

## PRÁCTICA 2: DNS (Domain Name System)

### 1 Objetivos

En esta práctica se pretende revisar el funcionamiento del servicio de resolución de nombres DNS, tanto desde vista del cliente como del servidor DNS.

### 2 Material

- PC Linux con conexión a Internet y paquete bind9 instalado

### 3 Servicio DNS

Se recomienda recordar el funcionamiento del servicio DNS. La RFC es <http://www.ietf.org/rfc/rfc1035.txt> y un resumen interesante está disponible en [http://es.wikipedia.org/wiki/Domain\\_Name\\_System](http://es.wikipedia.org/wiki/Domain_Name_System)

### 4 Cliente DNS

En el terminal de comandos de Linux hay 3 herramientas principales para hacer funciones de cliente DNS: dig, nslookup, y host. Puede trabajar con cualquiera de ellas (consulte el manual en línea de las mismas) aunque dig es la más flexible. Estas herramientas resuelven nombres de DNS igual que lo hace cualquier otra aplicación de la máquina. En concreto, la búsqueda de un nombre sigue el orden de búsqueda marcado por `/etc/nsswitch.conf`. En ese fichero, en la entrada hosts normalmente hace referencia a dos medios de búsqueda en orden, pasando al segundo si no se encuentra en el primero:

- 1- files: se mira el fichero `/etc/hosts` para buscar el mapeo
  - 2- dns: se realiza la consulta DNS contra el servidor marcado en `/etc/resolv.conf`
- 4.1 Compruebe su configuración de `/etc/nsswitch.conf`, `/etc/hosts` y `/etc/resolv.conf`, y deduzca cual va a ser el proceso de búsqueda de nombres en su máquina.
  - 4.2 Realice las consultas de nombres: `unavarra.es`, `www.unavarra.es` ¿Diferencias?
  - 4.3 Realice consultas de DNS de otros nombres de dominio ¿Qué es el servidor autoritativo?
  - 4.4 Realice las consultas de nombres inversas: `130.206.164.68` y de otras direcciones IP.
  - 4.5 ¿A qué servidor DNS está consultando? ¿Cómo lo puede cambiar?
  - 4.6 Con relación al dominio `www.navarra.es`, averigüe el nombre y dirección IP de los servidores de DNS de dicho dominio, y diga cuál es primario y cuáles secundarios.
  - 4.7 Obtenga el registro SOA (Start of Authority) del dominio `www.navarra.es` preguntándoselo al servidor DNS de google `8.8.8.8`, y preguntándoselo directamente al servidor primario del dominio `www.navarra.es`. Compruebe que

en un caso es información autorizada y en otro no.

- 4.8 Consulte la dirección IP de [www.elpais.com](http://www.elpais.com). ¿Cuánto tiempo almacenará en cache su DNS local este registro de recurso? Pregunte varias veces a su DNS local por esta dirección. ¿Qué observa en el TTL del registro de recurso?
- 4.9 Averigüe cuantas máquinas (diferentes direcciones IP) están detrás del dominio web [www.google.es](http://www.google.es). ¿Obtiene siempre las mismas y en el mismo orden? ¿Por qué?
- 4.10 Pregunte ahora lo mismo a un servidor raíz (por ejemplo J.ROOT-SERVERS.NET) y compruebe en el paquete de respuesta si dicho servidor acepta el modo recursivo.
- 4.11 Haciendo consultas iterativas (opción +norecurse de dig), averigüe la dirección IP de [www.timesonline.co.uk](http://www.timesonline.co.uk). ¿Qué pasos ha dado?
- 4.12 Puede hacer esto mismo con la opción +trace de dig. Compruebe el resultado que obtiene.
- 4.13 Utilizando la información disponible a través del DNS determine (nombre y dirección IP) la máquina o máquinas que actúan como servidoras de correo del dominio [tlm.unavarra.es](http://tlm.unavarra.es).
- 4.14 Repita una resolución de DNS capturando la petición y respuesta con Wireshark. Interprete la captura con la petición/respuesta obtenidas.

**Checkpoint P02.1:** Avisar al responsable de prácticas cuando haya completado las prácticas hasta este apartado. No se quede bloqueado, mientras tanto avance con las siguientes secciones.

## 5 Servidor DNS

El servicio de resolución de nombres se provee a través de un proceso corriendo en la máquina servidora. En concreto usaremos el paquete bind que es el servidor DNS más utilizado. Para saber si está instalado: `dpkg -l | grep bind9`

Detalles para la configuración del servidor los puede encontrar en <https://help.ubuntu.com/community/BIND9ServerHowto>

El paquete bind tiene por un lado el ejecutable de la aplicación servidora (llamado named) y por otro sus archivos de configuración (disponibles en `/etc/bind`). De los archivos de configuración, el principal es el `named.conf` que se encarga de hacer referencias al resto de ficheros de configuración.

En el caso del servidor de nombres se necesita un fichero de configuración por cada una de las zonas a definir. Cada zona va a ser un dominio de DNS directo, o una subred de la que realizar resolución inversa.

Al servidor se le puede preguntar:

- 1- Por un nombre de un ordenador de un dominio determinado: devuelve la IP
- 2- Por una IP de una subred determinada: devuelve el nombre DNS

- 3- Ídem con los dominios y redes por defecto, es decir, el localhost y su subred particular (127/8).
- 4- También se tiene que definir cómo se responderán a las preguntas sobre redes ajenas al control de este servidor (aquellas para las que este servidor no es autoritativo).

Para responder a cada pregunta, se tiene una lista (ordenada) que se denomina zona, por cada dominio o subred configurada en el servidor. Consiste en una lista de nombres DNS de una red determinada, una lista de IPs de una subred determinada, etc. Estas son las zonas que se definen en los ficheros de configuración.

Por defecto la instalación de bind trae una configuración muy básica que funciona sin realizar cambios.

- 5.1 Examine el fichero `/etc/bind/named.conf` y los archivos que referencia para entender la utilidad de cada entrada. ¿Qué zonas se definen y cuál es su función?
- 5.2 Habitualmente los servidores se lanzan como procesos en segundo plano. Lance el servidor con `“named -g”` para que el proceso no vaya en segundo plano y se vuelque en pantalla la información de debug ¿Qué error está obteniendo y por qué? Verifique el puerto que está utilizando el servidor DNS.
- 5.3 Copie el ejecutable `/usr/sbin/named` al directorio `~ /bind` para usar esa copia para lanzar el servicio en adelante.
- 5.4 Pruebe a lanzar el servidor con `“sudo privbind -u staXX ~/bind/named -g”` y observe de nuevo la salida en pantalla. ¿Para qué sirve `privbind`? Verifique el puerto que está utilizando el servidor DNS.
- 5.5 Para poder modificar los ficheros de configuración, copie la carpeta `/etc/bind/` a vuestro directorio `~ /bind`. Crear una carpeta en `~ bind/cache` para luego apuntar ahí la creación de los ficheros temporales del servidor.
- 5.6 Revisar la ruta a los ficheros que se referencian en `~/bind/named.conf` y la de todos los ficheros referenciados para que apunten ahora a su nueva localización (incluida la cache).

En `~ /bind/named.conf`, se pueden añadir otras opciones como el puerto e interfaz de escucha (`listen-on`) o la ruta donde se crea el identificador de proceso (`pid-file`).

- 5.7 Tenemos así la configuración mínima del servidor primario para resolver direcciones de loopback localmente y resolver de forma recursiva aquellas externas. Arrancar el proceso con sus ficheros de configuración `“sudo privbind -u staXX ~/bind/named -g -c /opt3/sta/staXX/bind/named.conf”` y verificar si ha arrancado correctamente. Puede obtener información extra de funcionamiento del servidor activando el debug con `“-d 1”` a la hora de lanzar el `named`.
- 5.8 Hacer un script de arranque del servicio en `$HOME/bind/named.sh` con la línea de comando anterior.
- 5.9 Realizar una consulta DNS y verificar que nuestro servidor DNS es el que contesta, viendo la salida de debug y los paquetes sobre la red.

A continuación hay más cambios de configuración. Por cada cambio, se sugiere probar (parar y arrancar el servidor para que actualice los cambios), comentar las entradas que se quieren modificar y añadir las nuevas entradas modificadas.

- 5.10 Cambiar nombres simbólicos (y/o IPs) de ordenadores, y añadir más. Tanto nombres DNS a IP, como de IP a nombres DNS. Por ejemplo, para que responda a la consulta de 127.0.0.2 con el nombre de “otro-localhost” (pista: fichero db.127).
- 5.11 Copiar el fichero db.local con el nombre db.mizona para los nombres asociados a “minombrededominio.com” (puede elegir el nombre de dominio de primer nivel que desee para ese “minombrededominio.com”). Configurar una nueva zona para el mapeo nombre ->IP (resolución directa) de nombre “minombrededominio.com” para que coja los nombres del fichero db.mizona.
- 5.12 Copiar el fichero db.127 con el nombre db.123 para mapear la resolución inversa de 1.2.3.0/24. Configurar una nueva zona para el mapeo inverso IP -> nombre (resolución inversa) para la red 1.2.3.0/24 con la configuración del fichero db.123
- 5.13 Crear la relación “yo.minombrededominio.com” con la IP 1.2.3.4 en ambos sentidos de la resolución directa e inversa.
- 5.14 Nuestro servidor ¿Conoce a priori las direcciones IP de los servidores DNS raíces?
- 5.15 Añada a su resolución la dirección IP y nombre DNS propia de su ordenador en el nuevo dominio (por ejemplo, tlm114.minombrededominio.com si trabaja en el ordenador tlm114). Lo mismo para las direcciones IP y nombres DNS de ordenadores próximos físicamente al suyo.
- 5.16 ¿En base a qué configuración sabe mi servidor DNS contestar a las peticiones de nombres de dominios externos como www.google.com? ¿Sabe resolverlos? Realice una petición iterativa contra su servidor de DNS de un dominio como www.ebay.co.uk y verifique el proceso de resolución que hace su servidor (mediante el log y captura de tráfico).
- 5.17 Configure como servidor de correo de “minombrededominio.com” el 10.1.1.1
- 5.18 Configure una entrada “upna.minombrededominio.com” que apunte a www.unavarra.es. Acceda en el navegador a “upna.minombrededominio.com”.
- 5.19 Verifique el TTL de “upna.minombrededominio.com” y cámbielo a 60 segundos.
- 5.20 ¿Qué necesitaría hacer para que otras máquinas del laboratorio pudieran resolver nombres de mi dominio? ¿Y para otras máquinas de Internet externas al laboratorio también pudieran resolver su nombre de dominio?
- 5.21 Configure un registro TXT en su dominio. ¿Para qué sirve?
- 5.22 Configure un subdominio del tipo “subdominio.minombrededominio.com” y añada algunas entradas para la resolución directa e inversa.
- 5.23 Hasta ahora se ha trabajado con un servidor primario. Configure un segundo servidor en otra máquina que sea servidor secundario (slave) del que ya tiene configurado. Verifique su funcionamiento.

**Checkpoint P02.2:** Avisar al responsable de prácticas cuando haya completado las prácticas hasta este apartado. No se quede bloqueado, mientras tanto avance con las siguientes secciones.