Prácticas con NetGUI
Práctica 5: Domain Name System (DNS)

Arquitectura de Redes de Ordenadores
Arquitectura de Internet

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

Abril de 2017

Resumen

En esta práctica se aprende el funcionamiento básico del DNS. Para su realización es necesario descomprimir el fichero `DNS-lab.tgz`.

1. Introducción

1.1. 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.

1.2. Servidores de DNS

En las máquinas del escenario que están configuradas como servidor de DNS se utiliza el paquete `bind9`. Los ficheros de configuración básica de `bind9` son los siguientes (se encuentran en la carpeta `/etc/bind` de cada máquina virtual):

- `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` (todos los nombres de máquinas que terminen en `.com`) también indica el fichero que almacena el mapa del dominio `com`, en este caso `/etc/bind/db.com`.

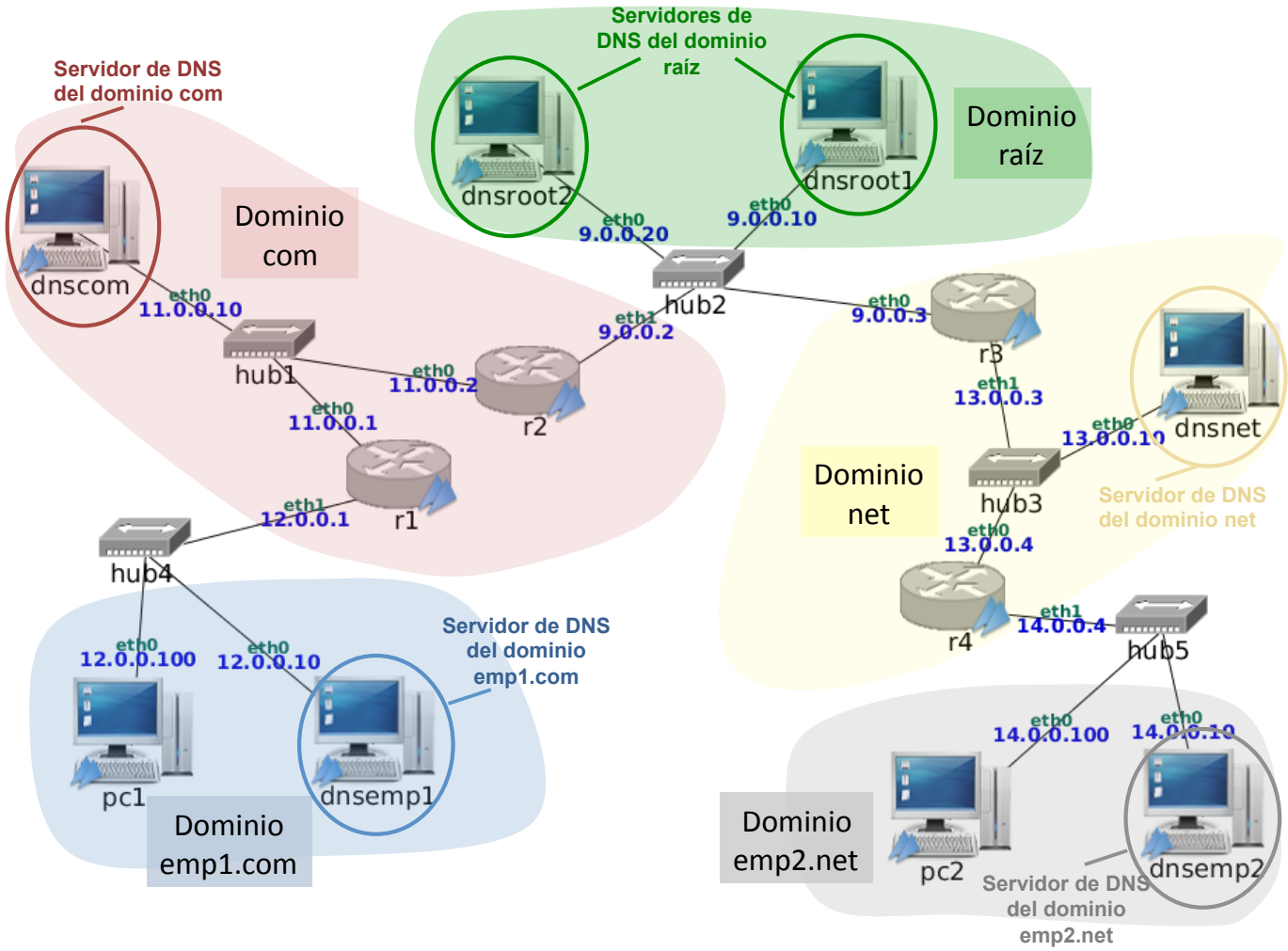

Figura 1: Árbol de dominios

- `db.root`:

  En el caso de los propios servidores de DNS del dominio raíz este fichero es el que contiene el mapa de dicho dominio raíz (dominio "."). Para el escenario de la práctica, el contenido de `db.root` en `dnsroot1` es:

Mapa del dominio raíz (en dnsroot1)

```
TTL             1d      ; default ttl
.                       IN      SOA     ROOT-SERVER1.   root.ROOT-SERVER1.
(
                                                2009120901 ; serial
                                                8h ; refresh
                                                4h ; retry
                                                1000h ; expire
                                                20m ; negative cache ttl
                                              )

.                       IN      NS      ROOT-SERVER1.
ROOT-SERVER1.           IN      A       9.0.0.10
dnsroot1.               IN      A       9.0.0.10

.                       IN      NS      ROOT-SERVER2.
ROOT-SERVER2.           IN      A       9.0.0.20
dnsroot2.               IN      A       9.0.0.20

com.                    IN      NS      dnscom.com.
dnscom.com.             IN      A       11.0.0.10

net.                    IN      NS      dnsnet.net.
dnsnet.net.             IN      A       13.0.0.10
```

Servidores de DNS del dominio raíz

Servidor de DNS del dominio com

Servidor de DNS del dominio net

En `dnsroot2` el fichero `db.root` tendrá un contenido similar, modificando los valores del registro SOA.

En el caso del resto de servidores (`dnscom`, `dnsnet`, `dnsemp1` `dnsemp2`) el fichero `db.root` contiene una relación inicial de IPs de servidores del dominio raíz[1].

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       9.0.0.10
ROOT-SERVER2.       518400  IN      A       9.0.0.20
```

Servidores de DNS del dominio raíz

- `db.*`:

  Los ficheros que empiezan por `db.` contienen el mapa del dominio que sirve un determinado servidor. Así, el servidor de DNS de `dnsemp1` sirve el mapa del dominio `emp1.com` y por tanto, tiene el fichero `/etc/bind/db.emp1.com` que contiene el mapa del dominio `emp1.com`:

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       12.0.0.10
pc1.emp1.com.       1s  IN      A       12.0.0.100
```

Servidor de DNS del dominio emp1.com

La siguiente tabla muestra las máquinas del escenario en las que se ha configurado `bind` para que sean 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`

Para ver el mapa de un cierto dominio puedes ejecutar la orden `less`[2] en la máquina que contiene dicho mapa:

```
less <fichero-del-mapa>
```

[1] La primera vez que un servidor tenga que enviar un mensaje a un servidor raíz, le enviará otro mensaje más con una consulta preguntando la lista de servidores del dominio raíz, por si hubiera habido cambios

[2] `less` es un visor de ficheros de texto, para salir de `less` pulsa `q`

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
```

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

```
rndc flush
```

1.3. Configuración de resolución de nombres en las máquinas

Todas las máquinas del escenario tiene configurado su fichero `/etc/nsswitch.conf` de tal 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`.

1.4. Programa host

Para interrogar al DNS puede utilizarse la orden `host`. Este programa es una herramienta que permite realizar consultas a un servidor de DNS, y lo usaremos este programa de la siguiente forma:

```
host <nombreDeMáquina>
```

El programa `host` devolverá 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.

1.5. Formato de los mensajes de DNS

El formato de mensaje de DNS tiene muchos campos. Para la realización de esta práctica consulta las transparencias 44–46 del tema de teoría que contienen resaltados los campos más importantes de los mensajes, que son los que debes intentar localizar en las capturas de `wireshark`.

2. 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 las capturas de tráfico que consideres necesarias para ver todos los mensajes de DNS generados[3]. Fíjate que al menos deberás realizar una captura en la red 12.0.0.0/24 ya que es ahí donde se encuentra conectado `pc1`, que es la máquina que va a enviar el primer mensaje de consulta. La captura en la red 12.0.0.0/24 la podrás obtener ejecutando `tcpdump` en cualquiera de las máquinas que están conectadas directamente a esta red, por ejemplo, podrías realizar la captura en la interfaz `eth1` de `r1`.

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.

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. 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 las capturas de tráfico que consideres necesarias 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 las capturas de tráfico que consideres necesarias para ver todos los mensajes de DNS generados.

11. 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?

12. Ejecuta la resolución anterior en `pc2`, realizando las capturas de tráfico que consideres necesarias para ver todos los mensajes de DNS generados. Explica lo sucedido comparado con lo ocurrido en el apartado 7.

13. Imagina que 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?

14. Ejecuta la resolución anterior en `pc1`, realizando las capturas de tráfico que consideres necesarias para ver todos los mensajes de DNS generados.

15. 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.

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

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

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

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

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

[3]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`.

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?

17. Ejecuta las órdenes anteriores, realizando las capturas que consideres necesarias para ver los mensajes de DNS.

18. 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`.

19. Ejecuta la resolución anterior en `pc1`, realizando las capturas de tráfico que consideres necesarias para ver todos los mensajes de DNS generados. Indica durante cuanto tiempo se obtendría esta/s misma/s captura/s.

3. Servidor esclavo

Vamos a cambiar la configuración de `dnsnet` para que se convierta en un servidor esclavo del dominio `emp2.net`. Para ello, en la máquina `dnsnet` copia el fichero `/etc/bind/named.conf2` a `/etc/bind/named.conf` mediante la instrucción:

```
dnsnet:~# cp /etc/bind/named.conf2 /etc/bind/named.conf
```

Ahora el fichero `/etc/bind/named.conf` de `dnsnet` contendrá las siguientes líneas:

```
zone "emp2.net" {
        type slave;
        masters { 14.0.0.10; };
        file "/etc/bind/db.emp2.net";
};
```

Donde se indica que el servidor `dnsnet`, que es el que tiene este fichero `named.conf`, es servidor esclavo del dominio `emp2.net`, y deberá pedir el mapa del dominio `emp2.net` a 14.0.0.10 (`dnsemp2`), almacenando dicho mapa cuando lo reciba en el fichero `db.emp2.net`.

Reinicia el servidor de DNS de `dnsnet` ejecutando en esta máquina:

```
dnsnet:~# /etc/init.d/bind restart
```

Una vez reiniciado el servidor de DNS de `dnsnet`, éste se bajará del maestro el mapa del dominio `emp2.net` y lo dejará en el fichero `/etc/bind/db.emp2.net`. Mira el contenido del directorio `/etc/bind` de `dnsnet` para ver si ha aparecido dicho fichero, utilizando la siguiente instrucción:

```
dnsnet:~# ls /etc/bind
```

1. ¿Crees que las resoluciones que realice `pc1` se verán beneficiadas por este cambio? Explica por qué.

2. En el servidor maestro del dominio `emp2.net`, abre con el editor `mcedit` el fichero del mapa `db.emp2.net`:

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

   Realiza los siguientes cambios en dicho mapa:

   - Modifica el registro A para que asocie el nombre `pc200.emp2.net` a la dirección IP 14.0.0.200. No hace falta que crees este nuevo PC en el dibujo.
   - Incrementa el número de serie dentro del registro SOA, para indicar que el fichero se ha actualizado.

Reinicia sólo los siguientes servidores: el servidor de DNS maestro del dominio `emp2.net` (para que cargue el nuevo mapa) y el servidor de DNS de `dnsemp1` (para que se borre la caché de este servidor).

3. Realiza la resolución de `pc200.emp2.net` desde `pc1` y también desde `pc2`. Explica el resultado. Haz las capturas que consideres necesarias.

4. ¿Qué crees que ocurriría si se reinicia el servidor de DNS de `dnsnet`?

   Compruébalo: reinicia el servidor de DNS de `dnsnet`, y el servidor de DNS de `dnsemp1` (para que se borre la caché de este servidor).

   Repite la resolución de `pc200.emp2.net` desde `pc1` y desde `pc2`.

   Comprobarás que desde `pc1` sigue sin obtenerse la nueva IP. Esto es debido a que aún no se ha cumplido el tiempo de refresco del mapa, por lo que `dnsnet` no comprueba si ha cambiado el número de serie en `dnsemp2`. Mientras no se cumpla el tiempo de refresco del mapa, `dnsnet` responde con la información que está en su mapa pero puede resultar obsoleta.

   Comprueba cuál es el tiempo de refresco en el mapa de `db.emp2.net`. Mira en `dnsnet` a qué hora se bajó la versión anterior del mapa con la instrucción:

   ```
   dnsnet:~# ls -l /etc/bind/db.emp2.net
   ```

   Espera a que pase el tiempo suficiente, y reinicia sólo el servidor de DNS de `dnsemp1` (para que se borre su caché).

   Realiza otra vez la resolución de `pc200.emp2.net` desde `pc1` para comprobar que ahora sí se obtiene la nueva IP.