Prácticas con NetGUI
Práctica 6: Domain Name System (DNS)

Fundamentos de Redes de Ordenadores

GSyC
Departamento de Teoría de la Señal y Comunicaciones y Sistemas Telemáticos y Computación

Enero de 2021

Resumen

En esta práctica se aprende el funcionamiento básico del DNS. Para su realización es necesario que descargues el fichero del escenario:

`http://mobiquo.gsyc.urjc.es/practicas/fro/p6.html`

NOTA: Para realizar todas las capturas de esta práctica utiliza `tcpdump` tal y como venías usándolo en otras prácticas pero además añade la opción `-n` para que la propia aplicación `tcpdump` no solicite otras resoluciones adicionales al DNS para mostrar la información de forma más amigable.

Introducción

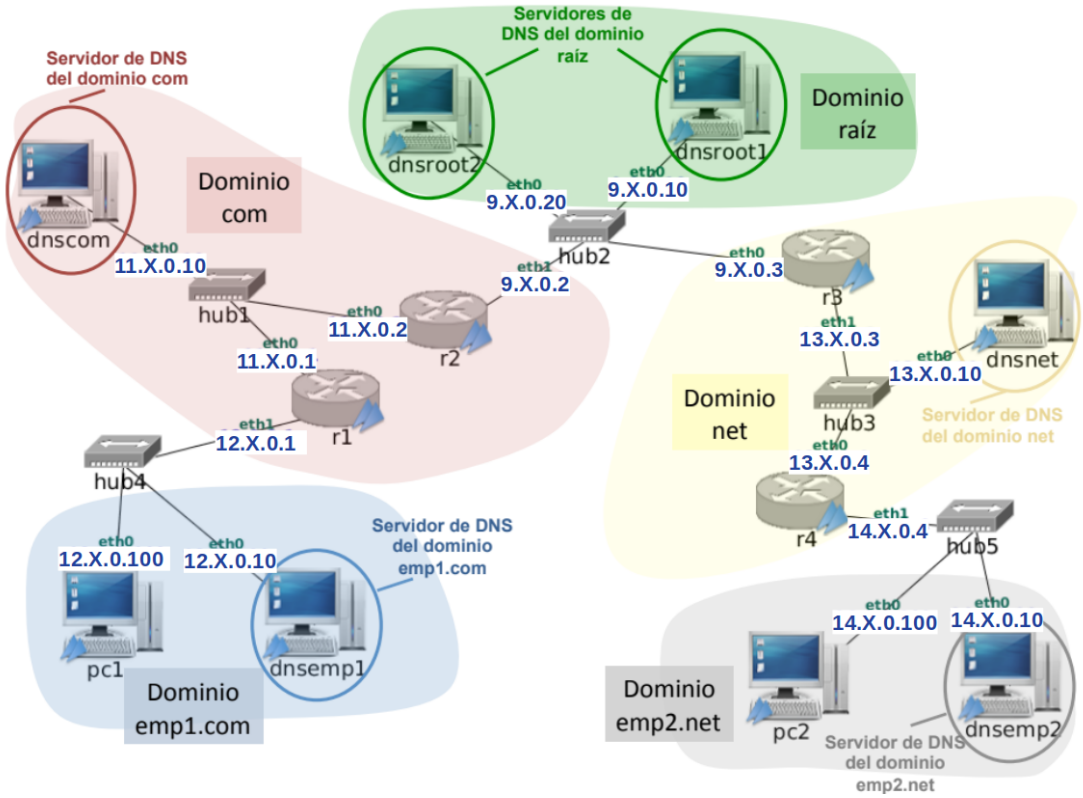


Figura 1: Árbol de dominios

Árbol de dominios

El escenario definido en `DNS-lab` está formado por 4 *routers* y 8 máquinas. Dentro de este escenario existen los siguientes dominios (véase la figura 1):

- Dominio raíz donde se encuentran las máquinas `dnsroot1` y `dnsroot2`.
- Dominio com: donde se encuentran los *routers* `r1` y `r2` y la máquina `dnscom`. Por tanto, su nombre completo es `r1.com`, `r2.com` y `dnscom.com` respectivamente.
- Dominio `emp1.com`: donde se encuentran las máquinas `pc1` y `dnsemp1`. Por tanto, su nombre completo es `pc1.emp1.com` y `dnsemp1.emp1.com` respectivamente.
- Dominio net: donde se encuentran los *routers* `r3` y `r4` y la máquina `dnsnet`. Por tanto, su nombre completo es `r3.net`, `r4.net` y `dnsnet.net` respectivamente.
- Dominio `emp2.net`: donde se encuentran las máquinas `pc2` y `dnsemp2`. Por tanto su nombre completo es: `pc2.emp2.net` y `dnsemp2.emp2.net` respectivamente.

Servidores de DNS: Ficheros de configuración y mapas

La siguiente tabla muestra las máquinas del escenario que son servidores de DNS:

Máquina	Descripción	Ficheros de configuración
`dnsroot1`	Servidor de nombres raíz	`/etc/bind/named.conf` `/etc/bind/db.root`
`dnsroot2`	Servidor de nombres raíz	`/etc/bind/named.conf` `/etc/bind/db.root`

`dnscom`	Servidor de nombres del dominio `com`	`/etc/bind/named.conf`
		`/etc/bind/db.root`
		`/etc/bind/db.com`

`dnsemp1`	Servidor de nombres del dominio `emp1.com`	`/etc/bind/named.conf`
		`/etc/bind/db.root`
		`/etc/bind/db.emp1.com`

`dnsnet`	Servidor de nombres del dominio `net`	`/etc/bind/named.conf`
		`/etc/bind/db.root`
		`/etc/bind/db.net`

`dnsemp2`	Servidor de nombres del dominio `emp2.net`	`/etc/bind/named.conf`
		`/etc/bind/db.root`
		`/etc/bind/db.emp2.net`

En esas máquinas se ha utilzado el paquete `bind9` para instalar el servidor de DNS. En la tabla anterior aparecen especificados los ficheros de configuración más importantes en cada servidor. Todos ellos se encuentran en la carpeta `/etc/bind` de cada máquina virtual).

Para ver el contenido de un ficheros en una máquina virtual puedes utilizar la la orden `less`en la máquina que contiene dicho fichero:

```
less <nombre-del-fichero-incluyendo-ruta>
```

Así, por ejemplo, para el ver el mapa del dominio `emp2.net`, tienes que escribir en la ventana de terminal de la máquina `dnsemp2.emp2.net` la orden:

```
dnsemp2~:# less /etc/bind/db.emp2.net
```

Mientras usas `less` puedes moverte adelante y atrás por el contenido del fichero utilizando las flechas del cursor. Para salir de `less` pulsa la tecla `q` (*quit*).

A continuación se explica el propósito y contenido de estos ficheros de configuración de los servidores de DNS:

- `named.conf`:

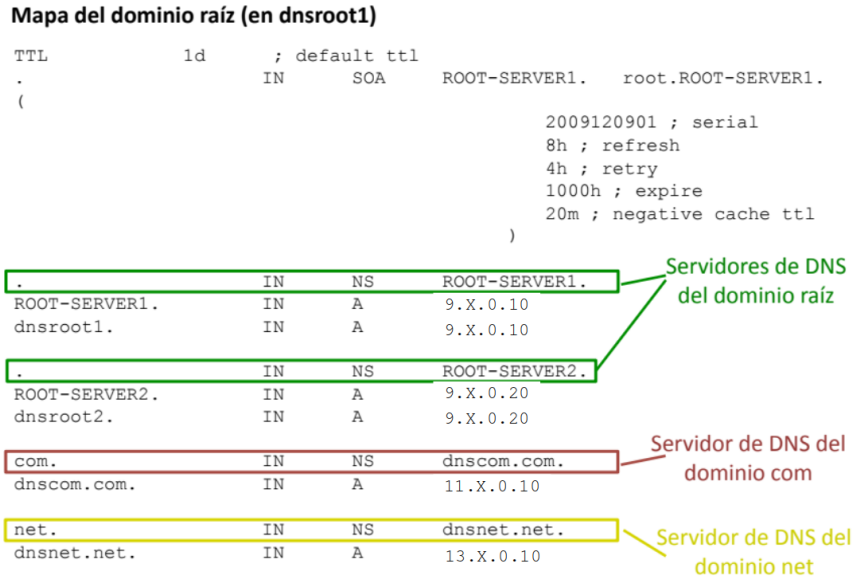
  Fichero con la configuración general del servidor de DNS: lista de dominios (zonas) para las que el servidor es maestro y/o esclavo y nombres de los ficheros que contienen los mapas de esos dominios. Como ejemplo se muestra a continuación parte del contenido de este fichero en el servidor `dnscom`:

```
zone "com" {
        type master;
        file "/etc/bind/db.com";
};
```

  El contenido de este fichero indica que la máquina donde se encuentra dicho fichero, `dnscom`, es servidor maestro del dominio `.com` y que el fichero que almacena el mapa de ese dominio es `/etc/bind/db.com`

- `db.root`:

  Mapa del dominio raíz de DNS (dominio "."), almacenado en los servidores de dicho dominio (`dnsroot1` y `dnsroot2`). Su contenido en `dnsroot1` es:



  En dicho mapa se encuentra la relación de subdominios directos del raíz, que en este escenario son `.com` y `.net`, junto con el nombre e IP de los servidores de ese subdominio.

  En `dnsroot2` el fichero `db.root` tendrá un contenido similar, con leves cambios en el registro SOA.

  En el resto de servidores (`dnscom`, `dnsnet`, `dnsemp1` `dnsemp2`), pese a que no son servidores del dominio raíz, también existe este fichero `db.root`. En estos casos el fichero contiene simplemente la lista de las IPs de servidores del dominio raíz. Esta información la necesitan los servidores para iniciar la cadena de búsqueda de nombres que no conozcan. El contenido de este fichero es considerado "provisional" por los servidores, y la primera vez que un servidor tenga que enviar un mensaje a un servidor raíz sacado de este dichero, le enviará también una consulta adicional preguntando la lista de servidores del dominio raíz, por si hubiera habido cambios.

En esos servidores (`dnscom`, `dnsnet`, `dnsemp1` `dnsemp2`) el contenido de `db.root` es:

Fichero db.root (en los servidores que no son del dominio raíz)

```
.                   518400   IN      NS      ROOT-SERVER1.
.                   518400   IN      NS      ROOT-SERVER2.

ROOT-SERVER1.       518400   IN      A       9.X.0.10
ROOT-SERVER2.       518400   IN      A       9.X.0.20
```

Servidores de DNS del dominio raíz

- `db.*`:

  Los ficheros que empiezan por `db.` contienen el mapa del dominio que sirve un determinado servidor.

  Así, por ejemplo, el servidor de DNS del servidor `dnsemp1` sirve el mapa del dominio `emp1.com` y por tanto, tiene el fichero `/etc/bind/db.emp1.com` que almacena el mapa del dominio `emp1.com`, cuyo contenido es

Fichero db.emp1.com

```
$TTL                1d      ; default ttl
emp1.com.               IN    SOA       dnsemp1.emp1.com.  root.dnsemp1.emp1.com. (
                                                2009120901 ; serial
                                                8h ; refresh
                                                4h ; retry
                                                1000h ; expire
                                                20m ; negative cache ttl
                                                )

emp1.com.               IN      NS      dnsemp1.emp1.com.
dnsemp1.emp1.com.       IN      A       12.X.0.10
pc1.emp1.com.       1s  IN      A       12.X.0.100
```

Servidor de DNS del dominio emp1.com

Caché de un servidor DNS

Para ver el contenido de la caché de DNS de un servidor de DNS, ejecuta en su máquina la siguientes dos órdenes, una detrás de otra:

```
rndc dumpdb -cache
less /var/cache/bind/named_dump.db
```

La primera orden vue lca el contenido de la caché de DNS del servidor en el fichero `/var/cache/bind/named_dump.db`, y la segunda te permite consultar su contenido. Un ejemplo de contenido de una caché en un momento dado sería:

```
;
;
; Cache dump of view '_default'
;
$DATE 20190426104439
; authanswer
.                       78497   IN NS   ROOT-SERVER1.
                        78497   IN NS   ROOT-SERVER2.
; glue
net.                    78497   NS      dnsnet.net.
; glue
dnsnet.net.             78497   A       13.0.0.10
; authauthority
emp2.net.               78497   NS      dnsemp2.emp2.net.
; glue
dnsemp2.emp2.net.       78497   A       14.0.0.10
; authanswer
pc2.emp2.net.           78497   A       14.0.0.100
; additional
ROOT-SERVER1.           78497   A       9.0.0.10
; additional
ROOT-SERVER2.           78497   A       9.0.0.20
;
```

Las líneas que empiezan por ";" son comentarios

valores cacheados

tiempo restante de vida en la caché a cada entrada

Ten en cuenta que cada vez que quieras ver de nuevo el contenido de la caché debes ejecutar primero la orden `rndc` para actualizar el contenido del fichero, y después ejecutar la orden `less` para mostar el nuevo contenido del fichero.

Para borrar todos los contenidos de la caché de DNS de un servidor, ejecuta en su máquina la orden:

```
rndc flush
```

Configuración del servidor de nombres de cada máquina cliente

Todas las máquinas del escenario tienen configurado su fichero `/etc/nsswitch.conf` de forma que cuando quieran saber la IP que se corresponde con un nombre, primero consultarán su fichero local `/etc/hosts`, y si no encuentran la respuesta, consultarán su servidor de DNS.

Cada máquina tiene configurado su servidor de DNS en su fichero `/etc/resolv.conf`, de la siguiente forma:

- Las máquinas `dnsroot1` y `dnsroot2` tienen cada una configurado como servidor de DNS a ella misma.
- Las máquinas `pc1` y `dnsemp1` tienen configurado como servidor de DNS a `dnsemp1`.
- Las máquinas `pc2` y `dnsemp2` tienen configurado como servidor de DNS a `dnsemp2`.
- La máquina `dnscom` y los *routers* `r1` y `r2` tienen configurado como servidor de DNS a `dnscom`.
- La máquina `dnsnet` y los *routers* `r3` y `r4` tienen configurado como servidor de DNS a `dnsnet`.

Programa `host`

Para consultar al DNS puede utilizarse la orden `host`, herramienta que permite realizar consultas a un servidor de DNS. Utilizaremos este programa de la siguiente forma:

```
host <nombreDeMáquina>
```

El programa `host` mostrá la dirección IP asociada a `<nombreDeMáquina>`, como resultado de haber consultado al servidor de DNS que tenga configurado la máquina donde se ejecuta el programa.

NOTA IMPORTANTE: El programa `host` consulta directamente al DNS, sin mirar nunca el fichero `/etc/hosts`, independientemente del contenido del fichero `/etc/nsswitch.conf`. El resto de órdenes como `ping`, `traceroute`, etc, utilizan dicho fichero, y con la configuración del escenario, primero mirarán en el `/etc/hosts` y luego interrogarán al DNS.

Formato de los mensajes de DNS

El formato de mensaje de DNS tiene muchos campos. Para la realización de esta práctica ten a mano para consultar las transparencias 41–43 del tema de teoría que contienen, en el formato utilizado por `wireshark`, los campos más importantes de los mensajes, que son los que debes intentar localizar en las capturas.

1. Resolución de nombres

Arranca las máquinas del escenario definido en `DNS-lab` **de una en una** y responde a las siguientes preguntas:

1. Imagina qué ocurriría si la máquina `pc1` ejecuta `host pc2.emp2.net`. ¿Cuántos mensajes de DNS se generarían y entre qué máquinas? Es importante que consideres que es la primera consulta que se realiza en ese escenario (las cachés de los servidores de DNS están vacías).

2. Ejecuta la instrucción anterior en `pc1`, realizando previamente una captura de tráfico en `r1(eth1)` para ver todos los mensajes de DNS generados[1]. Almacena los paquetes de la captura en el fichero `p6-dns-01.cap` ejecutando el comando con la opción `-n`:
   `tcpdump -n -s 0 -i <interfaz> -w <fichero>`[2].

3. Observa en la captura cómo el mensaje de consulta que envía `pc1` tiene activado el flag *Recursion desired* para que la consulta sea recursiva y los mensajes de consulta que envía `dnsemp1` no tienen activado el flag *Recursion desired* para que la consulta se realice de forma iterativa[3].

4. Observa en la/s captura/s el valor TTL (Time To Live) de la respuesta obtenida en `pc1`. NOTA: No confundir el TTL de los mensajes de DNS de respuesta con el TTL de cabecera IP. En esta práctica siempre hablamos del TTL de los mensajes de DNS.

5. Para cada uno de los mensajes de respuesta que observes, explica qué línea/s de cada uno de los mapas de dominio (db.*) proporcionan la información que viaja en dichos mensajes (registros A o registros NS). Para ello mira el contenido de los ficheros de dichos mapas.

6. Supón que ocurriría si después de haber realizado la consulta anterior, en `pc1` se solicita de nuevo la resolución de `pc2.emp2.net`. ¿Cuántos mensajes de DNS se generarían y entre qué máquinas? ¿Por qué?

7. Ejecuta la resolución anterior en `pc1`, realizando de nuevo una captura en `r1(eth1)` y guardando su contenido en el fichero `p6-dns-02.cap` para ver todos los mensajes de DNS generados.

8. Explica el valor TTL (Time To Live) de la respuesta obtenida en `pc1`. Compáralo con el valor obtenido en el apartado 2.

9. Imagina qué mensajes de DNS se generarían y entre qué máquinas si en `pc2` se pide la resolución de `pc1.emp1.com`.

10. Ejecuta la resolución anterior en `pc2`, realizando una captura de tráfico en la interfaz `r4(eth1)` para ver todos los mensajes de DNS generados y guarda su contenido en el fichero `p6-dns-03.cap`.

11. Consulta la caché de DNS en el servidor de DNS de `pc2`, `dnsemp2`. Explica su contenido.

12. Supón que ocurriría si después de haber realizado la consulta anterior, en `pc2` se solicita de nuevo la resolución de `pc1.emp1.com`. ¿Cuántos mensajes de DNS se generarían y entre qué máquinas? ¿Por qué?

13. Ejecuta la resolución anterior en `pc2`, realizando una captura tráfico en la interfaz `r4(eth1)` para ver todos los mensajes de DNS generados y guarda su contenido en el fichero `p6-dns-04.cap`. Explica lo sucedido comparado con lo ocurrido en el apartado 7.

14. Consulta la caché de DNS en el servidor de DNS de `pc1`, `dnsemp1`. Explica su contenido.

15. Imagina qué ocurriría si después de haber realizado las consultas anteriores, en `pc1` se solicita la resolución de `r4.net`. ¿Cuántos mensajes de DNS se generarían y entre qué máquinas?

[1] Recuerda que si realizas más de una consulta a un servidor de DNS, éste almacena información en su caché. Para borrar la caché de un determinado servidor de DNS ejecuta en dicho servidor la instrucción: `rndc flush`.

[2] Utiliza la opción -n para que tcpdump no intente realizar resoluciones de DNS adicionales a las que genera el comando host.

[3] Observarás en la captura que el servidor además de consultar al servidor de DNS raíz por la resolucióng que se está realizando, como es la primera vez que el servidor envía un mensaje al servidor raíz, le enviará además otro mensaje con una consulta preguntando la lista de servidores del dominio raíz, por si ésta hubiera cambiado.

16. Ejecuta la resolución anterior en `pc1`, realizando una captura tráfico en la interfaz `r1(eth1)` para ver todos los mensajes de DNS generados y guarda su contenido en el fichero `p6-dns-05.cap`.

17. El nombre `r4.net` tiene asociadas las dos direcciones IP del *router* `r4`. Comprueba que al solicitar la resolución de `r4.net` sucesivas veces en `pc1`, el orden en el que se obtienen las direcciones IP de `r4` es aleatorio.

18. Imagina qué ocurriría en cada uno de los siguientes casos:

    a) En `pc1` se ejecuta la orden `ping -n pc200.emp1.com`.

    b) En `pc1` se ejecuta la orden `ping -n pc200.emp2.net`.

    c) En `pc1` se ejecuta la orden `ping -n pc20.emp2.net`.

    Ten en cuenta que ahora no vas a usar la orden `host`, que interroga directamente al DNS, sino una aplicación normal, `ping`, que usará la configuración de la máquina. Lo que significa que primero se buscará el nombre en el fichero `/etc/hosts` y si ahí no aparece, se preguntará al servidor de DNS.

    NOTA: la opción `-n` en el ping, igual que en el tcpdump o en traceroute, evita que el propio ping haga consultas adicionales al DNS para aportar más información a sus resultados. En esta práctica usa ping siempre con la opción `-n`.

    Para cada uno de los casos responde a las siguientes cuestiones:

    a) ¿Funcionaría el `ping`?

    b) ¿Al ejecutar el `ping` puedes ver la dirección IP asociada al nombre? ¿En qué fichero o mapa está esa asociación de nombre e IP?

    c) ¿Cuántos mensajes de DNS se generarían y entre qué máquinas?

19. Ejecuta las órdenes anteriores, realizando una captura de tráfico en cada caso:

    a) En `pc1` se ejecuta la orden `ping -n pc200.emp1.com` y se captura tráfico en `r1(eth1)` guardando el tráfico en el fichero `p6-dns-06.cap`.

    b) En `pc1` se ejecuta la orden `ping -n pc200.emp2.net` y se captura tráfico en `r1(eth1)` guardando el tráfico en el fichero `p6-dns-07.cap`.

    c) En `pc1` se ejecuta la orden `ping -n pc20.emp2.net` y se captura tráfico en `r1(eth1)` guardando el tráfico en el fichero `p6-dns-08.cap`.

20. Observando los ficheros de configuración de los servidores de DNS, indica qué ocurriría si en `pc1` se solicita por segunda vez la resolución de `pc20.emp2.net`.

21. Ejecuta la resolución anterior en `pc1`, realizando una captura de tráfico en `r1(eth1)` y guardando su contenido en `p6-dns-09.cap`. Indica durante cuanto tiempo se obtendría esta/s misma/s captura/s.

2. Entrega de la práctica

Para entregar la práctica sube a aulavirtual un fichero `p6.zip` que contenga la memoria y las capturas de tráfico dde `p6-dns-01.cap` a `p6-dns-11.cap`.

Sube al enlace que encontrarás en Aula Virtual, y antes de que termine el plazo de entrega, un único fichero de nombre `p6.zip`, resultado de comprimir el siguiente contenido:

- Memoria
- Ficheros de captura:
  - `p6-dns-01.cap`, `p6-dns-09.cap`