Sumario

UT 03: Servicio de resolución de nombres (DNS)

1 Introducción

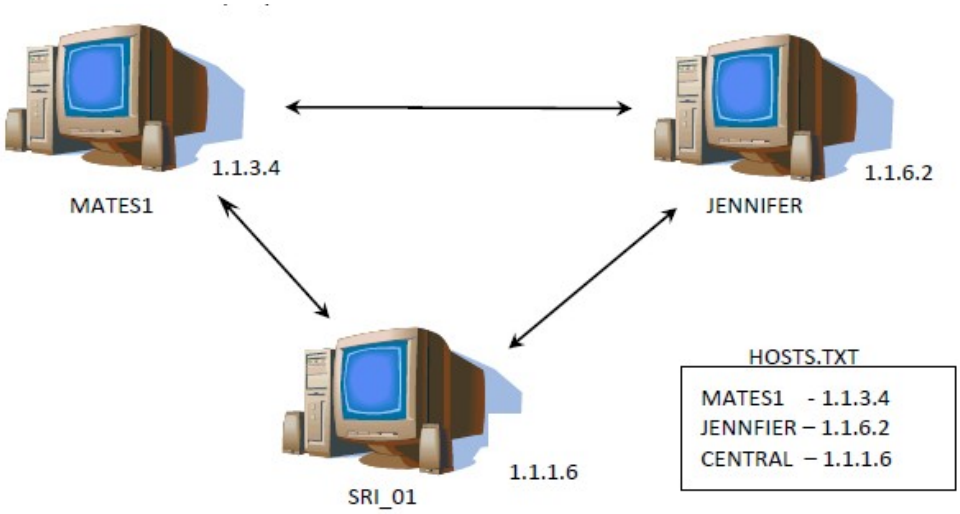
Todos los nodos de una red deben tener una dirección IP (siglas en inglés de Internet Protocol, traducido significa Protocolo de Internet). El protocolo IP utiliza esta dirección para identificar los distintos nodos de Internet. Las direcciones IP se organizan en cuatro grupos de 8 bits y una dirección se representa de esta forma: 208.86.217.103.

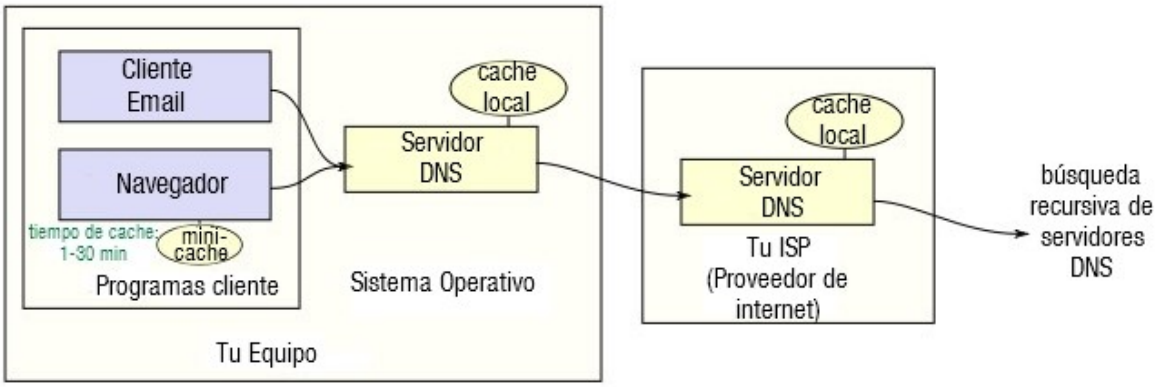
Las direcciones IP son difíciles de recordar y, por lo tanto, es muy engorroso su manejo. A las personas nos resulta más fácil acordarnos de www.google.es que de un conjunto de números.

El DNS (siglas en inglés de Domain Name System, traducido significa Sistema de Nombres de Dominio) tiene por objeto facilitar esta tarea y permite traducir una dirección del tipo www.google.es a una dirección IP y viceversa.

Por lo tanto, DNS es una base de datos distribuida, con información que se usa para traducir los nombres de dominio en números de protocolo de Internet (IP).

Los nombres son más fáciles de recordar y usar por las personas, pero hay que tener en cuenta, que la expresión numérica es la forma en que las máquinas pueden encontrarse en Internet.





Autoevaluación:

Rellena los huecos con los conceptos adecuados

DNS es una …… con información que se usa para traducir ……., fáciles de recordar y usar por las personas, en números de protocolo de Internet (……), que es la forma en la que, las máquinas pueden encontrarse en Internet.

***Respuestas**: Base de datos distribuida / Nombres de dominio / Direcciones IP*

2 Sistemas de nombres planos y jerárquicos

En los primeros días de ARPANET, antecesor de la Internet actual, sólo existía un pequeño número de equipos conectados a la red. El Centro de Información de Red (NIC), ubicado en el Instituto de Investigaciones de Stanford, SRI (Stanford Research Institute), era el responsable de compilar en un único archivo, HOSTS.TXT, los nombres y direcciones de todos los equipos. Los administradores debían mandar un mensaje al SRI, que actualizaba el archivo HOSTS.TXT. Después los usuarios de ARPANET debían descargar la nueva versión del archivo mediante FTP ("File Transfer Protocol"). Con el crecimiento de ARPANET, resultaba obvio que este método no era práctico, ya que:

- El ancho de banda consumido para transmitir las versiones actualizadas de un archivo de host de ARPANET crecía exponencialmente con el número de hosts incrementándose de forma continua (Con 100 hosts ya había que mandar un archivo de 100 KB a 100 equipos, ocupando un ancho de banda de 10.000 KB).
- El archivo de hosts plano y estático significaba que no podría haber dos equipos en la ARPANET con la misma dirección. Al crecer el número de hosts, crece el riesgo de añadir nombres duplicados y la dificultad de intentar un control centralizado.

- La naturaleza de la red subyacente estaba cambiando, los grandes equipos de tiempo compartido con que se había construido ARPANET se estaban viendo desplazados por miles de estaciones de trabajo y cada una necesitaba un nombre de host único. Empezaba a ser imposible controlar todos estos nombres centralizadamente desde un único equipo.

Se necesitaba una solución mejor. Se generaron varias propuestas según el concepto de servicio de nombres distribuido, que se basaban en un espacio de nombres jerárquico. Nacieron las RFC 882 y 883, donde se describe el diseño de un **sistema de nombres de dominio**, basado en una **base de datos distribuida** con información generalizada de recursos.

Este diseño evolucionó, y las RFC 1034 y 1035 describen el servicio del Sistema de nombres de dominio (DNS) que se usa hoy en Internet.

La jerarquía se utiliza para construir el nombre completo de cada uno de los elementos de la red, y está relacionada con su ubicación geográfica, con el departamento de una empresa u otra información que permita identificar a cada elemento.

Los organismos encargados de otorgar los nombres de dominio son:

- A nivel internacional, el “Internet Corporation for Assigned Names and Numbers (ICANN - https://www.icann.org/es)
- A nivel de España, todos los nombres de dominio que están bajo las siglas .es forman parte de la red.es del Gobierno de España (y se pueden consultar en http://dominios.es)

3 Espacio de nombres de dominio: dominio raíz, dominios superiores. Delegación de dominios.

Cuando un equipo se comunica con otro debe resolver, o convertir, un nombre de equipo en una dirección de IP. Esta conversión se realiza mediante un servicio de resolución de nombres. El espacio de nombres define las reglas para dar nombre a un equipo y cómo se resuelve un nombre en una dirección IP.

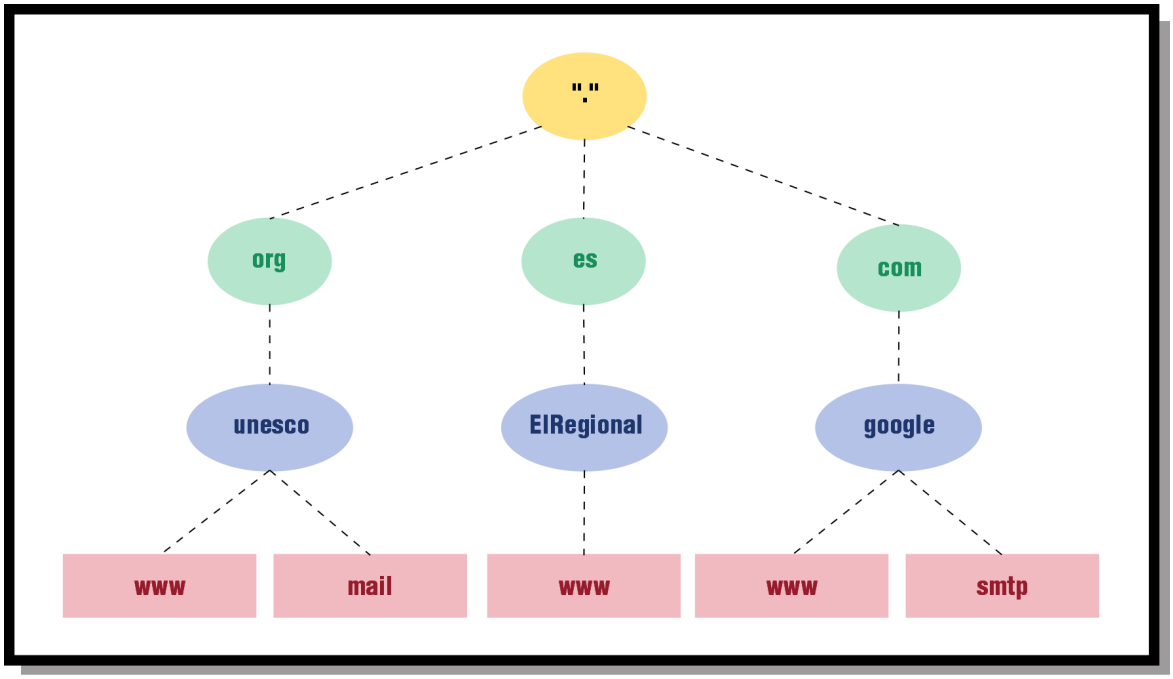
DNS es el servicio de nombres estándar. El servicio de DNS permite que un equipo cliente de la red registre y resuelva nombres de dominio de DNS. Estos nombres se utilizan para encontrar y acceder a recursos de otros equipos de la red o de otras redes como Internet. Los tres componentes principales de DNS son los siguientes:

- **Clientes DNS:** Un programa cliente DNS se ejecuta en el ordenador del usuario, generando peticiones DNS de resolución de nombres a un servidor DNS (Por ejemplo: ¿Qué dirección IP corresponde al nombre www.madrid.org ?).
- **Servidores DNS:** Contestan las peticiones de los clientes. Los servidores

recursivos tienen la capacidad de reenviar la petición si no disponen de la dirección solicitada.

- **Zonas de autoridad:** Porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.

El **espacio de nombres de dominio** está estructurado de manera jerárquica en un árbol que empieza en una raíz sin nombre para todas las operaciones de DNS. En el espacio de nombres DNS cada nodo y hoja del árbol representa un dominio con nombre. Cada dominio puede tener dominios hijos adicionales.



3.1 Nombre de dominio

El nombre de dominio completo o **FQDN (Full Qualified Domain Name)** incluye el nombre de la máquina o host, más los sucesivos dominios de orden jerárquico superior hasta la raiz, separados por puntos. El nombre de dominio completo no puede exceder de 255 caracteres (sumando letras, dígitos y guiones, único carácter especial admitido). Cada etiqueta (nombre de dominio o subdominio) puede tener hasta 63 caracteres.

Los nombres de dominio se pueden almacenar en mayúsculas o en minúsculas indistintamente, ya que todas las comparaciones y funciones de dominios se definen como insensibles a mayúsculas y minúsculas. Por tanto, www.midominio.com es idéntico a WWW.MIDOMINIO.COM para las operaciones DNS.

Ejemplos de nombres de FQDN serían, por ejemplo, www.google.com o es.Wikipedia.org. A la etiqueta ubicada más a la derecha (sin contar el punto) se le llama dominio de nivel superior (Top Level Domain). Como "com" en www.google.com o "es" en www.Wikipedia.es

Cada etiqueta a la izquierda especifica una subdivisión o subdominio. (No hay que confundir los “dominios y subdominios” DNS con los dominios y subdominios de Windows). En teoría, esta subdivisión puede tener hasta 127 niveles, siempre que la longitud total del nombre del dominio no exceda los 255 caracteres. En la práctica los dominios son casi siempre mucho más cortos.

La parte más a la izquierda del dominio suele expresar el nombre de la máquina (hostname) o incluso un prefijo como www, ftp, etc, que no forma parte real del nombre DNS y solo se utilizan para indicar que tipo de protocolo se va a usar para la conexión.

Resumen:

Diferencia entre **DNS**, **nombre de dominio**, **FQDN** y **URL** (sigla en inglés de uniform resource):

- ✔ DNS es un servidor de nombres de dominio.
- ✔ Nombre de dominio es un alias de una dirección IP, como ElRegional.es.
- ✔ FQDN es un nombre de dominio que identifica el trayecto completo hasta un equipo como Pc1.ElRegional.es.
- ✔ URL es el trayecto completo a un archivo o recurso de Internet como http://www.ElRegional.es/herramientas/herramientas.aspx.

Autoevaluación

De entre los siguientes nombres, marca todos los que pueden ser un nombre de dominio:

(a) www.wikipedia.org.
(b) ftp.rediris.es.
(c) Pc1.ElRegional.es.
(d) Cpd.unesco.org.

Solución: a y b

3.2 Dominios de primer nivel

Cuando quieras alquilar un dominio, solo puedes hacerlo con uno de segundo nivel. Es decir, este siempre tendrá que terminar en .com, .es, .fr, .org, etc. Para el publico en general y empresas no se permite comprar un domino de primer nivel.

Los dominios de primer nivel son:

- **Dominios genéricos o gTLD** (sigla en inglés de Generic Top level Domain) son aquellos que tienen tres o más letras: .com, .org, .info, .pro son algunos ejemplos.

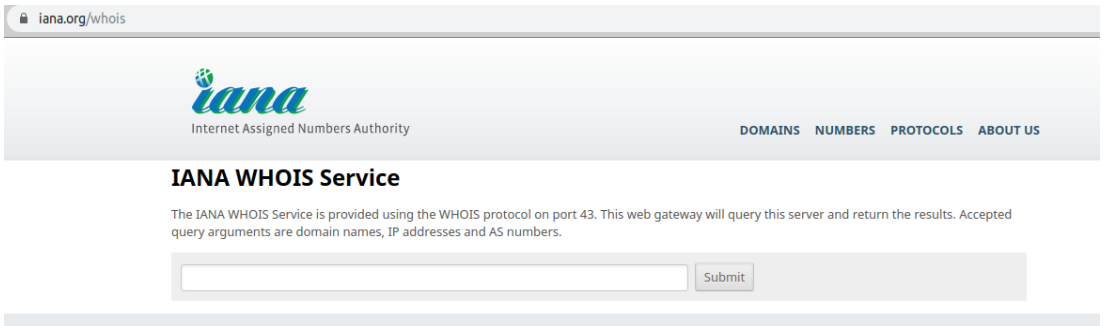
- **Dominios geográficos o ccTLD** (sigla en inglés de Country-Code Top_level Domain) son los formados por dos letras y en general hacen referencia a un país: .es, .uk, .us, .fr son algunos ejemplos. Piensa a que países corresponden.

- **Dominio .arpa** es una excepción y por eso aparece aparte. Este dominio se usa para poder obtener el nombre completo (FQDN) de una dirección IP. Ejemplo 5.78.200.100.in-addr.arpa.

En el RFC se propuso definir una serie de dominios de primer nivel reservados. Estos dominios no aparecen en la jerarquía de DNS en Internet, ya que están reservados y nunca se van a asignar a nadie. La razón de hacer esto es para usar dominios inexistentes a la hora de hacer pruebas en el servidor DNS. Los dominios reservados son .test, .example, .invalid, .localhost.

ICANN es la entidad que decide si un dominio de primer nivel debe existir o no. Visita su página Web: www.icann.org

Whois (https://www.iana.org/whois) es una base de datos distribuida que te puede informar de los datos de un dominio DNS. Esta base de datos puede ser usada para obtener información sobre el usuario registrante, el registrador o el listado de servidores de nombres para un determinado dominio.



3.3 Delegación de dominio / Delegación de zona

La delegación de zona DNS es el proceso por el cual el gestor de un determinado dominio delega la gestión del mismo a otra entidad. Por ejemplo, ICANN delega la gestión del ccTLD “es” a la empresa pública Red.es. A partir de aquí, ICANN ya no se encargará de gestionar este dominio.

Este proceso se puede repetir varias veces. A su vez, Red.es deberá gestionar el alta de los dominios jerárquicamente inferiores, y puede delegar en empresas para que estas gestionen los nombres bajo su autoridad.

Autoevaluación

Los dominios de primer nivel son:

(a) Genéricos
(b) Geográficos
(c) Genéricos, geográficos y .arpa.
(d) Genéricos y geográficos

Solución: c

4 Funcionamiento DNS: características, consultas iterativas/ recursivas; resolución directa/inversa.

Los servidores DNS realizan estas operaciones típicas:

1. **Resolución de nombres:** Convertir un nombre de host en la dirección IP que le corresponde. Por ejemplo, al nombre de dominio www.google.es, le corresponde la dirección IP 216.58.211.55.
2. **Resolución inversa de direcciones:** Es el mecanismo inverso al anterior, de una dirección IP obtener el nombre de host correspondiente.
3. **Resolución de servidores de correo:** Dado un nombre de dominio (por ejemplo gmail.com), obtener su servidor de correo electrónico.

4.1 Resolución directa

Cuando escribimos en nuestro navegador la dirección de una página web, por ejemplo: **http://www.sitio.com**, a la que en otras ocasiones hemos accedido, es probable que la caché de nuestro navegador o en la del servidor del que depende nuestra conexión, tengamos registrada la dirección IP que le corresponde, por lo que la conexión será directa, sin intermediarios.

4.2 Operación de solicitud DNS

Cuando nuestra maquina necesita resolver un nombre de dominio (por ejemplo www.bekkoame.co.jp), enviará una petición **por el puerto 53** al servidor DNS (configurado en las propiedades de red). Si nuestro servidor DNS tiene respuesta a nuestra petición nos la enviará directamente, con lo que sabremos que su dirección ip es 202.11.252.20. Pero es bastante habitual que nuestro servidor DNS no tenga ningún registro sobre ese nombre (sería imposible e indeseable que en un solo servidor estuvieran almacenados todos los nombres de todas las máquinas de internet).

En estos casos, nuestro servidor DNS manda una petición de ayuda a un servidor de nivel superior, como los servidores root de Internet (hay 13 root-servers principales en internet). El servidor root normalmente no devuelve la dirección IP de nuestra petición, sino que busca la dirección IP del servidor DNS que tiene autoridad (SOA, Start of Autority) sobre nuestra petición. En nuestro caso, y como nuestra petición www.bekkoame.co.jp pertenece a Japón (jp) nos devolvería la dirección a un servidor con autoridad sobre Japón.

Ahora realizaremos la petición al nuevo servidor DNS de Japón, que normalmente responderá. Si no puede encontrar el host, obtendríamos el mensaje de host inexistente.

4.3 Solicitud inversa

Una solicitud inversa es aquella en la que se solicita a un servidor de DNS el nombre de dominio de DNS de un host con una dirección de IP para que nos devuelva el nombre.

4.4 Clases de solicitudes

Las solicitudes de DNS pueden ser de dos clases: recursivas o iterativas.

- Una solicitud **recursiva** es una solicitud de DNS que se envía a un servidor de DNS en la que el host solicitante pregunta al servidor de DNS para que le proporcione una **respuesta completa** a la solicitud, aunque ello signifique que tenga que ponerse en contacto con otros servidores para obtener la respuesta.
- Una solicitud **iterativa** es una solicitud de DNS en la que el host solicitante pide que se devuelva la **mejor respuesta** que el servidor de DNS pueda proporcionar, sin ayuda de otros servidores de DNS, es decir, se obtiene la dirección de otro servidor intermedio, que puede no ser el servidor de autoridad del dominio buscado, pero está más cerca que el anterior. El servidor consultará directamente al intermedio que acaba de recibir y así sucesivamente, hasta llegar al servidor autorizado.

En general, los equipos envían solicitudes recursivas. Los equipos suponen que el servidor de DNS conoce la respuesta a la solicitud, o puede encontrarla. Por otra parte, un servidor de DNS normalmente enviará solicitudes iterativas a otros servidores de DNS si no puede responder a la solicitud con la información de que dispone.

Autoevaluación:

La consulta se envía al servidor DNS primario, y si este no contesta, se usa el secundario. La comunicación se realiza por el puerto:

✔ *33*
✔ *35*
✔ *53*
✔ *63*

Respuesta: 53

5 Servidores de nombres

5.1 Tipos de servidores

Hay un conjunto de servidores de nombres denominados autoritativos porque son los que tienen la información real y veraz de la zona. Pueden ser de dos tipos:

- **Primario:** Es el servidor principal, a veces llamado master, de la zona. En él, el administrador del DNS efectúa las operaciones de alta y baja de nombres.
- **Secundarios:** el resto de servidores de la zona, que contienen copia de la zona, habitualmente obtenida del servidor primario.

Para cada zona deberemos tener un servidor primario y uno o más secundarios. Existen otros tipos de servidores DNS:

- **Reenviador:** denominados forwarders en ingles, es un servidor DNS que recibe las consultas DNS externas hacia fuera de una red corporativa en la que existan varios servidores DNS.

- **Cache:** Es un tipo de servidor DNS que no es autoritativo (ni primario ni secundario) de ninguna zona en especial. Se usa para que el trafico DNS al exterior disminuya. También se puede usar para no sobrecargar los servidores autoritativos de una zona. Un ISP puede definir que el servidor DNS que usan sus clientes no sea uno de los servidores de su zona sino que puede configurar un servidor caché que solo sirve para atender las peticiones de estos clientes.

5.2 El servicio de servidores públicos DNS de Google.

Desde Diciembre del 2009, Google ofrece un servicio público de DNS, que ha contribuido a que la internet sea más rápida. Es un servicio gratuito que goza de gran popularidad. Su uso permite incrementar el rendimiento de nuestra conexión, con gran eficiencia debida a la efectiva dispersión geográfica de los servidores.

Dirección IP de los servidores DNS de Google:

- Para el protocolo IPv4.
  - Servidor primario: 8.8.8.8
  - Servidor secundario: 8.8.4.4
- Para el protocolo IPv6
  - Servidor primario: 2001:4860:4860::8888
  - Servidor secundario: 2001:4860:4860::8844

5.3 El servicio OpenDNS.

Otros servidores DNS muy eficientes y renombrados son los de **OpenDNS**.

Dirección IP de los servidores de OpenDNS

- Servidor primario: 208.67.222.222
- Servidor secundario: 208.67.220.220

Existen en internet otros servicios que se pueden utilizar. Incluso debido a su ubicación geográfica algunos de ellos pueden resultar más eficientes en tu caso.

6 Clientes DNS (resolvers). Herramientas de consulta DNS. Caché del resolutor

Hay varias formas de realizar consultas de DNS.

6.1 Conocer los servidores DNS usando la consola de Microsoft Windows

En Windows, abrimos un consola de comandos y escribimos el comando:

```
ipconfig /all|FINDSTR /C:"Servidores DNS"
```

También se puede usar el comando `nslookup`, tanto en Windows como Linux.

6.2 Conocer los servidores DNS usando la consola de GNU/Linux.

Para identificar la IP de una URL conocida:

```
jose@Audax:~/Desktop$ nslookup www.google.es
Server:         127.0.0.53
Address:   127.0.0.53#53

Non-authoritative answer:
Name: www.google.es
Address: 216.58.214.163
Name: www.google.es
Address: 2a00:1450:4003:80a::2003
```

El dominio y servidor DNS se configuran en el archivo `/etc/resolv.conf`, así como la IP del servidor DNS que usamos.

6.3 Conocer los servidores DNS manualmente en la conexión de red.

Los servidores DNS aparecen en las propiedades del protocolo TCP/IP de la conexión con la cual te conectas a internet.

6.4 Resolución de nombres. Resolutor DNS (Resolver)

El resolutor (o "resolver") de DNS es un componente del sistema, que realiza solicitudes de DNS a otro u otros servidores de DNS.

En el caso de Windows, la pila de TCP/IP se configura, normalmente, con la dirección IP de al menos un servidor de DNS al que el resolutor envía una o más solicitudes de información de DNS. El servicio cliente se instala automáticamente con TCP/IP.

6.5 Caché del resolutor DNS

Un host podría necesitar ponerse en contacto periódicamente con otro host y por tanto necesitaría resolver un nombre concreto de DNS muchas veces (por ejemplo el nombre del servidor de correo electrónico). Para evitar tener que enviar solicitudes a un servidor de DNS cada vez que el host quiere resolver el nombre, los servicios cliente de DNS mantiene una caché de respuestas recibidas a las solicitudes de DNS.

La información se mantiene durante un Período de vida TTL (Time To Live) y se puede utilizar para responder solicitudes posteriores. De forma predeterminada, la caché utiliza el valor de TTL recibido en la respuesta de solicitud de DNS, que es definido por el servidor autoridad de DNS.

En Windows se puede usar `IPCONFIG /DISPLAYDNS` para mostrar la caché del resolutor.

6.6 Caché negativa

El servicio Cliente de DNS también utiliza una **caché negativa**. La caché negativa ocurre cuando no existe registro de un nombre de dominio solicitado o cuando el propio nombre de dominio no existe, en cuyo caso se guarda la **falta de resolución**. La caché negativa evita repetir solicitudes adicionales de recursos o dominios que no existen.

Si se realiza una solicitud a un servidor de DNS y la respuesta es negativa, las siguientes solicitudes al mismo nombre de dominio se responden negativamente durante un tiempo predeterminado de 300 segundos. Para evitar guardar en la caché información negativa anticuada, cualquier información de solicitud respondida negativamente se mantiene durante un período de tiempo inferior al que se utiliza para las respuestas positivas. Con la caché negativa se reduce la carga en los servidores de DNS.

Si se realiza una solicitud a todos los servidores de DNS y no está disponible ninguno

durante un tiempo predeterminado de 30 segundos, las solicitudes posteriores por nombre fallarán inmediatamente en lugar de esperar los plazos. De esta forma se puede ahorrar tiempo en servicios que utilizan DNS durante el proceso de arranque, sobre todo cuando se arranca de la red.

Para vaciar la caché en Windows se usa la orden `IPCONFIG /FLUSHDNS` (también elimina la caché negativa).

7 Bases de datos del servicio

Como vimos anteriormente, cada servidor DNS se encarga de resolver nombres de uno o varios dominios. A las ramas del árbol jerárquico de nombres que resuelve un servidor se le denomina **zona**.

Lo normal es que cada zona tenga un servidor primario que obtiene los datos de un fichero y uno o más secundarios que obtienen los datos de un servidor primario. Los servidores de nombres situados inmediatamente por encima en el árbol del espacio de nombres apuntarán a los servidores encargados de resolver estas zonas, de tal forma que estos servidores responderán directamente a peticiones de nombre que pertenezcan a su zona.

Hay que distinguir entre **zona** y el de **dominio**. Una zona es un concepto que representa a uno o más dominios, conteniendo sus datos. Un dominio es un nombre que agrupa a otras computadoras o subdominios. Normalmente, además del servidor primario de zona, se dispone de uno o más servidores secundarios. Para que los ordenadores usen datos correctos, los secundarios piden información al servidor primario (transferencia de zona).

Todos estos datos deben guardarse de alguna forma en el servidor de nombres. La opción escogida es almacenarlos como una serie de entradas de texto, formando lo que se conoce como un **registro de recursos (RR)**. En el servicio BIND, estos registros se recogen en archivos denominados "db".

Un registro de recursos está compuesto por cinco campos cuyo formato es:

[Propietario] [TTL] [clase] [Tipo de Registro] [RDATA - Valor del dato]

- **Propietario**: Nombre de la máquina o dominio DNS al que pertenece el recurso. El símbolo "@" indica el nombre de la zona.
- **TTL**: tiempo de vida. Indica cuánto tiempo ha de guardarse un registro en caché.
- **Clase**: familia de protocolos en uso. Actualmente solo se usa IN (de Internet).
- **Tipo de registro**. En función de la clase (ver tabla más abajo).
- **RDATA**: puede ser un número, un nombre de dominio o una cadena ASCII.

Los tipos de registros son los siguientes:

Registro	Función
SOA	Inicio de autoridad. Fija los parámetros de la zona.
NS	Servidor de Nombre. Nombre de un servidor autorizado para el dominio.
A	Dirección de anfitrión. Asigna a un nombre una dirección.
CNAME	Nombre canónico. Establece un alias para un nombre verdadero.
MX	Intercambio de correo. Especifica qué máquinas intercambian correo.
TXT	Texto arbitrario. Forma de añadir comentarios.
PTR	Puntero. Permite la conversión de una dirección a nombre.
HINFO	Descripción de la computadora. CPU y S.O.
WKS	Servicios Públicos disponibles en la computadora

7.1 Registro SOA.

Cada zona contiene un registro de recursos denominado Inicio de Autoridad o SOA (Start of Authority) al comienzo de la zona. Los registros SOA incluyen los siguientes campos (sólo se incluyen los que poseen un significado específico para el tipo de registro):

- ✔ **Propietario**: nombre de dominio de la zona.
- ✔ **Tipo**: "SOA".
- ✔ **Persona responsable**: contiene la dirección de correo electrónico del responsable de la zona. En esta dirección de correo se utiliza un punto en el lugar del símbolo "@".
- ✔ **Número de serie**: muestra el número de versión de la zona, es decir, un número que sirve de referencia a los servidores secundarios de la zona para saber cuándo deben proceder a una actualización de su base de datos de la zona (o transferencia de zona). Cuando el número de serie del servidor secundario sea

menor que el número del maestro, esto significa que el maestro ha cambiado la zona, y por tanto el secundario debe solicitar al maestro una transferencia de zona. Por tanto, este número debe ser incrementado (manualmente) por el administrador de la zona cada vez que realiza un cambio en algún registro de la zona (en el servidor maestro).

- ✔ **Actualización**: muestra cada cuánto tiempo un servidor secundario debe ponerse en contacto con el maestro para comprobar si ha habido cambios en la zona.

- ✔ **Reintentos**: define el tiempo que el servidor secundario, después de enviar una solicitud de transferencia de zona, espera para obtener una respuesta del servidor maestro antes de volverlo a intentar.

- ✔ **Caducidad**: define el tiempo que el servidor secundario de la zona, después de la transferencia de zona anterior, responderá a las consultas de la zona antes de descartar la suya propia como no válida.

- ✔ **TTL mínimo**: este campo especifica el tiempo de validez (o de vida) de las respuestas "negativas" que realiza el servidor. Una respuesta negativa significa que el servidor contesta que un registro no existe en la zona. Hasta la versión 8.2 de BIND, este campo establecía el tiempo de vida por defecto de todos los registros de la zona que no tuvieran un campo TTL específico. A partir de esta versión, esto último se consigue con una directiva que debe situarse al principio del fichero de la zona. Esta directiva se especifica así:

  $TTL tiempo

Un ejemplo de este registro es:

```
ejemplo.es. IN SOA servidor.ejemplo.es. root.servidor.ejemplo.es. (
1998072701 ; Serial Number
86400      ; Refresh 24 hours
3600       ; Retry 1 hour
3600000    ; Expire 1000 hours
86400 )    ; Minimun 24 hours
```

Con este registro, se indica que el dominio ejemplmacenarlos como una serie de o.es está controlado por la computadora servidor y que el correo lo envíe al root de dicha máquina. Los secundarios se conectarán cada 24 horas al primario, si el número de serie es menor que el del primario, realizar una transferencia de zona para actualizarse (ya que el primario se habrá actualizado). Si el secundario no logra conectarse, se le indica que lo reintente dentro de una hora y si no es capaz de hacerlo en 1.000 horas, que deje de responder a consultas de resolución. El valor de 86.400 (24 horas) que se indica en el registro SOA, es el valor por defecto usado para los registro en los que no se indica el TTL

(este es el funcionamiento implementado, aunque no el definido en la RFC 1035).

A veces aparece en vez como nombre de dominio una arroba (@), que representa al propio nombre del dominio.

Para cada zona existirá un solo registro SOA.

7.2 Registro NS.

El registro de recursos NS indica los servidores de nombres autorizados para la zona. Cada zona debe contener registros indicando tanto los servidores principales como los secundarios. Por tanto, cada zona debe contener, como mínimo, un registro NS.

Por otra parte, estos registros también se utilizan para indicar quiénes son los servidores de nombres con autoridad en subdominios delegados, por lo que la zona contendrá, al menos, un registro NS por cada subdominio que haya delegado.

El formato es el siguiente:

```
    [nombre_zona]        IN  NS    [FQDN del Servidor]
```

Deben existir tantos registros NS como servidores de nombres hay para esa zona. Estos servidores pueden estar dentro de la misma zona o fuera de esta.

```
    miempresa.es.          IN          NS          dns1.miempresa.es.
    miempresa.es.          IN          NS          dns2. miempresa.es.
    miempresa.es.          IN          NS          dns.otro-sitio.com.
    miempresa.es.          IN          NS          dns.otro_lugar.eu.
```

7.3 Registro MX.

Los registros MX indican el servidor es de correo electrónico que son los encargados de recibir email para el nombre de dominio indicado.

```
[nombre_zona]             IN    MX    [Prioridad]     [FQDN del Servidor]
```

En este caso, nombre puede ser o bien un dominio (google.com, miempresa.es.) o bien el nombre de un ordenador (pc-direccion.miempresa.es.). El campo prioridad indica la prioridad de ese servidor. Cuanto más bajo sea ese número, mayor prioridad.

```
miempresa.es.   IN   MX   10   correo.miempresa.es.
miempresa.es.   IN   MX   20   correo2.miempresa.es.
miempresa.es.   IN   MX   30   smtp.otro-sitio.es.
```

7.4 Registro A.

Los registro que hemos visto anteriormente son importantes pero no nos permiten especificar una dirección IP. Eso es lo que hace un registro A.

```
[nombre del host]              IN      A     [Dirección IP]
```

Nombre puede ser o bien un FQDN o un nombre relativo.

```
ldap.miempresa.es.    IN            A              130.206.8.10
pc-direccion          IN            A              130.206.7.200
```

7.5 Registro CNAME.

Estos registros se usan cuando quiero que varios nombres apunten al mismo ordenador.

```
     [alias]             IN           CNAME    [nombre verdadero]
```

Alias hace referencia a todos los nombres que queremos que apunte a la misma máquina con definida antes como un nombreen un registro A.

```
     pop3      IN            CNAME      ldap
     imap      IN            CNAME      ldap
     smtp      IN            CNAME      ldap
```

Los CNAME no tienen por qué apuntar a algo dentro del mismo dominio sino que pueden apuntar a algo en otro dominio. En el caso que nuestro servidor web este hospedado en otro servidor de la empresa.

```
     www      IN CNAME ghs.google.com.
```

Es importante señalar que las entradas CNAME no se pueden usar para servidores DNS (entradas NS) ni para servidores de correo (entradas MX).

7.6 Registros PTR. Resolución Inversa.

La operación más habitual es obtener la dirección IP de un nombre de nodo, pero a veces queremos hacer la operación opuesta: encontrar el nombre asociado a la dirección IP. Diversas aplicaciones usan resolución inversa para comprobar la identidad del cliente.

Cuando se usa el fichero hosts, se podría resolver con una búsqueda simple en el fichero. Con DNS, la búsqueda de IPs se hace demasiado compleja. Existe un dominio especial, el **in-addr.arpa**, que contiene las direcciones IP de todos los sistemas en **notación de puntos invertida**. A la dirección 1.2.3.4 le correspondería el nombre 4.3.2.1.in-addr.arpa.

El registro de recurso (RR) que define esto se llama registro PTR. Para configurar la zona de búsqueda inversa se escribe en el fichero /etc/named.conf.local una entrada como:

```
[nombre_in-addr]      IN    PTR   [nombre FQDN]
10.8.206.130.in-addr.arpa. IN    PTR   ldap.miempresa.es.
```

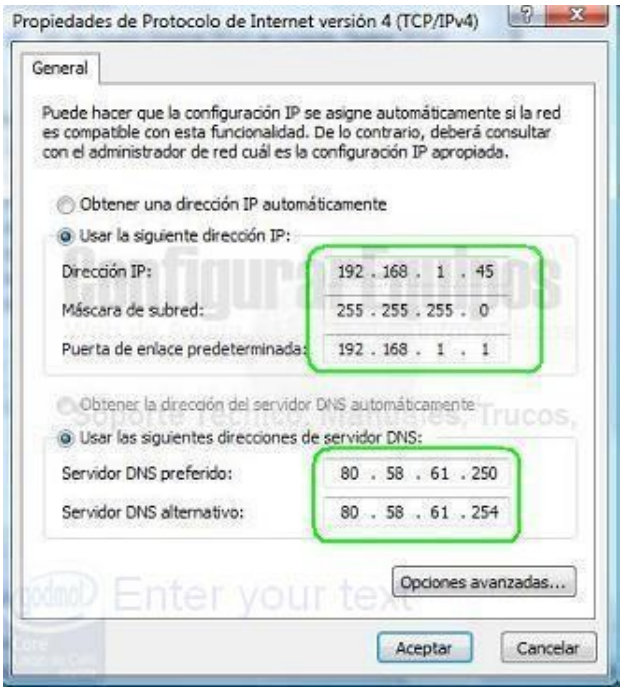
8 Servicio DNS en Windows.

8.1 Configuración básica

Una de las tareas que más tendrás que realizar, si alguna vez eres administradora o administrador de una red, es configurar los clientes de los servidores DNS. La verdad que no es una tarea complicada y es posible que ya la conozcas, pero vamos a repasarlo.

Un cliente DNS en Windows, al igual que en cualquier otro sistema operativo, necesita una configuración mínima. Normalmente, ésta se recibe mediante el protocolo DHCP si existe un servidor DHCP en la LAN a la que estamos conectados. Pero algunas veces necesitaras realizar la configuración manual.

Para que un cliente DNS funcione correctamente, es necesario especificar la dirección IP de al menos un servidor DNS. En Windows, se realiza en ***propiedades de conexión de área local***, una opción que puede variar ligeramente en función del sistema Windows en que te encuentres. Dentro de esta opción seleccionas ***Protocolo de Internet versión 4*** y hacemos clic en ***propiedades***. Entonces aparecerá la pantalla capturada a la derecha.

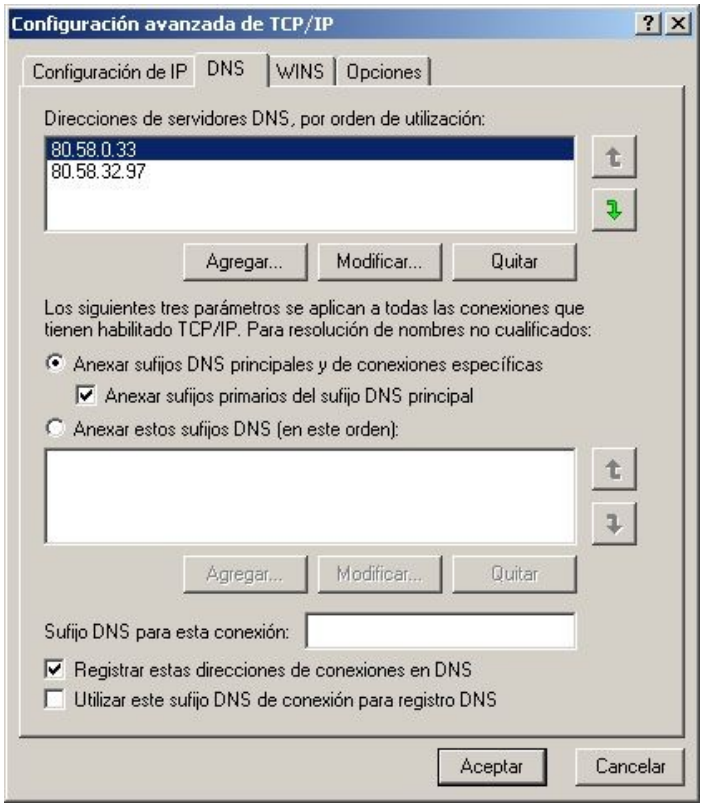


En este caso no estamos usando DHCP y, como ves, nos solicita las direcciones del servidor DNS. Te ofrece la posibilidad de configurar hasta dos servidores DNS. El primero de ellos (preferido) es obligatorio, dado que si no lo especificamos nuestro ordenador no podrá resolver ningún nombre.

El servidor DNS alternativo se utiliza si el preferido no está disponible. La mayor parte de los proveedores te van a proporcionar dos servidores DNS, por lo que es recomendable configurar los dos servidores.

8.2 Configuración avanzada

Si quieres realizar una configuración mas avanzada del cliente DNS, tendrías que pulsar en el botón opciones avanzadas. Y aparece la ventana representada abajo:



En la pestaña DNS puedes acceder a las opciones avanzadas. En la parte superior aparecen los servidores DNS que se van a utilizar. Mediante el botón agregar puedes añadir más servidores DNS y no solo dos como aparece en la configuración básica. Con las flechas puedes modificar el orden en el que se acceden.

En la parte del medio se configuran los sufijos DNS. Éstos se tienen que usar si se usa un nombre que no está cualificado completamente. Por ejemplo, si tecleamos "ping PC1" en la resolución DNS se añadirán los sufijos que aparezcan aquí, por ejemplo, "miempresa.com".

Las opciones de esta ventana están configuradas por defecto. Las diferentes opciones sirven para:

Anexar sufijos DNS principales y específicos: indica que se van a añadir los sufijos principales, el nombre de dominio que se ha configurado cuando se configuró el PC y uno específico que te explicaré más adelante.

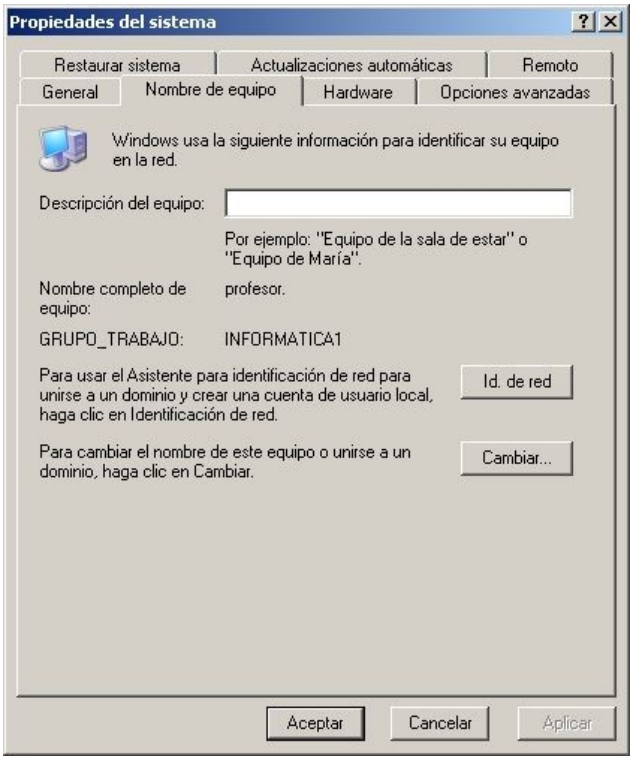
Anexar estos sufijos DNS: si seleccionas esta opción, tienes que especificar un conjunto de sufijos DNS que se añaden en este orden.

Registrar en DNS las direcciones de la conexión: en la última parte se especifica si quieres configurar tu PC para que actualice su dirección IP en el servidor DNS. Esta opción no es muy habitual con lo cual la debemos desmarcar.

8.3 Configurar el nombre DNS en un cliente

Cuando instalaste Windows le asignaste un nombre a nuestro equipo, pero si quieres tener configurado el cliente DNS será necesario configurar el dominio DNS al que pertenece. Aunque el ordenador accederá correctamente a Internet sin necesidad de configurar el sufijo DNS principal, es una buena idea configurarlo si gestionas la red de una empresa bajo un mismo dominio DNS. Este sufijo se añade automáticamente a un nombre no cualificado.

Para hacer esto hay que entrar en el panel de control, seleccionar el icono de Sistema y pulsar en la pestaña de nombre de equipo. Aparece la ventana que se muestra a la derecha:

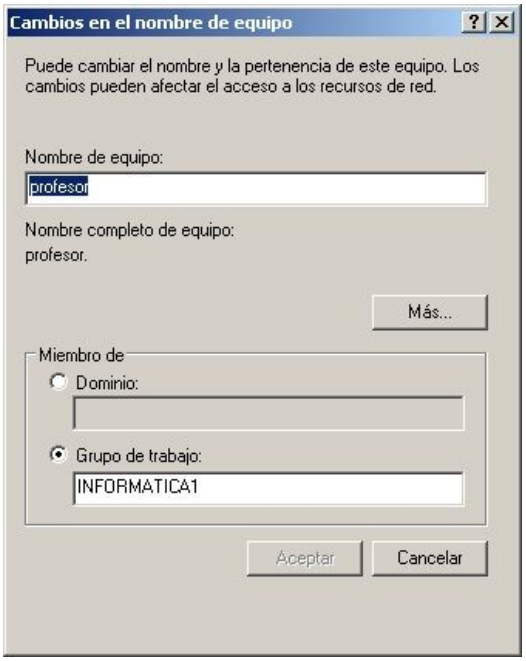


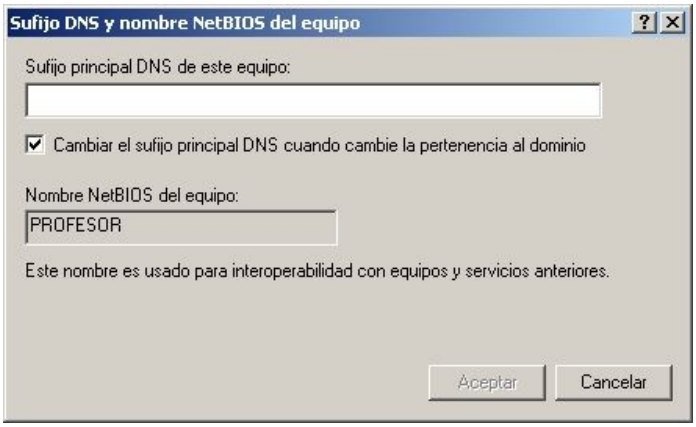
En esta ventana hay que pulsar el botón "*Cambiar*".

Y en la ventana que nos aparece después "*Cambios en el nombre de equipo*" podemos cambiar el nombre de nuestro ordenador que, en este caso, se llama profesor por otro más genérico, por ejemplo, "*profesorado"*.

El nombre del PC corresponde con el nombre de un nodo. Además, puede observarse que este PC no tiene configurado ningún nombre de dominio dado que el nombre del equipo es profesor sin más.

Para configurar el nombre de dominio al que pertenece este PC hay que pulsar "*Más*". Aparece la ventana "Sufijo DNS y nombre NetBios del equipo"; es aquí donde puedes cambiar el nombre del sufijo DNS principal del dominio al que pertenece este ordenador.





9 Servicio DNS en Linux. Instalación, parada/arranque; ficheros y parámetros de configuración básica.

El cliente DNS debe estar conectado en la misma red que el servidor, y configurar sus parámetros de red para que su resolver se conecte con el servicio DNS.

En el caso de Windows, esta configuración se realiza en el Panel de Control, Conexiones de Red.

En Linux tenemos los archivos `/etc/nsswitch.conf` y `/etc/resolv.conf`.

```
$ cat /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         compat systemd
group:          compat systemd
shadow:         compat
gshadow:        files

hosts:          files mdns4_minimal [NOTFOUND=return] dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Si quieres editar a mano los nombres e IPs de algunos hosts, se puede usar el fichero `/etc/hosts`.

El nombre del ordenador en Linux se especifica en el fichero `/etc/hostname`.

En Windows también existe un fichero `hosts` en `\Windows\System32\drivers\etc` y tiene el mismo formato que en Linux.

En la versión 18.04 de Linux Ubuntu aparece un nuevo método para configurar las redes, mediante `/etc/netplan`, que hay que tener en cuenta para configurar los servicios.

En cuanto al servidor DNS, en Linux es necesario instalar el paquete Bind, que lanza el demonio "`named`", cuyos archivos de configuración se encuentran en /etc/bind:

```
servidordns:/etc/bind$ ls -al
total 68
drwxr-sr-x   2 root bind  4096 oct 20 00:29 .
drwxr-xr-x 122 root root 12288 oct 20 00:29 ..
-rw-r--r--   1 root root  2761 ago 10 08:26 bind.keys
-rw-r--r--   1 root root   237 mar 23  2018 db.0
-rw-r--r--   1 root root   271 mar 23  2018 db.127
-rw-r--r--   1 root root   237 mar 23  2018 db.255
-rw-r--r--   1 root root   353 mar 23  2018 db.empty
-rw-r--r--   1 root root   270 mar 23  2018 db.local
-rw-r--r--   1 root root  3171 mar 23  2018 db.root
-rw-r--r--   1 root bind   463 mar 23  2018 named.conf
-rw-r--r--   1 root bind   490 mar 23  2018 named.conf.default-zones
-rw-r--r--   1 root bind   165 mar 23  2018 named.conf.local
-rw-r--r--   1 root bind   890 mar 23  2018 named.conf.options
-rw-r-----   1 bind bind    77 oct 20 00:29 rndc.key
-rw-r--r--   1 root root  1317 mar 23  2018 zones.rfc1918
```

Los ficheros de configuración que debemos modificar son `named.conf.local` (registros de recursos de zonas) y `named.conf.options` (opciones locales).

El servicio se gestiona mediante el comando `systemctl`, como el resto de servicios en sistemas Linux basados en SystemD:

```
jose@servidordns:/etc/bind$ sudo systemctl restart bind9
jose@servidordns:/etc/bind$ sudo systemctl status bind9
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor
preset: en
   Active: active (running) since Sat 2018-10-20 01:29:03 CEST; 4s ago
     Docs: man:named(8)
  Process: 2662 ExecStop=/usr/sbin/rndc stop (code=exited,
status=0/SUCCESS)
 Main PID: 2665 (named)
    Tasks: 4 (limit: 2321)
   CGroup: /system.slice/bind9.service
           └─2665 /usr/sbin/named -f -u bind
```

Una vez que los ficheros de configuración están correctos y se reinicia el servicio, ya disponemos de un servidor DNS para resolver las búsquedas de nuestros clientes.

En el documento de Prácticas disponemos de un completo **ejemplo de configuración de cliente y servidor DNS** con Linux Ubuntu 18.04.

10 DNS dinámico.

El DNS dinámico (DDNS) es un servicio que permite la actualización en tiempo real de la información sobre nombres de dominio situada en un servidor de nombres.

El uso más común que se le da es permitir la asignación de un nombre de dominio de Internet a un **dispositivo con dirección IP dinámica**, lo que permite conectarse con la máquina en cuestión sin necesidad de conocer su IP en ese momento.

El DNS dinámico hace posible utilizar un software de servidor en un dispositivo con dirección IP dinámica (como la suelen facilitar muchos ISP) para, por ejemplo, alojar un sitio web en la PC de nuestra casa, sin necesidad de contratar un hosting de terceros.

10.1 DNS dinámico para administradores de zona.

El sistema DNS incorpora un mecanismo denominado <<update>> que permite que un cliente DNS registre de forma dinámica su nombre y dirección IP ante su servidor DNS y que provoque que se actualice la zona de forma automática

- Configurar el cliente DNS: Configurar el ordenador cuya IP queremos que se registre de forma automática.
- Configurar el servidor DNS: Por defecto los servidores DNS no aceptan el mecanismo <<update>> a no ser que lo configuremos de otra forma.

10.2 DNS dinámico para usuarios.

Para que el usuario gestiona desde su ordenador la IP dinámica con una aplicación existen dos formas de hacer esto:

- Usando un dominio de tercer nivel: algunas empresas proveen este servicio sobre un dominio de segundo nivel de su propiedad de esta forma si la empresa provee el servicio nosotros podemos configurar un servidor web con IP dinámica.
- Usando nuestro propio dominio: si tenemos comprado un dominio pero la gestión de los servidores DNS de nuestro dominio la realiza.

Existen empresas que proporcionan servicios de DDNS. Las mas conocidas son:

- DynDNS. http://www.dyn.com.
- No-IP. http://www.noip.com.