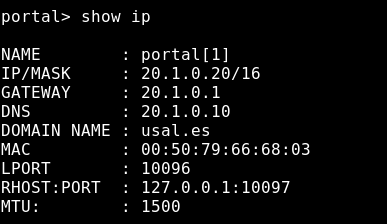
La ip del dns para pces es: 20.0.0.10

Su nombre de dominio: es



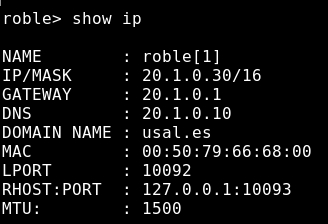
La ip del dns para portal es: 20.1.0.10

Su nombre de dominio: usal.es



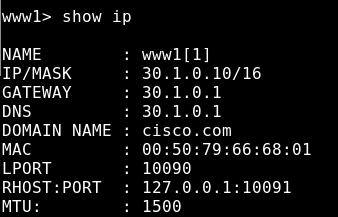
La ip del dns para roble es: 20.1.0.10

Su nombre de dominio: usal.es

****

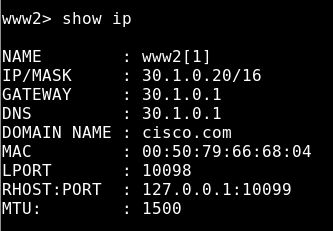
**La Ip del dns para www1 es: 30.1.0.1**

**Su nombre de dominio: usal.es**



La ip del dns para www2 es: 30.1.0.1

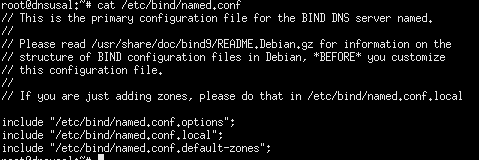
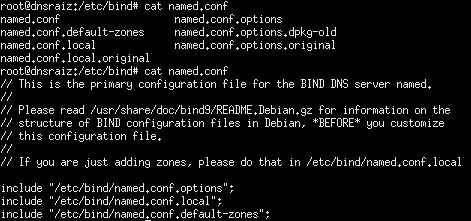
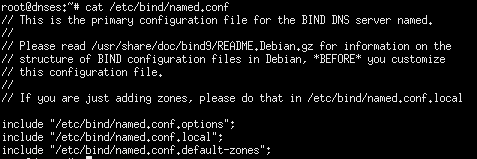
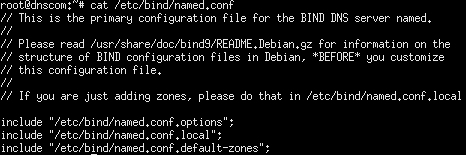
Su nombre de dominio: cisco.com



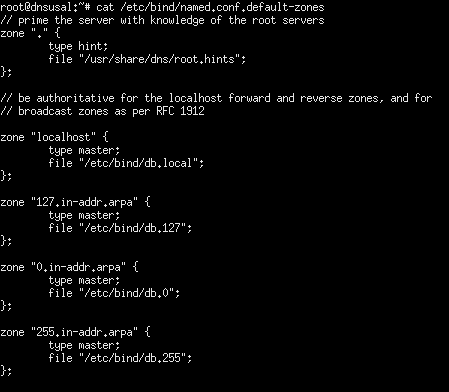
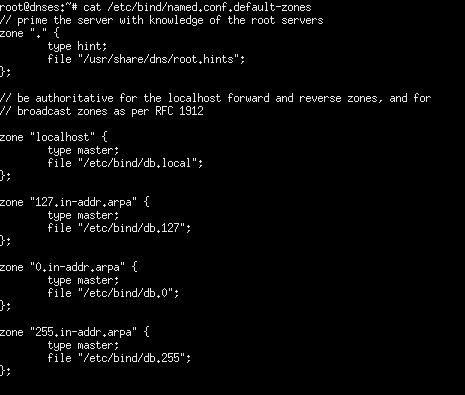
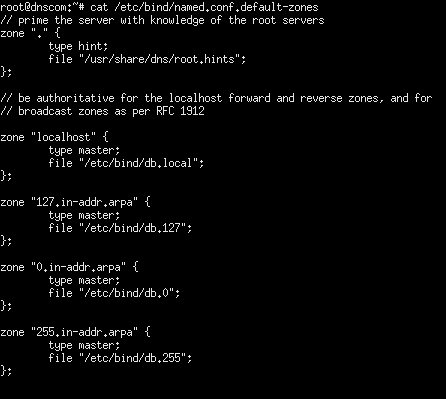
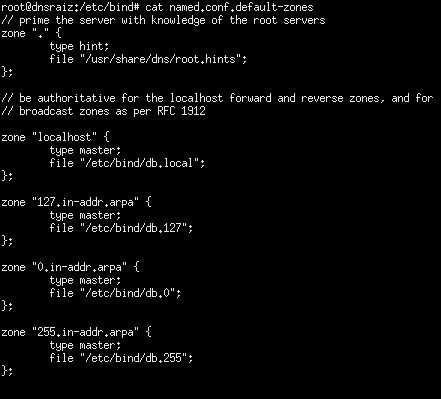
**Revisión del escenario configurado**

1. Revisa y comenta brevemente los ficheros de configuración de todos los servidores de DNS del escenario (dnsraiz, dnscom, dnses y dnsusal).

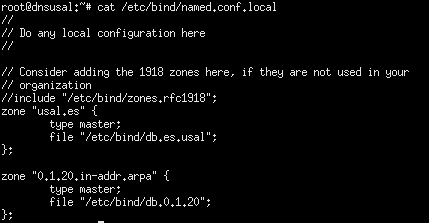
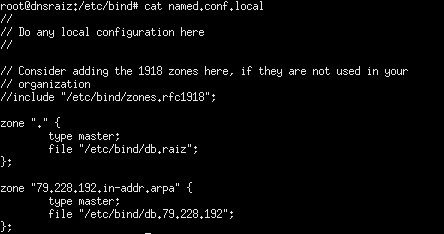
RESPUESTA

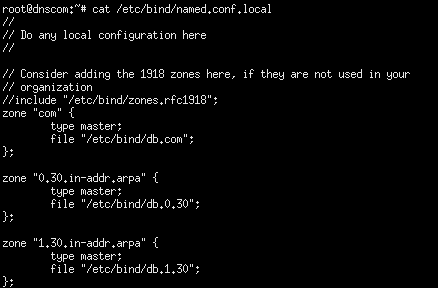
El fichero named.conf es el fichero de configuración que incluye a los demás. Aporta informacion sobre la configuración principal para el servidor dns asignado

El fichero named.conf.default-zones incluye la configuración de las zonas predeterminadas.

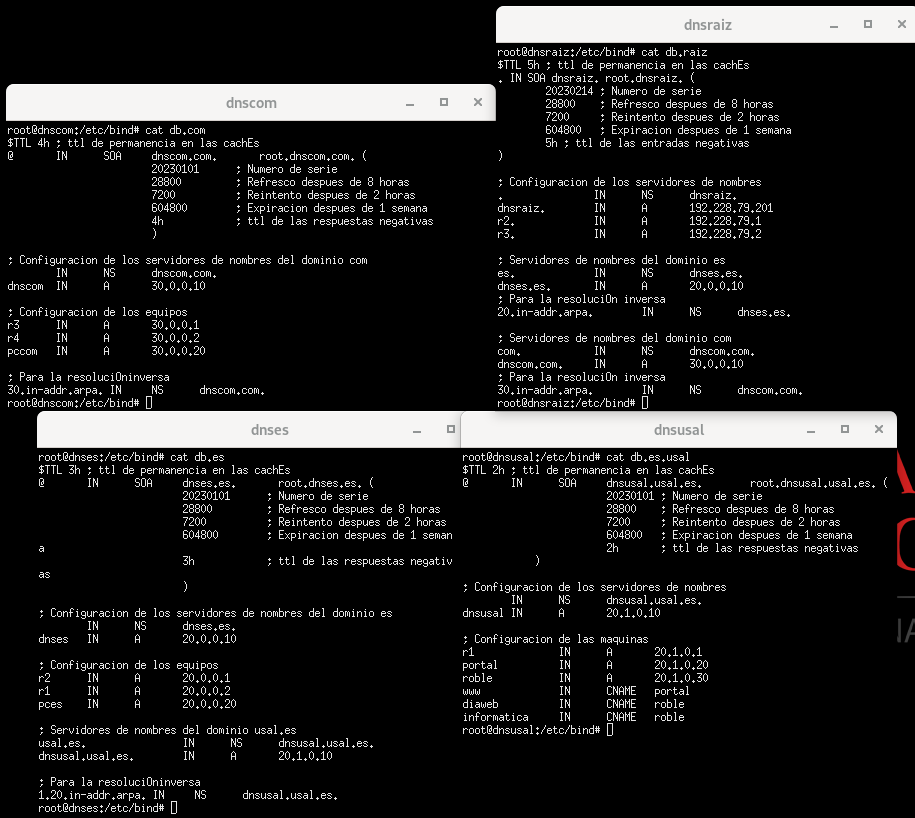


El fichero named.conf.local es el fichero de configuración para incluir dominios locales.





Como vemos entre todos los ficheros de configuración solo named.conf.local tiene diferencias entre los 4 equipos. Los dominios para los cuales cada servidor es maestro es distinto dependiendo del servidor. Para dns com es la zona “com” , “in-addr.arpa” y “1.30. in-addr.arpa”.



Cuando consultamos los ficheros de configuración *db.minombrededominio*; es decir:

*cat db.com*

*cat db.es*

*cat db.raiz*

*cat db.es.usal*

Tomando como ejemplo dnes consultando db.es:

Observamos las direcciones IP y los nombres de los servidores raíces:





La configuración de los equipos:



Y lo relativo a la resolución inversa



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

# 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.

## ¿Los routers son servidores DNS caché?

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

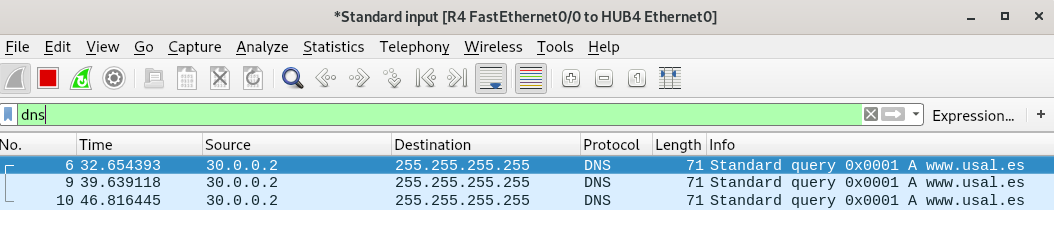
1. Én el router R4 realiza un ping a [www.usal.es](http://www.usal.es). Captura el tráfico en sus dos interfaces para responder a las preguntas: ¿Qué ha ocurrido? ¿por qué? Incluye en el informe el tráfico implicado.

RESPUESTA

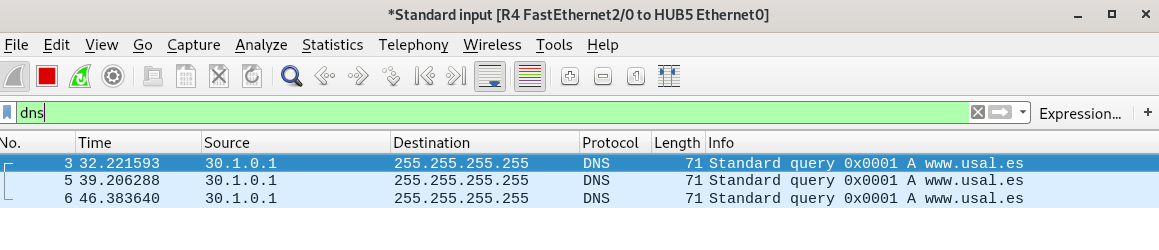
Cuando realizamos un ping desde R4 hasta [www.usal.es](http://www.usal.es). El terminal nos avisa que no puede reconocer la dirección. No había un servidor de nombres asignado a R4, luego cuando buscan las interfaces en su propia red, no encuentran la dirección..



Para e0/0:



Para e2/0:



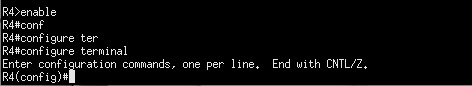
1. Asigna a R4 un servidor de nombre (en nuestro caso dnscom – 30.0.0.10) y el dominio *cisco.com*. Incluye las órdenes utilizadas.

RESPUESTA

Entramos primero en el modo configuración:

enable

configure terminal



Asignamos a R4 un servidor de nombre (dnscom cuya dirección es 30.0.0.10):

ip name-server 30.0.0.10



Asignamos a R4 el dominio cisco.com:

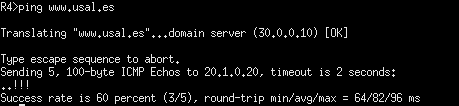
ip domain-name cisco.com



1. Realiza de nuevo un ping a [www.usal.es](http://www.usal.es) ¿Qué ha ocurrido? ¿por qué? ¿Hay alguna entrada nueva en la cache de resolución de nombres? ¿Qué orden has utilizado para consultarla? ¿Cuanto tiempo permanecerán en la cache? ¿Donde se configura este tiempo?

RESPUESTA

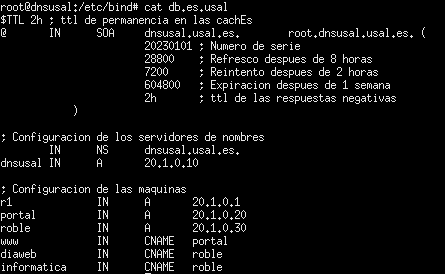
Ahora que se ha asignado el servidor de nombres al router cuando se realiza el ping lo realiza de forma exitosa y recibe el ping de respuesta.



Al consultar la caché de resolución de nombres con *show hosts* hay una nueva entrada: www.usal.es y el dns utilizado para resolver el nombre: dnsusal



Si consultamos el contenido del fichero db.es.usal en el servidor dnsusal descubrimos que el ttl es de 2h. Y por tanto las nuevas entradas permanecerán 2 horas en caché. En la primera línea del fichero se configura este tiempo:



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

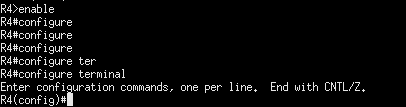
Para configurar R4 (o dnscisco) como responsable del dominio cisco.com hemos de seguir los siguientes pasos:

* + Habilitar DNS server
  + Añadir los recursos: SOA, NS y A
  + Añadir un balanceo de tráfico para [www.cisco.com](http://www.cisco.com) entre www1 y www2
  + Modificar los ficheros necesarios en dnscom para esta delegación

1. Incluye las ordenes utilizadas, su ejecución en el router y los ficheros modificados en dnscom.

RESPUESTA

Habilitamos y configuramos la terminal de R4.



Habilitamos el DNS server: ip dns server



Para añadir el SOA y el NS: ip dns primary dnscisco.com. soa root.dnscisco.com. mailbox.root.dnscisco.com. 28800 7200 604800 14400

ip host cisco.com ns dns.cisco.com



Para las direcciones A:

ip host www1.cisco.com 30.1.0.10



ip host ww2.cisco.com 30.1.0.20



Para conseguir el balanceo de tráfico: ip domain round-robin



Modificando el fichero db.com disponible en dnscom:

nano etc/bind/db.com

Añadiendo las siguientes 2 lineas al fichero:

cisco.com IN NS dnscisco.cisco.com

dnscisco.cisco.com IN A 30.1.0.1



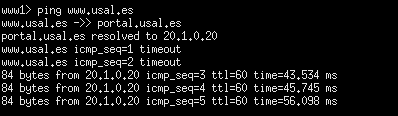
La primera línea indica que el servidor dns cisco.com está en dnscisco.cisco.com

La segunda línea define la dirección IP del servidor de nombres dnscisco.cisco.com, mediante un registro de tipo A (Address)

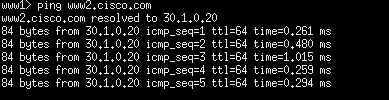
1. Comprueba tu configuración desde los equipos www1 y www2 resolviendo nombres del dominio .com y usal.es. ¿Qué órdenes has utilizado? Muestra y comenta las salidas obtenidas. Consulta la caché del DNS de R4. ¿Qué orden has utilizado? ¿Justifica las entradas encontradas?

RESPUESTA

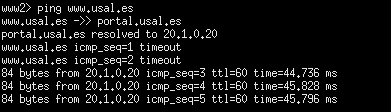
ping de www1 a [www.usal.es](http://www.usal.es):



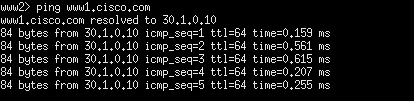
ping de www1 a www2.cisco.com:



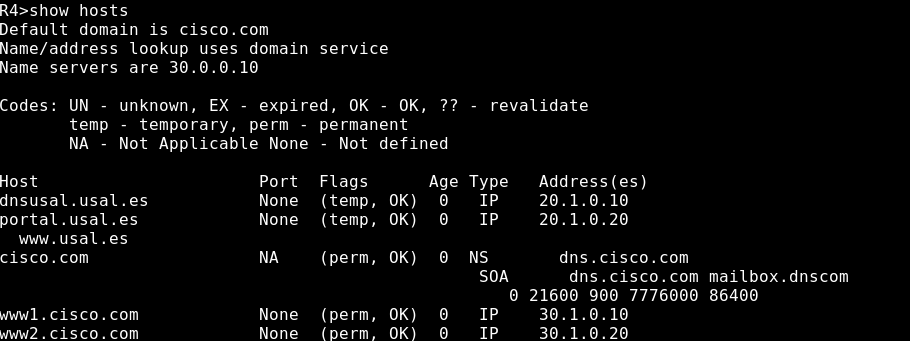
ping de www2 a [www.usal.es](http://www.usal.es):



ping de www2 a www1.cisco.com:



Después de realizar los pings correspondientes:



# Entendiendo las consultas a la jerarquía y las cachés

Antes de comenzar este apartado aseguraté 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



Se repite el proceso con las otras 4 dns.

1. Desde la máquina *roble* (del dominio usal.es) ejecuta *ping* [*www.cisco.com*](http://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 ordenes

rndc dumpdb -cache

cat /var/cache/bind/named\_dump.db

RESPUESTA

ping www.cisco.com



1. 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.

RESPUESTA

1. 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](http://www.cisco.com) > www1.log

dig [r4.com](http://www.cisco.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?

RESPUESTA

# 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.

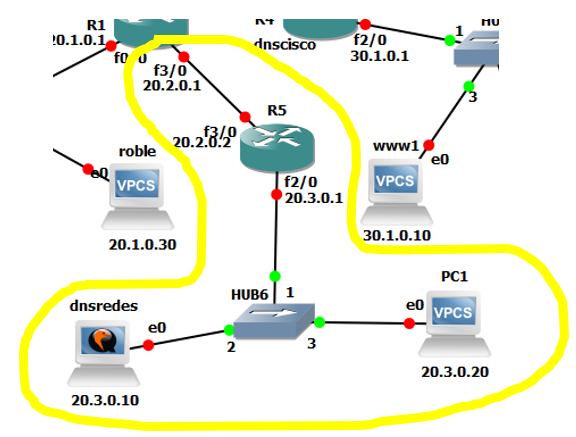


Figura 2: Dominio redes.usal.es

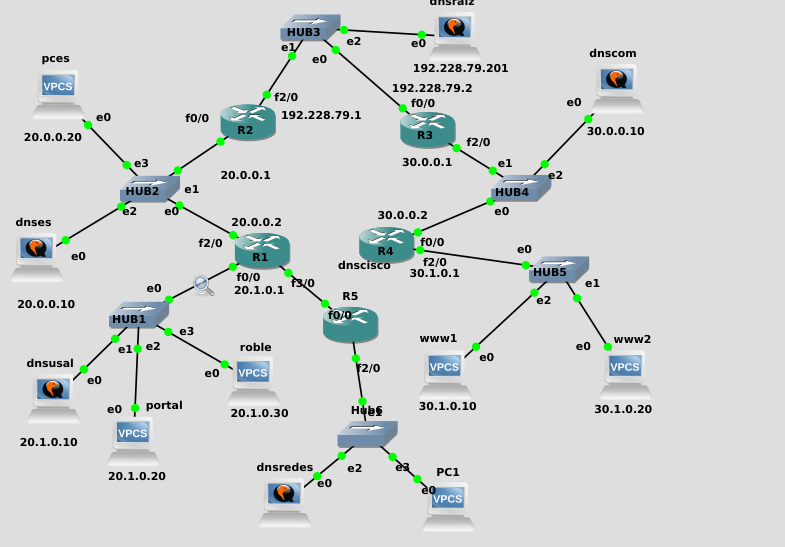
Se pide:

1. 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 *dnsredes*, 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?

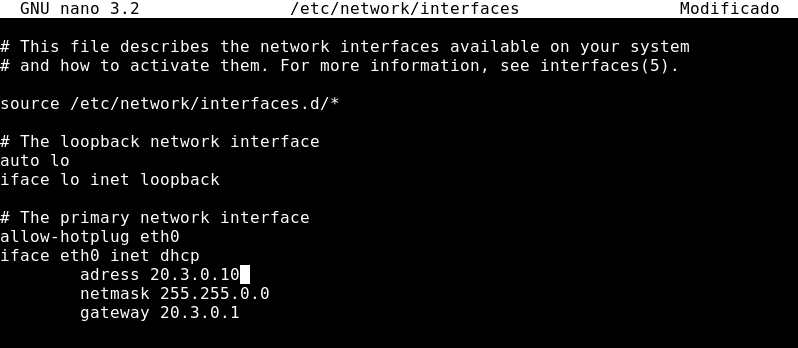
**NOTA**:

* Para configurar *dnsredes* 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).

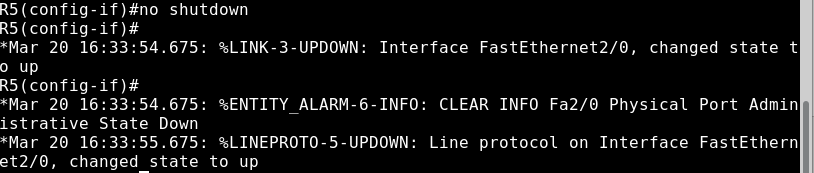
RESPUESTA

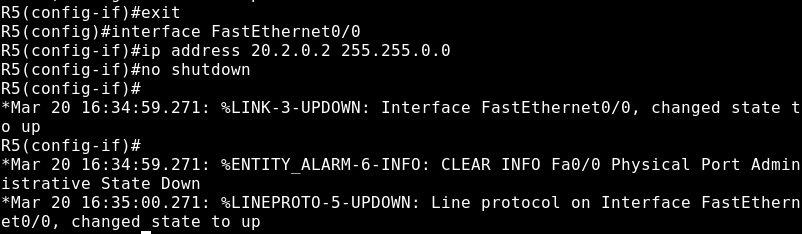


—---









Para R1:



Tabla de ruta de r5:

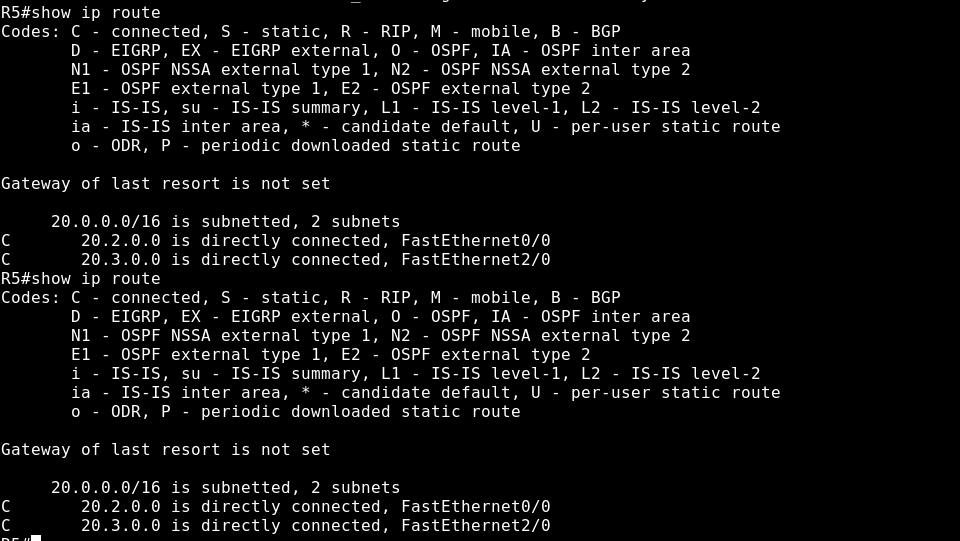
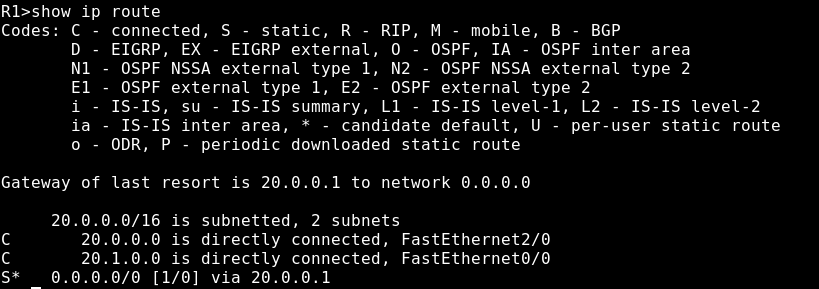


Tabla de ruta de r1:



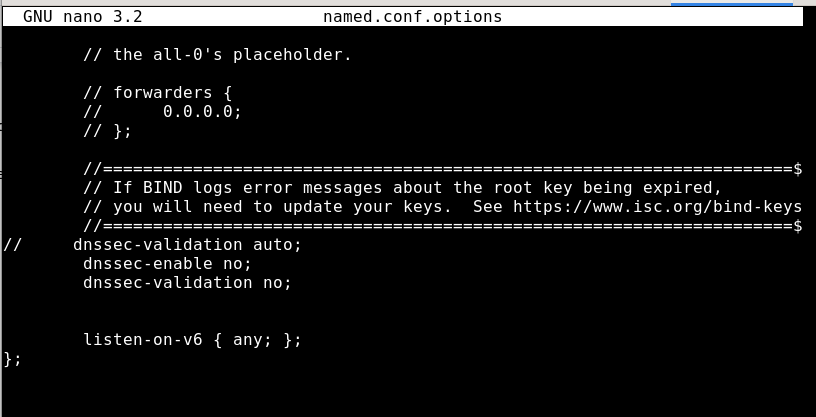
1. Configurar un servidor DNS que sea maestro del dominio “redes.usal.es” en la máquina *dnsredes* de tal forma que sea capaz de responder peticiones internas tanto de forma directa como inversa.
   * 1. En el fichero /etc/bind/named.conf.options deshabilitar las opciones de seguridad. Cambiar:

dnssec-validation auto; por

// dnssec-validation auto;

dnssec-enable no;

dnssec-validation no;



* + 1. 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";

};

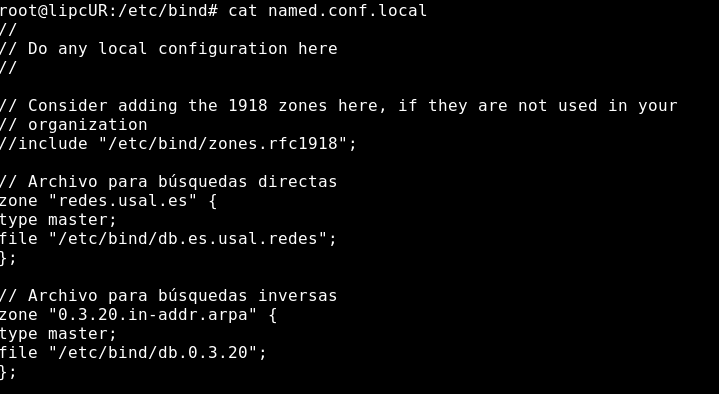
// Archivo para búsquedas inversas

zone "0.3.20.in-addr.arpa" {

type master;

file "/etc/bind/db.0.3.20";

};



* + 1. 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

; rediris recomienda poner la fecha

604800 ; Refresco 1 semana (servidores secundarios)

86400 ; Reintento tras 1 día

2419200 ; Expira después de 4 semanas

1d) ; ttl de las respuestas negativas

IN NS dnsredes.redes.usal.es.

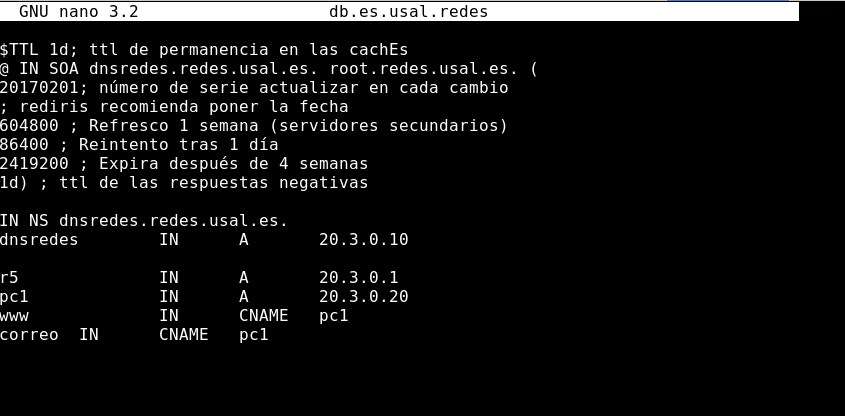
dnsredes IN A 20.3.0.10

r5 IN A 20.3.0.1

pc1 IN A 20.3.0.20

www IN CNAME pc1

correo IN CNAME pc1



* + 1. 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 ; Reintento tras 1 día

2419200 ; Expira después de 4 semanas

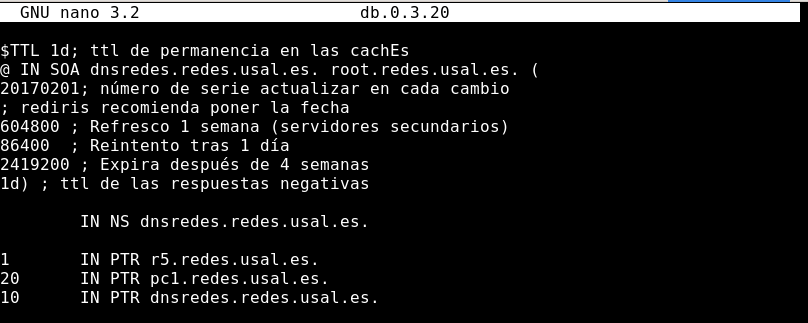
1d) ; ttl de las respuestas negativas

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.



* + 1. 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:

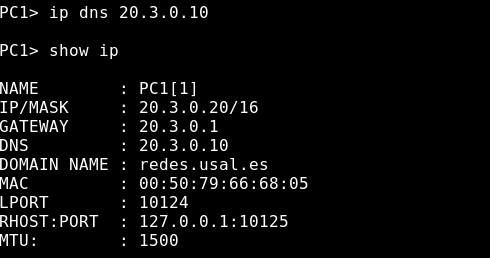
domain redes.usal.es

nameserver 127.0.0.1



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).

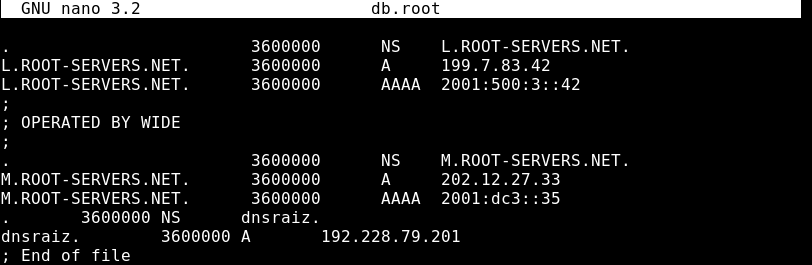
Para PC1:



* + 1. Configura adecuadamente nuestro servidor local para que alcance los DNS raíces. Incluye en el informe los ficheros de configuración.

RESPUESTA

En /etc/bind/db.root:



* + 1. Ante de poner en marcha el servidor verifica que los ficheros de configuración son correctos con la orden: *named-checkconf. Incluye la salida obtenida.*

RESPUESTA



* + 1. Por último pon en marcha nuestro servidor de nombres ejecutando la siguiente orden: service bind9 restart o /etc/init.d/bind9 restart

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

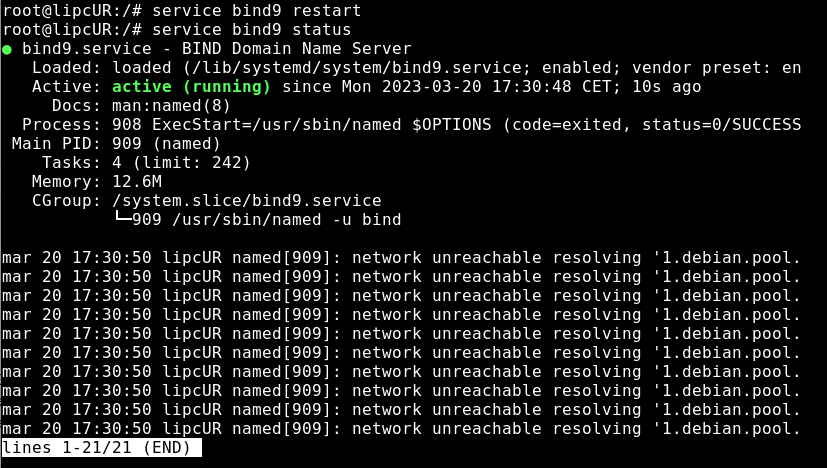
service bind9 status

systemctl status bind9.service

journalctl -xe

Incluye la salida de la orden utilizada.

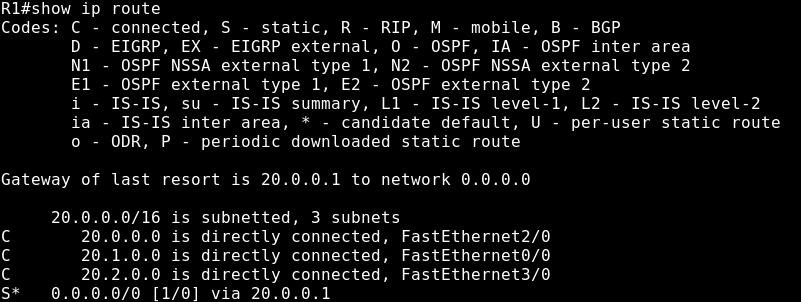
RESPUESTA

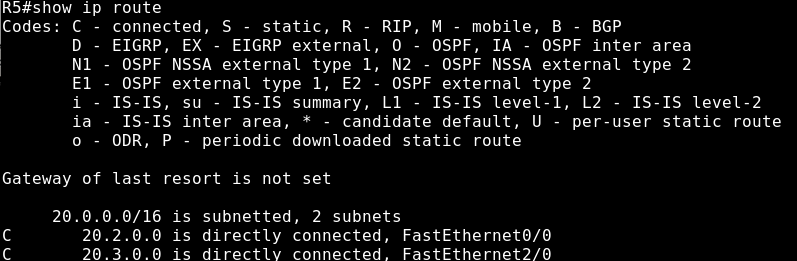


1. Desde pc1 intenta resolver el nombre *dnsredes.redes.usal.es.* Especifica la orden que has utilizado y realiza las capturas de tráfico que consideres necesarias para obtener los mensajes de DNS que se generan en todo el esquema.

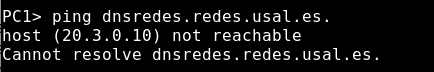
RESPUESTA

De acuerdo a las tablas de rutas que podemos consultar con show ip route tanto para r1 como para r5, PC1 debería poder resolver el nombre:





Aunque cuando se realiza el ping: ping dnsredes.redes.usal.es Aparece lo siguiente:



1. 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.

RESPUESTA

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

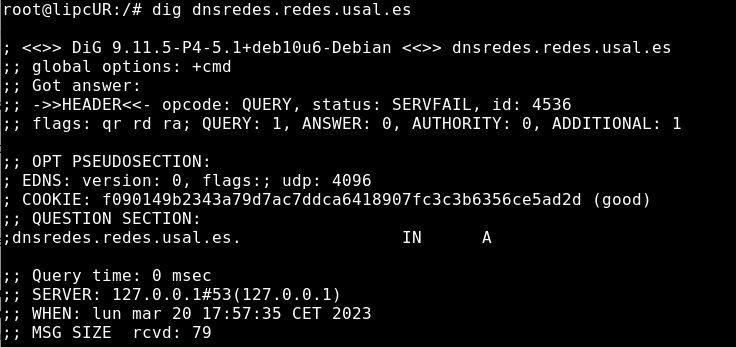
dig dnsredes.redes.usal.es (anota el tiempo de respuesta)

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?

RESPUESTA

Primera respuesta:



Segunda respuesta:

1. 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.

RESPUESTA