

Servicios en red

Joaquin Andreu



Unidad 1. Servicios DHCP	ISBN 978-84-9003-083-7
Unidad 2. Servicios DNS	ISBN 978-84-9003-084-4
Unidad 3. Servicios de acceso remoto	ISBN 978-84-9003-085-1
Unidad 4. Servicios FTP	ISBN 978-84-9003-086-8
Unidad 5. Gestión de servicios de correo electrónico	ISBN 978-84-9003-087-5
Unidad 6. Gestión de servidores web	ISBN 978-84-9003-088-2
Unidad 7. Interconexión de red	ISBN 978-84-9003-089-9
Unidad 8. Redes inalámbricas	ISBN 978-84-9003-090-5
Unidad 9. Voz IP	ISBN 978-84-9003-091-2
Servicios en red (obra completa)	ISBN 978-84-9771-760-1

2

Servicios DNS

vamos a conocer...

1. Sistemas de nombres planos y jerárquicos
2. Espacio de nombres de dominio
3. Dominios genéricos
4. Delegación
5. Funcionamiento DNS (*Domain Name Service*)
6. Servidores de nombres
7. Zonas primarias y secundarias
8. Base de datos DNS
9. DNS dinámico
10. Clientes DNS (*resolvers*) en sistemas operativos libres y propietarios
11. Servidores DNS en sistemas operativos libres y propietarios
12. Herramientas para consultar un servidor DNS

PRÁCTICA PROFESIONAL

Instalación y configuración de un servidor DNS (BIND) en Linux y dos clientes en Windows

MUNDO LABORAL

Los nombres de dominio superan los 180 millones

y al finalizar esta unidad...

- Identificarás escenarios donde se necesite un servicio de resolución de nombres.
- Clasificarás los principales mecanismos de resolución de nombres.
- Conocerás la estructura, nomenclatura y funcionalidad de los sistemas de nombres jerárquicos.
- Instalarás un servicio jerárquico de resolución de nombres.
- Prepararás el servicio para almacenar las respuestas procedentes de servidores de redes públicas y para, posteriormente, poder servirlas a los equipos de la red local.
- Modificarás la configuración añadiendo registros de nombres correspondientes a una zona nueva, con opciones relativas a servidores de correo y alias.
- Transferirás zonas entre dos o más servidores.
- Comprobarás el correcto funcionamiento del servidor.



CASO PRÁCTICO INICIAL

situación de partida

Sabella es administradora de red local en la editorial Editex. Ella tiene resuelta la configuración de direcciones IP de la LAN corporativa. El problema que se le plantea ahora es que debe integrar la LAN e internet, para conseguir servicios de intranet y extranet adicionales.

Recientemente la empresa ha alquilado un dominio en internet, llamado «editex.es», a un ISP (*Internet Service Provider*, Proveedor de Servicios de Internet) que le permite la delegación de dominios.

Otra prioridad que se le acaba de plantear es conseguir 500 cuentas de correo electrónico corporativas, actualmente solo tiene 10 reales (una de ellas «sumidero», recoge los correos de to-

das las direcciones que no existen), y la posibilidad de crear alias para esas mismas direcciones, pero lo interesante es tener un número mucho más elevado de cuentas de correo electrónico reales.

Google ofrece la posibilidad, de forma gratuita, de usar Gmail de manera transparente con los dominios de la empresa, pero le pide que modifique los valores de su servidor DNS. Ya que va a configurarlo, va a nombrar varios equipos de la red para poder tener servicio de correo en la LAN y acelerar las conexiones a internet.

Sabella no tiene claro qué servidor DNS le interesa, y solo se le ocurren los servidores LAN para Linux.

estudio del caso

Analiza cada punto de la Unidad de Trabajo, con el objetivo de contestar las preguntas de este caso práctico.

1. ¿Qué le interesa más, servidores DNS exclusivamente locales o mixtos que permitan el servicio tanto local como de servicios de internet?
2. ¿Debe utilizar los servidores DNS de su proveedor de servicios de internet o le conviene utilizar los suyos propios, que se administran de forma local y que pueden ser consultados desde la red local e internet de forma indistinta?
3. ¿Merece la pena configurar el servidor DNS local de forma completa (servidores locales, correo electrónico, filtro de paquetes, etc.) o solo para el correo electrónico y así manejar el correo de Gmail?
4. Las direcciones DNS privadas no llegan al 8% de las direcciones IP (no contamos con los blogs ya que no son serios para una empresa), ¿le interesa a Sabella la configuración DNS en LAN o utilizar la de su proveedor?
5. Si tenemos servidores fijos (de correo, transferencia de archivos, etc.), ¿le interesa más a Sabella incluirlos en el servicio DNS o que estos funcionen solo con direccionamiento TCP/IP?

1. Sistemas de nombres planos y jerárquicos

saber más

Puedes conocer más detalles en las normas: RFC 882, 883 y 1983, para nombres planos, y RFC 1034, 1035 y 1886, para nombres jerárquicos.

saber más

Rutas del archivo de configuración para la LAN:

Linux, Mac OS

/etc/hosts

Windows 95, 98 o Millennium

C:\windows\hosts

Windows NT, 2000

C:\windows\system32\drivers\etc\hosts

Windows XP, 2003, Vista o 7

C:\windows\system32\drivers\etc\hosts

Cuando hablamos de sistemas de nombres nos referimos a los registros que relacionan nombres, pseudónimos o alias con unas direcciones IP.

Es mucho más fácil recordar un nombre que una sucesión de números. Por ejemplo, si alguien nos pide que visitemos la página 216.64.210.28 lo más seguro es que a los pocos segundos ya ni la recordemos; sin embargo, si lo que nos solicitan es que entremos en «cocacola.com» lo recordaremos mucho mejor.

Hace años, en 1983, las páginas web no existían y los servidores eran tan pocos que TODOS los host tenían la lista de nombres de dominio completa y la actualizaban diariamente. Se trataba de un **sistema de nombres planos**.

En el archivo hosts.txt o en hosts de Linux teníamos la lista de nombres. Hoy todavía podemos usarlo a nivel local (LAN).

Un ejemplo de archivo hosts es:

EJEMPLO

127.0.0.1	localhost
192.168.0.2	mi-servidor.lan
192.168.0.3	otro-pc.lan

En Linux puede existir una tercera columna con los alias:

EJEMPLO

192.168.0.2	mi-servidor.lan	servidor
-------------	-----------------	----------

Ahora se hace imposible manejar los más de 50.000 nombres nuevos diarios y, por ello, se utiliza un sistema de gestión de forma distribuida (en millones de servidores DNS) y jerárquica.

El *Domain Name System* o DNS es el servicio encargado de esta gestión, traduce un nombre en una dirección IP consultando la base de datos distribuida, conformada por todos los servidores DNS. Este sistema se denomina de **nombres jerárquicos**.

Es curioso que la estadística de cantidad de dominios registrados en 2006 no llegaba al 8% de los sites (el resto trabajaba con IP), y al 55% en 2008 (gracias a los blogs). Esto se debe a que alquilar una DNS cuesta unos 35 dólares/año (existen empresas mayoristas que los rebajan un 30% e incluso hasta un 90%). Los organismos que alquilan los nombres de dominio son:

- A nivel internacional los alquila *Internet Corporation for Assigned Names and Numbers* (ICANN).
- En el caso de los .es los reparte nic.es, que forma parte de red.es y este, a su vez, del Gobierno de España.

Debemos recordar que un nombre de dominio solo apuntará a una dirección IP en un momento concreto, aunque este pueda variar en el futuro.

Varios nombres pueden marcar a la misma IP.

saber más

Desde 1969 solo existía el dominio militar .arpa.

El primer dominio .com se registró en 1985.

caso práctico inicial

Es importante recordar que un nombre de dominio se traduce por una única dirección IP.

2. Espacio de nombres de dominio

El nombre del nodo es el trayecto completo de cada nodo de los niveles superiores, separado por puntos. Los nombres de dominio son sucesiones de 2 a 5 grupos, de 1 a 63 caracteres, separados por un punto (.). Tienen un nombre por cada nodo o host hasta el nodo raíz (nombre con 0 caracteres).

Sintaxis: nodo.nodo4nivel.nodo3nivel.nodo2nivel.TLD

Ejemplos:

- ua.es
- cochesdesegundamano.com
- dccia.ua.es
- 3.14159.org
- alerta-antivirus.red.es

El **espacio de nombres de dominio** es un árbol de nombres de dominio controlado desde un servidor DNS. Está compuesto por todos los host de nivel inferior.

El término **FQDN** (*Fully Qualified Domain Name*), o nombre de dominio completamente cualificado, define un nombre de dominio completo, es decir, incluye el nombre de una máquina o host y no de servicios. En total, el FQDN no debe exceder los 255 caracteres, que únicamente deben ser las letras (a-z, excepto las no anglosajonas como ñ, ç, y las que llevan tildes y diéresis á, à, ä, â, etc.), los dígitos (0-9) y los guiones (-).

Un servidor DNS tiene registros de los nombres de dominio y de los de servicios que tienen bajo su autoridad delegada (pueden administrar y/o configurar directamente).

Ejemplos:

- nombres de dominio:
 - dccia.ua.es
 - cpd.ua.es
 - ua.es
- nombres de servicios:
 - ftp.ua.es
 - www.ua.es
 - irc.ua.es

caso práctico inicial

Alquilaremos un nombre de dominio que no supere los 63 caracteres.

recuerda

Diferenciamos DNS, nombre de dominio, FQDN y URL:

DNS es un servidor de nombres de dominio, aunque coloquialmente se confunde con nombre de dominio.

Nombre de dominio es un alias de una dirección IP, como editex.es.

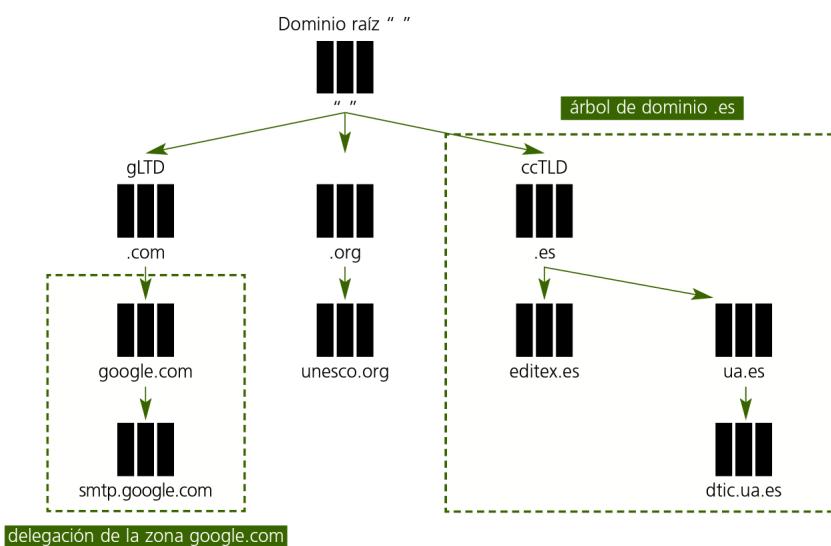
FQDN es un nombre de dominio que identifica el trayecto completo hasta un equipo, como: dccia.ua.es.

Una **URL** es el trayecto completo a un archivo o recurso de internet: <http://www.editex.es/Novedades/Novedades.aspx>.

saber más

Desde 2004 es posible registrar dominios con otro tipo de letras, aunque esta opción no está teniendo mucho éxito. Un ejemplo puede ser:

rae.es o RealAcademiadelal LenguaEspañola.es



3. Dominios genéricos

recuerda

Alquilar un nombre de dominio es fácil. Es más económico si lo alquilas junto con los servicios de host (espacio para el hospedaje de páginas web y correo electrónico).

saber más

El dominio .tk lo ha comprado una empresa y lo presta gratuitamente. Pero mira bien el contrato, ya que pueden quitártelo cuando quieran y alquilárselo a otras empresas. No es recomendable profesionalmente, ya que no resulta muy serio.

caso práctico inicial

Crear un TLD por 50.000 dólares (más de 35.000 euros) es un coste muy poco justificable para una empresa de cualquier tamaño.

caso práctico inicial

Es recomendable usar .com, pero a veces está justificado el uso de .es, .eu o .cat, dependiendo de las necesidades de la empresa; por ejemplo .org en el caso de las ONG.

saber más

Para ampliar información consulta la norma de facto RFC 920.

Al principio, y hasta 1985, nadie podía obtener un nombre de dominio, solo existía .arpa, que pertenecía a los militares de Estados Unidos. Entre 1985 y 2006 se crearon unos 280.

Tipos de dominios genéricos:

- gTLD: son los dominios genéricos de primer nivel, son los llamados **globales** o internacionales.
 - Alquilables por todo el mundo: .com (compañías), .net (telecomunicaciones), .org (organizaciones), .info (información). Se pueden alquilar por 35 dólares.
 - Alquilables cumpliendo unas restricciones: .biz (para empresas), .name (para nombres propios antonio.lopez.name), .pro (destinados a profesionales de diferentes sectores), .int (incluye organizaciones con tratados internacionales y organizaciones no gubernamentales con el estatus de «observadores» de las Naciones Unidas), .edu (universidades e institutos, educación), .mil (para el departamento de defensa de los Estados Unidos, fue uno de los primeros en crearse), .gov (organismos gubernamentales de Estados Unidos), etc.
 - sTLD: están patrocinados, promovidos por una fundación independiente o se obtienen pagando unos 50.000 dólares (más de 35.000 euros). Tenemos .aero (aeropuertos), .coop (sociedades cooperativas), .museum (museos), y los .travel (agencias de viajes).
 - mTLD: son los patrocinados para móviles, como .mobi.
 - lTLD: patrocinados para una lengua, como .cat para el catalán.
 - ccTLD: son dominios geográficos o *country codes*, están regulados por la norma ISO 3166-1 alpha-2, en la lengua materna están escritos en ASCII. Algunos se atreven a traducir *country* por país, es políticamente arriesgado, aunque coincidan en su mayoría (existen .eu de Unión Europea, .ic de Canarias, .ea de Ceuta y Melilla, .ps de Palestina, .va del Vaticano, etc.). Todos constan de dos letras, excepto en el caso de una provincia de China. Más ejemplos son: .de Alemania, .cn China, .uk Reino Unido, .nl Holanda, .ar Argentina, .it Italia, .us Estados Unidos, .br Brasil, .ch Suiza, .es España, .fr Francia, .mx México, etc.
 - SLD: algunas autoridades crean un segundo nivel genérico, como España, Reino Unido o Colombia: .nom.es, .org.uk, .com.co, etc.
 - IDN: son conversiones de lenguas no latinas a ASCII: كملاً، عَصْرَةً، فهُنْ، 文字もじも， etc.
 - Dominios de tercer nivel: son los subdominios, los que alquila una empresa, como el caso de: cocacola.com.uk.

No debemos confundir los ccTLD con dominios lingüísticos, ya que, por ejemplo, existen muchas páginas en español en Alemania (como es el caso de lapagina.de) y en Estados Unidos existen páginas en varias lenguas, sobre todo en inglés y español. Podemos encontrar páginas en español en .com, .net, .org, .es, .eu, .de, .name, .info, .edu, .gov, .ar, .fm, .tv, .co, etc. y en catalán en .com, .cc, .es, .cat, etc.

Existen ccTLD que se han vendido, como **.fm** (Estados Federados de Micronesia) utilizado en radio, o **.tv** (Tuvalu) para televisiones.

Hay países como Argelia, en los que no nos encontramos este tipo de ccTLD porque no tienen acceso a internet público.

4. Delegación

Existe la posibilidad de delegar a un nivel inferior la administración y la configuración. ICANN maneja la delegación de los gTLD (.com, .net, .org, etc.) y de los ccTLD (.es, .de, etc.). En España Nic.es delega los dominios de segundo y tercer nivel: turismomadrid.es o nationalgeographic.com.es. Por ejemplo, dentro de la Universidad de Alicante pueden delegar a nivel local (CAN) eps.ua.es, dccia.ua.es, etc. Y así cada nivel a sus niveles inferiores.

Si alquilamos el dominio «editex.es» y conseguimos un registrador por ICANN que nos delegue, podríamos configurar «ciclos.editex.es», «bachillerato.editex.es», «eso.editex.es», «www.editex.es», «smtp.editex.es» o «ftp.editex.es».

La delegación es una administración descendente. La autoridad superior puede delegar la administración, coordinando los resultados.

caso práctico inicial

Si la empresa es una radio o una televisión es recomendable estudiar la posibilidad de alquilar un **.fm** o un **.tv**, pero son más caros y los servicios son difíciles de transferir y de configurar.

caso práctico inicial

Es importante que nuestro registrador permita la delegación.

recuerda

Los tipos de redes según el tamaño son:

LAN: Red de Área Local, en una sala o edificio (máximo 500 metros).

CAN: Red de Área Campus, en una serie de edificios.

MAN: Red de Área Metropolitana, a nivel municipal (máximo unas pocas decenas de kilómetros).

WAN: Red de Área Mundial.



ACTIVIDADES

1. Modifica el archivo hosts de Linux para poner un nombre a tu equipo y al de dos compañeros del aula.
2. Modifica el archivo hosts de Windows para poner un nombre a tu equipo y al de dos compañeros.
3. Consulta en nominalia.com si google.es está registrado, así como cuándo, por quién, etc., se registró.
4. Busca en internet ofertas de dominios y host; compara máximo de alojamiento, máximo de tráfico mensual, cantidad de cuentas de correo electrónico, etc.
5. Crea un dominio gratuito .tk. Para ello necesitas un host inicial <http://my.dot.tk> o <http://dominiosfree.com/es>.

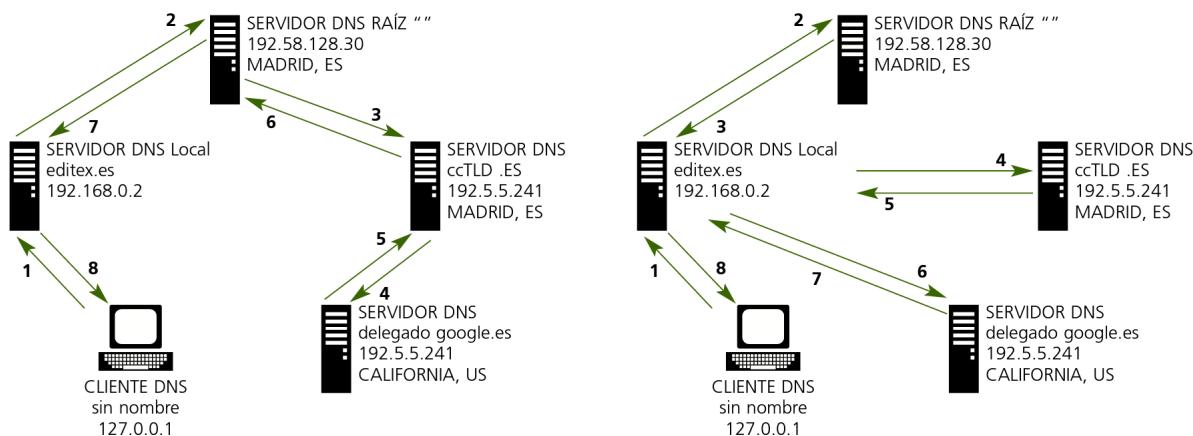
5. Funcionamiento DNS (*Domain Name Service*)

5.1. Consultas DNS

El servicio DNS se basa en una consulta del cliente a un servidor DNS. El sistema operativo suele tener configurados por el usuario, al menos, dos servidores DNS (sus direcciones IP) o, si se tiene activada la opción de configuración DHCP, la mayoría de los ISP actuales lo configuran automáticamente. La consulta se envía al servidor DNS primario, si este no contesta, o tarda en exceso, se usa el secundario. La comunicación se realiza a través del puerto 53.

5.2. Consultas recursivas e iterativas

Cuando un cliente hace una consulta a un servidor, este comprueba sus datos locales (nombres planos, jerárquicos, incluso cache) y ofrece la mejor respuesta. Si no la tiene, consulta al servidor raíz que menos tarde en ofrecer la respuesta, este, a su vez, consultará al intermedio, y así sucesivamente hasta llegar al autorizado. Una vez que el autorizado responde al nivel anterior, con acierto o con error, se van devolviendo los mensajes hasta llegar de nuevo al servidor local, y de este al cliente. A este proceso se le denomina **consulta recursiva**.



En cambio, en la **consulta iterativa** el servidor DNS no tiene la información pedida, lanza una consulta a un nivel superior hasta obtener una respuesta. Este le remite a un nivel intermedio, el servidor local le pregunta directamente al intermedio, este le contesta, y así hasta obtener la respuesta directamente del servidor autorizado.

5.3. Resolución inversa

La resolución inversa es justo al revés, se consulta una IP para conocer su nombre de dominio. Es usada por los protocolos RARP (*Reverse Address Resolution Protocol*).

6. Servidores de nombres

6.1. Características

Los servidores de nombres son sistemas informáticos que tienen instalado un software que permite administrar y consultar las bases de datos de nombres de dominio. Existen para Linux, Windows, Mac OS, etc. El programa que se utiliza con más frecuencia es BIND.

6.2. Tipos (primario, secundario, cache, reenviador)

Existen muchísimos tipos de servidores DNS, pero o son una combinación o se pueden resumir en estos tipos:

- **Primario (master):** es un servidor autosuficiente, donde podremos actualizar, modificar o añadir nombres de dominio. Debemos tener al menos uno si nos han delegado una zona o dominio, pero no tiene sentido si no somos autoridad delegada de ninguna zona. Si tenemos varios se hace difícil la administración, pero contestará el que haya tardado menos tiempo en las pruebas del cliente.
- **Secundario (slave):** depende de un servidor primario, el secundario le pide una copia de solo lectura cada cierto tiempo. No puede existir si no tiene asociado un servidor primario que le permita pedir y recibir copias de la base de datos. Suele usarse de servidor redundante y es más que aconsejable. Por defecto, entre secundarios y primarios no se debe exceder de tres servidores.
- **Cache (hint):** se usa cuando no tenemos la delegación de ninguna zona o dominio. Hace una copia de los nombres de dominio más utilizados durante un cierto tiempo, para acelerar las consultas y minimizar el tráfico de la red.
- **Reenviador (forward):** sirve para descargar el tráfico local y la carga de trabajo de los servidores DNS externos. Solo se recomienda si usamos un punto de acceso PPP. Normalmente se usan los servidores de un ISP propio o de uno conocido y que sea muy rápido.

caso práctico inicial

Seleccionaremos BIND (*Berkeley Internet Name Domain*) como servidor DNS, por ser el más utilizado.

caso práctico inicial

Debemos seleccionar el número de servidores primarios, secundarios y/o cache, y que no excedan de tres.

vocabulario

Los *resolvers* o resolvidores son una biblioteca de rutinas que tiene el servidor DNS para consultar las bases de datos distribuidas de nombres de dominio.

7. Zonas primarias y secundarias

Las zonas primarias son las que tenemos cuando nos han delegado una zona o dominio, pues son las únicas que se pueden editar y modificar. En cambio, las zonas secundarias dependen de una zona primaria y solo son de lectura.

7.1. Transferencias de zona

La transferencia de zona se hace de un servidor primario a otro no primario. El primario es el único que puede modificar los registros de la base de datos de nombres de dominio; los secundarios, sobre todo, lo que hacen es pedir una copia de solo lectura de los registros de la base de datos al primario. El primario consulta si puede hacer esa «transferencia» y, en caso afirmativo, le envía la última versión de los registros de la base de datos; en caso contrario no hace nada. El tener permiso para pedir transferencia nunca implica que esa máquina vaya a actuar de secundario o que vaya a pedir alguna vez los registros.

8. Base de datos DNS

8.1. Estructura

EJEMPLO

BIND en Linux requiere, como mínimo, un 486x, a 100 MHz, con 16 MB de RAM, con Linux kernel 2.2.20.

En el caso de Windows BIND necesita, como mínimo, un Pentium Pro, con Windows NT 4.

La base de datos DNS consiste en, al menos, dos archivos (aconsejamos tres o cuatro) que contengan la configuración de zonas y registros. En BIND, el archivo de configuración se llama **named.conf** y los registros están en otros archivos que suelen denominarse **db**. El nombre del dominio es: db.editex.es, y a veces otro llamado como la red: db.192.168.0.

8.2. Tipos de registros

En las bases de datos de nombres de dominio distribuidas lo más importante son los registros. Estos contienen realmente la configuración para traducir tanto los nombres de dominio a direcciones IP, como los pseudónimos, direccionamientos inversos, servicios distintos en un mismo servidor, etc.

- **A** (dirección): este registro se usa para traducir nombres de dominio a direcciones IPv4.

EJEMPLO

google.es	A	216.239.39.104
-----------	---	----------------

- **AAAA**: dependiendo de la versión se usa **AAAA** (menor que la versión 9.3.2 de BIND) o **A6** para la IPv6.
- **CNAME** (nombre canónico): se usa para crear nombres de hosts adicionales, alias. No es aconsejable utilizar CNAME cuando un mismo servidor lo es de distintos protocolos con la misma IP, pero sí cuando tenemos que poner un alias a un servidor externo. Por ejemplo, no lo usaremos para crear «www.editex.es» ni «ftp.editex.es», pero sí cuando queramos redirigir nuestro servidor de correo «smtp.editex.es» a «smtp1.google.com», para usar nuestros correos «editex.es» con Gmail.
- **NS** (servidor de nombres): define la asociación que existe entre un nombre de dominio y los servidores de nombres que almacenan la información de dicho dominio.

EJEMPLO

@	IN	NS	google.es
---	----	----	-----------

- **MX** (registro de intercambio de correo): asocia un nombre de dominio a un servidor de intercambio de correo (SMTP, SSMTMP, etc.).
- **PTR** (puntero o registro inverso): traduce direcciones IP a nombres de dominio.
- **SOA** (autoridad de la zona): proporciona información sobre la zona.
- **SRV** (servicios): permite indicar los servicios que ofrece el dominio (FTP, HTTP, etc.).

EJEMPLO

http.tcp.www.google.es.	SRV	0	1	80	ns1.google.es
-------------------------	-----	---	---	----	---------------

- **SPF** (política de envío): para combatir el spam, se especifica qué host está autorizado para enviar correo desde el dominio dado.

9. DNS dinámico

Cuando tenemos una IP dinámica es imposible crear un servidor de alojamiento de páginas web y muchos otros servicios que requieren una IP estática. La forma de resolverlo es utilizando el servicio de DNS dinámico o **DDNS**, que consiste en un servidor DNS que permite la actualización del registro en tiempo real.

Muchos ISP tienen esta opción, incluso algunas páginas lo ofrecen gratuitamente, como es el caso de: DynDNS.com, No-IP.com, ZoneEdit.com, etc.

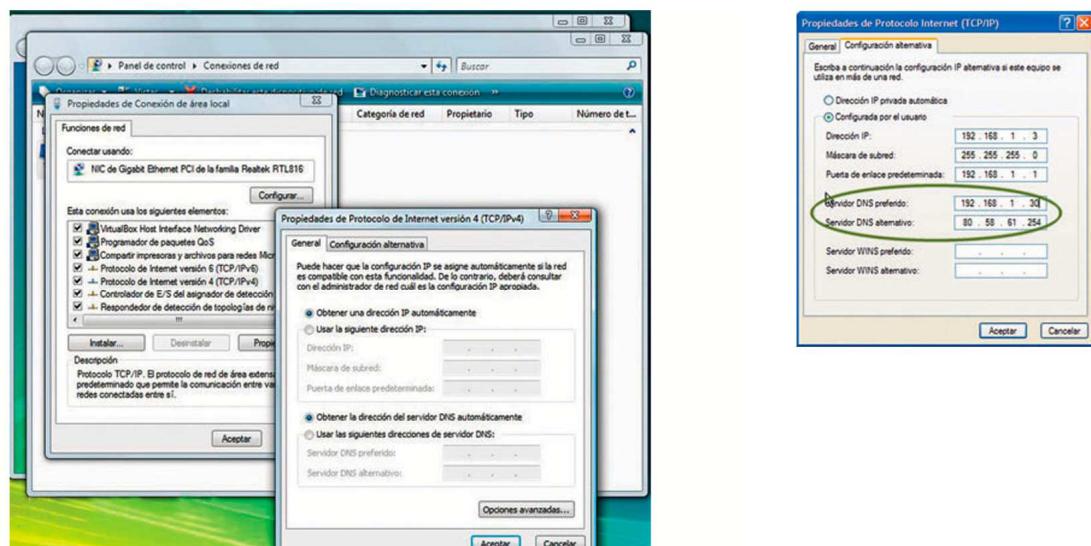
10. Clientes DNS (*resolvers*) en sistemas operativos libres y propietarios

10.1. Configuración

En Linux, edita el archivo `/etc/resolv.conf` y escribe una línea por cada servidor DNS, el orden importa (por defecto, secundario1, secundario2, etc.).

```
nameserver 80.58.0.33
nameserver 80.58.32.97
```

También puedes hacerlo de forma gráfica desde Linux o Windows, como explicamos en la unidad de DHCP, pues la dirección IP y las direcciones DNS están en las mismas pantallas de configuración, tal y como se muestra en las imágenes.



ACTIVIDADES

6. Comprueba las DNS que tienes (con `ipconfig /all`) y configúralo manualmente en Windows.
7. Realiza el ejercicio anterior en Linux.
8. Consulta en internet los servidores DNS de, al menos, tres ISP distintos.

11. Servidores DNS en sistemas operativos libres y propietarios

11.1. Instalación

recuerda

Para instalar en **Linux** usa:

```
#apt-get install bind9
```

Puedes bajar la versión desde:

<https://www.isc.org/downloads>

Para **Windows XP** usa:

<ftp://ftp.bind.com/pub/bind9>

Para **Mac OS X**:

<ftp://ftp.isc.org/isc/bind9>

Versiones estables y seguras:

- Para sistemas Mac OS X v10.4.11, o inferiores, BIND se actualiza a la versión 9.3.5-P2. Para sistemas Mac OS X v10.5.4, o superiores, BIND se actualiza a la versión 9.4.2-P2.
- Hasta Windows XP v9.3.2 para IPv6 y v8.4.7 solo para IPv4.
- Para Linux baja la última versión y consulta los foros.

Para instalar el servidor DNS BIND, debemos bajarnos el paquete bind9 en **Linux** (`#apt-get install bind9`).

Para **Mac OS** bájate el paquete BIND 9.4.2-REL. En línea de comandos ejecuta:

```
% curl -O ftp://ftp.isc.org/isc/bind9/9.4.2/bind-9.4.2.tar.gz
% tar zxvf bind-9.4.2.tar.gz
% cd bind-9.4.2
% ./configure --prefix=/usr/local/bind9
% make
% sudo make install
```

Por cuestiones de seguridad, bájate la versión estable, consúltalo en: <http://support.apple.com>

Para **Windows XP** bájate el archivo comprimido en formato zip (encontrarás la última versión en <ftp://ftp.bind.com/pub/bind9>).

Ejecuta: **BINDinstall.exe**. Inicialmente configura (ver la imagen que aparece en el lateral de la página):

- **TARGET DIRECTORY:** C:\WINDOWS\system32\dns o el que prefieras.
- **SERVICE ACCOUNT NAME:** named o cualquier otro.
- **SERVICE ACCOUNT PASSWORD:** introduce una contraseña.
- **CONFIRM SERVICE ACCOUNT PASSWORD:** repite la contraseña.
- **ENSURE THAT AUTOMATIC STARTUP:** actívalo si quieres que se arranque justo después de la instalación (es recomendable para comprobar que funciona) o déjalo desactivado si no lo vas a probar aún.

La configuración inicial requiere que, desde el símbolo de sistema (**INICIO > EJECUTAR CMD**), ejecutes:

```
cd C:
rndc-confgen -a
rndc-confgen > ...conf
```

11.2. Arranque y parada

Para arrancar el servidor en Linux como administrador ejecuta: `/etc/init.d/bind9 start`

Para pararlo: `/etc/init.d/bind9 stop`

En Windows, desde **INICIO > PANEL DE CONTROL > HERRAMIENTAS ADMINISTRATIVAS > SERVICIOS**, busca **ISC BIND** y con el botón derecho pulsa **INICIAR**.

Para pararlo debes realizar los mismos pasos pero seleccionando **DETENER**.



Para Mac OS debes editar el archivo hostconfig: `sudo pico /etc/host config` y cambiar la línea `DNSERVER==YES`

A partir de ahora se iniciará el servidor en cada reinicio del equipo.



11.3. Ficheros y parámetros de configuración básica

El fichero de configuración básica para los diferentes sistemas operativos es:

- **Windows:** `C:\WINDOWS\system32\dns\etc\named.conf` que no existe por defecto y debes crearlo.
- **Linux:** `/etc/bind9/named.conf`
- **Mac OS:** `/var/named/named.conf`

En todos los sistemas operativos los parámetros de configuración básica son los mismos, solo que en Windows las rutas deben estar entre **comillas anglosajonas ("")** y en Linux y Mac OS no.

Las opciones son optativas:

- **directory:** es la ruta del directorio donde se encuentran los archivos de configuración adicional.
- **allow-query:** contiene las direcciones IP de las interfaces o redes que se permitirá que consulten la base de datos.

EJEMPLO

```
allow-query { 192.168.0.32; 10.0.0.0/8; } ;
```

- **allow-transfer:** contiene las interfaces que pueden pedir una copia de la base de datos (los servidores secundarios).

EJEMPLO

```
allow-transfer { any; } ;
allow-transfer { none; } ;
```

- **recursion yes:** activa consultas recursivas; **recursion no:** solo permite iterativas.
- **forward first:** acelera la remisión de las consultas fuera de la LAN.
- **forwarders:** contiene las direcciones IP de los servidores DNS externos.
- **blackhole:** se especifican las direcciones IP de las interfaces a las que no se va a contestar en ningún caso.

En las opciones donde se especifiquen direcciones IP, podemos añadir varias direcciones o redes separadas por **punto y coma (;**). Existe también la posibilidad de añadir el comodín **asterisco (*)**.

EJEMPLO

```
Archivo named.conf
options
{
    directory
        "C:\WINDOWS\system32\dns\etc";
    allow-query{ any; };
    allow-transfer{ none; };
    recursion no;
    forward first;
    forwarders{ 10.0.0.1; };
    blackhole{ !*; };
};
```

recuerda

Para especificar direcciones IP:

- **any, 0.0.0.0** o comodín asterisco (*): todos los hosts;
- **none** o comodín negado (!*): ninguno;
- 192.168.0.1 esta IP;
- 192.168.0.0/24 la LAN 192.168.0.0...

EJEMPLO

```
Archivo named.conf básico
zone "localhost" in {
    type master;
    file "db.localhost";
} ;
zone "0.0.127.in-addr.arpa" in {
    type master;
    file "db.127.0.0";
} ;
zone "." in {
    type hint;
    file "root.hint";
} ;
```

saber más

Si programas en C o C++:

```
#include <sys/socket.h>
// IEEE Std 1003.1
int bind(int socket,
const struct sockaddr *
*address, socklen_t
address_len);
```

11.4. Archivos de zona

En el archivo **named.conf** también se declaran las zonas. Como por ejemplo:

```
zone "editex.es" {
    type master;
    file "db.editex.es";
} ;
zone "0.168.192.in-addr.arpa" {
    type master;
    file "db.192.168.0";
} ;
```

La sintaxis del archivo **named.conf** es parecida a la de los lenguajes de programación más usados, toda sentencia termina con punto y coma (;) y las opciones van entre corchetes {}.

La orden más importante es la palabra **zone**, que permite identificar las zonas entre comillas anglosajonas (" "), entre las que pondremos el **nombre de dominio** que tenemos delegado o un punto “.” si queremos configurar los servidores raíces. Podemos configurar solo el nombre de dominio, pero es aconsejable declarar la resolución inversa, que es la IP de la red al revés (sin la parte de host) acabada en **.in-addr.arpa** (ver ejemplo anterior).

Con **type** identificamos si el servidor es primario (**master**), secundario (**slave**), o cache (**hint**).

Con **file** le decimos la ruta y el nombre del archivo donde tenemos los registros de los nombres de dominio. El archivo puede ser único para ambas resoluciones, pero aconsejamos hacer dos. Podemos poner el nombre que queramos pero se aconseja nombrarlos precedidos por **db.** para recordar que son una base de datos; uno tendrá el nombre del dominio y el otro la IP de la LAN sin la parte de host.

11.5. Configurar servidores primarios, secundarios y caches

En los servidores secundarios y caches no debemos crear los archivos de configuración **db.** porque en los secundarios se copiarán del primario, y en el cache se irán incrementando según se hagan consultas.

caso práctico inicial

Debemos configurar al menos un servidor primario si queremos administrar el dominio que tenemos de la empresa.

```
zone "." in { type hint;
    file "root.hint"; } ;
```

En el caso de los servidores secundarios es necesario añadir al archivo **named.conf** la línea que identifica los primarios de los que se copiará la base de datos.

A continuación te ofrecemos un ejemplo:

```
masters { 192.168.0.3; } ;
zone "editex.es" {
    type slave;
    file "db.editex.es";
} ;
```

Comentemos un ejemplo de archivo de configuración primario:

```
//216.239.39.104/ etc/bind/named.conf.local
```

```
zone "239.216.in-addr.arpa" {
    type master;
    file "/etc/bind/db.216.239"; } ;

zone "google.es"{
    type master;
    file "/etc/bind/db.google.es"; } ;

allow_transfer { 216.239.*.10; } ;
allow_query {any}; ;
```

La única complicación adicional de este archivo es el uso de comodines para especificar los servidores secundarios.

```
//216.239.39.104/etc/bind/db.216.239
$TTL 604800
@ IN SOA google.es. hostmaster.google.es.
(20090517001 ; 10800 ; 7200 ; 1296000 ; 172800 ) ;
@ IN NS google.es.
1 IN PTR ns1.google.es.
2 IN NS ns2.google.es.
3 IN MX smtp1.google.es.
4 IN MX smtp2.google.es.
```

\$TTL es el tiempo de vida de este archivo en segundos.

@ IN SOA indica que a continuación aparece la información de este servidor. Como podrás advertir, el nombre de dominio termina en punto, que es la representación del nodo raíz, ya que, aunque este sea un espacio en blanco, nosotros lo representaremos. Opcionalmente le sigue la dirección del administrador, sustituyendo la arroba @ por un punto (.).

Dentro de los paréntesis aparecen los siguientes elementos:

- **Serial:** es el número de serie de este archivo, se incrementa cada vez que se modifica para que los servidores secundarios y cache lo sepan. Lo ideal es utilizar el formato YYYYMMDDNN (AñoMesDíaNúmero), por ejemplo, si hoy fuese 12 de junio de 2014 y fuese la segunda vez que lo modificáramos sería: 2014061202.
- **Refresh:** tiempo en el que, si el secundario tiene este archivo, debe renovarlo, actualizarlo. Se recomienda que sea menos de 1 día.
- **Retry:** el intervalo de tiempo en el que el secundario debe volver a reintentar comunicarse después de un intento fallido. Se aconseja que sea de 2 horas. (Ejemplos: 7.200 segundos, 120 minutos, 2 horas, etc.)
- **Expire:** tiempo en el que, si no se ha recibido una nueva copia de la base de datos, la copia antigua deberá dejar de usarse. Se utiliza como máximo 1 mes.
- **Cached:** tiempo máximo de cache de los servidores cache que consulten a este primario. Máximo 2 dfas.

caso práctico inicial

Debemos cambiar los registros MX si queremos redirigir nuestras cuentas a gmail.com.

recuerda

Tipo de registro (**RR**) para direccionamiento inverso:

- **NS:** servidor de nombres.
- **MX:** correo.
- **PTR:** puntero inverso.

recuerda

Los tiempos se especifican por defecto en segundos, pero se pueden usar letras (que proceden del inglés) para abreviar otras medidas:

- **m:** minutos.
- **h:** horas.
- **d:** días.
- **w:** semanas.

recuerda

No olvides poner el punto al final de los nombres de dominio si estás configurando para internet o mixto. Aunque no es necesario si lo haces solo para la LAN.

En el direccionamiento inverso debemos tener en cuenta que la arroba (@) siempre es para el servidor. Después enumeraremos cada dirección IP diferente con un número distinto, pero no hace falta que se diferencien en una unidad:

10	IN	NS	ns1.google.es.
23	IN	NS	ns2.google.es.

Podría ser más sencillo si utilizásemos la terminación (o la diferencia) de las direcciones IP, pero cuidado, porque puede que tengamos distintas subredes o que el servidor DNS no sea la primera IP:

32	IN	NS	ns1.google.es.
34	IN	NS	ns2.google.es.

caso práctico inicial

Debemos usar registros CNAME para usar **Gmail** con nuestro dominio delegado.

En cuanto al archivo de los registros de nombres de dominio propiamente dichos (para protocolos ARP), el nombre aconsejado sería db.google.es, en nuestro ejemplo, y trabajaría en la red 216.239.0.0/16, siendo el servidor el 216.239.39.104. Tendríamos dos servidores de nombres (216.239.32.10 y 216.239.34.10) que serían a la vez servidores de páginas web (HTTP) y páginas web seguras (HTTPS) y dos servidores de correo electrónico SMTP (216.239.167.25 y 216.239.39.104). Deberíamos consentir que el usuario escribiese `http://www.google.es` y `http://google.es` indistintamente. Y como medida preventiva cerraríamos todos las peticiones de protocolos TCP/IP (servicio * .tcp, enviado al puerto 0, «fuera» de la red).

//216.239.39.104/etc/bind/ db. google.es

\$TTL 604800		
@ IN SOA google.es. hostmaster.google.es.		
(20090517001 ; 10800 ; 7200 ; 1296000 ; 172800) ;		
// esta parte es igual a la del otro archivo		
localhost.google.es. A 127.0.0.1		
google.es. A 216.239.39.104		
dc-in-f104.google.es. A 216.239.39.104		
ns1.google.es. A 216.239.32.10		
ns2.google.es. A 216.239.34.10		
smtp1.google.es. A 216.239.57.25		
smtp2.google.es. A 216.239.167.25		
www.google.es. A 216.239.39.104		
http.tcp.google.es. SRV 0 1 80 ns1.google.es.		
http.tcp.google.es. SRV 0 1 80 ns2.google.es.		
http.tcp.www.google.es. SRV 0 1 80 ns1.google.es.		
http.tcp.www.google.es. SRV 0 1 80 ns2.google.es.		
https.tcp.google.es. SRV 0 1 443 ns1.google.es.		
https.tcp.google.es. SRV 0 1 443 ns2.google.es.		
https.tcp.www.google.es. SRV 0 1 443 ns1.google.es.		
https.tcp.www.google.es. SRV 0 1 443 ns2.google.es.		
mailto.tcp.smtp1.google.es. SRV 0 1 25 smtp1.google.es.		
mailto.tcp.smtp2.google.es. SRV 0 1 25 smtp2.google.es.		
*.tcp SRV 0 0 0 .		

recuerda

Puertos importantes:

- 21 FTP
- 22 SSH
- 25 SMTP
- 80 HTTP, SKYPE
- 110 POP3
- 119 NNTP – News Groups
- 194 Internet Relay Chat
- 389 NetMeeting
- 443 HTTPS, SKYPE
- 465 SMTP SSL
- 522 NetMeeting
- 992 Telnet SSL
- 993 IMAP4 SSL
- 995 POP3 SSL

Consulta más puertos en el RFC 2052.

Los registros A simplemente asocian el nombre de dominio a la dirección IP. Es importante que no olvidemos el punto al final del dominio.

La sintaxis completa es la siguiente: Nombredominio.subdominio.TLD.

	[TTL]	[Clase]	Tipo	RData
google.es.	604800	IN	A	216.239.39.104
smtp.google.es.		IN	CNAME	gmail.com
google.es.			A	216.239.39.104

Los registros CNAME asocian una dirección DNS a otra dirección DNS. Se usan dentro del mismo dominio para crear alias (smtp.google.es con mail.google.es o correo.google.es) y con distintos dominios para redirecciónamientos transparentes (smtp.google.es con gmail.com). Aún los CNAME no están muy aconsejados, se están volviendo a utilizar muy frecuentemente para casos de gestiones externas (CPanel, webmail... y otros servicios externos o subcontratados).

La sintaxis de los servicios es: servicio.protocolo.dominio.TLD.

	[TTL]	[Clase]	Tipo	Prioridad	Peso	Puerto	Destino
http.tcp.google.es.	7200	IN	SRV	0	1	80	ns1.google.es.
*.udp.google.es.			SRV	0	0	0	.

Existe la posibilidad de tener servidores redundantes para suplir a los primarios cuando fallen.

En este caso, en el apartado **PRIORIDAD**, pondremos un valor distinto a 0, poniendo el número más pequeño a los principales y el más grande al último secundario.

http.tcp.google.es.	SRV 1 0 80	ns1.google.es.
http.tcp.google.es.	SRV 2 0 80	ns2.google.es.

Si por el contrario queremos que ambos trabajen igual, usaremos el peso, poniéndolos todos a 1:

http.tcp.google.es.	SRV 0 1 80	ns1.google.es.
http.tcp.google.es.	SRV 0 1 80	ns2.google.es.

Pero si una máquina es superior a otra, y queremos repartir el trabajo, pondremos el porcentaje de trabajo de cada uno:

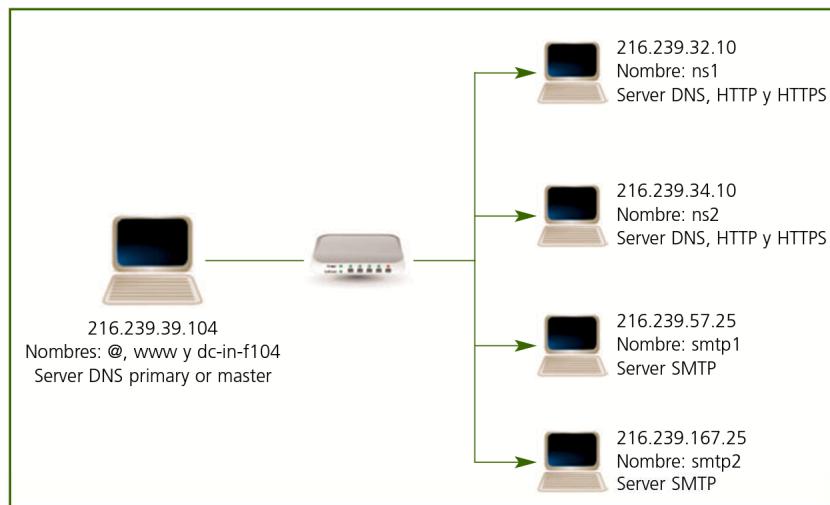
http.tcp.google.es.	SRV 0 75 80	ns1.google.es.
http.tcp.google.es.	SRV 0 25 80	ns2.google.es.

O reducido por su factor común:

http.tcp.google.es.	SRV 0 3 80	ns1.google.es.
http.tcp.google.es.	SRV 0 1 80	ns2.google.es.

caso práctico inicial

Repartir el trabajo entre distintos servidores es una técnica muy común y recomendable, pues en las empresas se estima que la renovación de hardware tiene una media de 8 años, por lo que los hosts son muy lentos.



→ Diagrama del ejemplo estudiado.

Por seguridad debemos redirigir «a ningún sitio» los servicios que no hayamos controlado:

```
*.tcp          SRV 0 0 0 .
*.udp          SRV 0 0 0 .
*.icmp         SRV 0 0 0 .
*.*           SRV 0 0 0 .
```

Otro ejemplo: hemos alquilado «cotsalicante.com», tenemos cuatro equipos, al primero lo llamaremos **server**, al segundo **gateway**, al tercero **pc02** y al cuarto **pc03**, **www** y **luna**. El **server** es el servidor DNS, el **www** admite consultas de páginas web:

```
$TTL 10800
@ IN SOA cotsalicante.com.
(20091005001; 10800; 900; 604800; 86400;)

luna          A       10.0.0.4
www          CNAME   luna
server        A       10.0.0.1
gateway       A       10.0.0.2
pc02          A       10.0.0.3
pc03          A       10.0.0.4
//inversa
@    IN  NS    server.cotsalicante.com.
1    IN  PTR   server.cotsalicante.com.
2    IN  PTR   gateway.cotsalicante.com.
3    IN  PTR   pc02.cotsalicante.com.
4    IN  PTR   pc03.cotsalicante.com.
4    IN  PTR   luna.cotsalicante.com.
//servicios
http.tcp.cotsalicante.com. SRV 0 0 80 www.cotsalicante.com.
*.tcp          SRV 0 0 0 .
```

En Linux existe la posibilidad de configurar el servidor DNS en modo gráfico con Webmin. Desde el navegador, entramos en **https://localhost:10000**; pinchamos en **RED > CONFIGURACIÓN DE RED > CLIENTE DNS**. No se aconseja utilizarlo, pues debemos crear las zonas y registros uno a uno, siendo más rápida e intuitiva la modificación del archivo `named.conf`.

Desde Windows 2003 Server (2008 y Servers posteriores) el servidor DNS está integrado en el **ACTIVE DIRECTORY**. Podemos configurarlo desde **INICIO > ADMINISTRACIÓN DE SERVIDOR > ADMINISTRAR ESTE SERVIDOR DNS** o desde **INICIO > HERRAMIENTAS ADMINISTRATIVAS > DNS**. En la consola que aparece podremos añadir zonas delegadas, desde **MENÚ > ACCIÓN > ZONA NUEVA > ZONA PRINCIPAL**.

recuerda

Casi el 99% de los servidores son de Linux, excepto los **HTTP**. BIND es el servidor DNS más utilizado, la presencia de Windows Server se ajusta solo a redes locales.

12. Herramientas para consultar un servidor DNS

Para comprobar si funciona el servidor, ejecutamos el comando **ping** desde una consola:

```
ping 127.0.0.1
ping localhost
ping miDominio.com
```

Si el problema es de sintaxis, podemos usar:

```
#named-checkconf
#named-checkzone aula.com /etc/bind/db.aula.com
```

Los registros del servidor se almacenan en el archivo `syslog`, que en Linux se encuentra en la carpeta `/var/log`. Si el servidor está en marcha no debemos editarlos, se aconseja usar `tail` (para consultar las últimas líneas): `tail -f /var/log/syslog`

También podemos usar las órdenes **dig**, **nslookup** y **host**:

- **dig** consulta los servidores DNS. Su sintaxis es:

```
dig [ @nombreDominioooIPServidor] [ opciones] FQDN [ tipo] [ opciones de acotación]
```

Consulta los 13 «súper» servidores DNS que controlan el nivel raíz (comprobable en `ftp.internic.net`):

```
dig . NS
o bien dig . NS +short | wc -l
```

saber más

Opciones dig:

-h: ayuda.

-x: consulta inversa.

-b IP: especificamos la interfaz si tenemos varias.

Tipo: A, NS, MX, CNAME, etc.

Acotación:

+[no]trace, +short, +nocmd,
+[no]comments, +[no]question,
+[no]answer, +[no]authority,
+[no]additional y +[no]stats.

ACTIVIDADES

9. Instala BIND en Linux.
10. Instala BIND en Windows.

Para saber los servidores que controlan un TLD consulta:

```
dig com. NS
dig es. NS
dig org. NS
```

O tu propio dominio, como por ejemplo el de «editex.es»:

```
dig editex.es. NS
```

Ejemplo completo:

```
dig -b 192.168.0.3 editex.es. +trace +nostats
```

- **nslookup** es como preguntar «¿quién es?», y se usa para saber si se está resolviendo bien la consulta de nombre:

```
nslookup google.com
```

- Para buscar un DNS y saber su información usamos la orden **host**:

```
host editex.es
```

Podemos usar la orden **ipconfig** en Windows para saber cómo está la cache:

```
ipconfig /displaydns
```

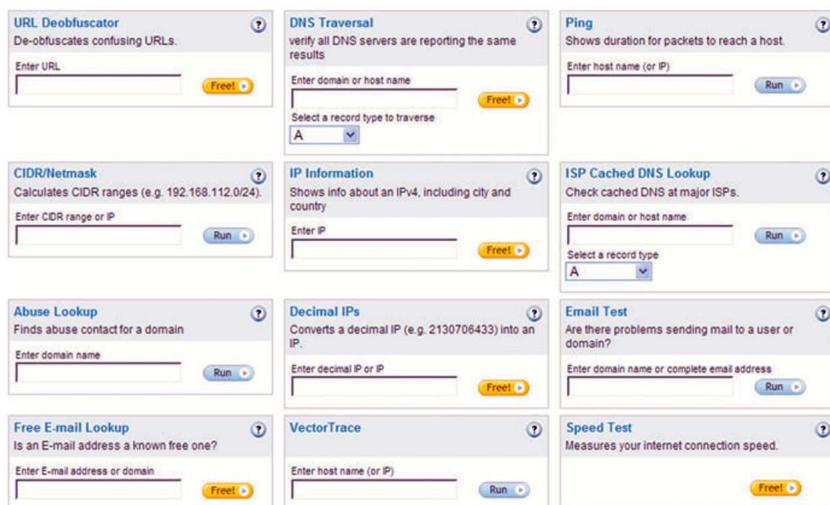
Estas herramientas son rápidas y eficientes para cuando tenemos prisa y conocimientos de Linux, pero para los amantes del sistema gráfico existen innumerables herramientas en internet para consultar las configuraciones de las direcciones DNS.

Bajo el nombre de «DNS Tools», tenemos multitud de servicios gratuitos (y más aún de pago) para consultar desde cualquier navegador:

- DNSTools.com: resolve, whois, chequeo de puertos, ping, etc.
- DNSStuff.com: lookup, traceroute, información de la IP, listado de registros de un servidor DNS, tiempos de respuesta del servidor DNS, etc.
- 4DNSTools.com: cache DNS de tu ISP, etc.
- network-tools.com: registros de la base de datos del servidor DNS.
- domaintools.com: histórico de entradas whois desde 1995.
- dnsgoodies.com: visitas a esa dirección DNS, servidores seguros, etc.
- 12dt.com, dnswatch.info, lookupserver.com, etc.

En el caso de DNSStuff.com, tenemos las siguientes opciones:

- **URL DE-OBFUSCATOR:** separa los elementos de una URI.
- **DNS TRAVERSAL:** crea informes del tipo de registros que selecciones.
- **IP INFORMATION:** lista información de una IPv4, incluyendo la localización del host (ciudad y país).
- **PING:** proporciona un ping a una IP o DNS.
- **CIRD:** calcula la máscara de red de donde está el host.
- **ISP CACHED DNS LOOKUP:** visualiza la cache de un registro DNS.



← Algunas herramientas gratuitas (free tools) de dnsstuff.com.

ACTIVIDADES

11. Edita el archivo named.conf y explica qué hace.
12. Edita el archivo named.conf.local y explica qué hace.
13. Edita uno de estos archivos db.127, db.0, db.255 y explica qué hace.
14. Edita el archivo db.localhost y explica qué hace. Si no existe busca uno llamado db.root.
15. Configura con BIND en Linux un dominio local (por ejemplo, dominiolocal) para tu ordenador y, al menos, el de dos compañeros del aula de prácticas.
16. Realiza el ejercicio anterior en Windows.
17. Comprueba en Linux y Windows que los servidores funcionan con las órdenes ping, etc.
18. Utiliza dig para saber los 13 servidores DNS del nivel raíz.
19. Utiliza dig para conocer el servidor de todos los ccTLD de los países, estados o regiones de tus compañeros.
20. Utiliza dig para ver qué servidores del nivel raíz están preparados para la versión de IPv6.
21. Entra en <http://www.root-servers.org/> para conocer los servidores redundantes del nivel raíz.
22. ¿Qué opinas de que los servidores se concentren en California, Nueva York, el norte de Europa y Japón?
23. Utiliza las órdenes dig, host, nslookup, ping, ipconfig y las páginas de registradores (nominalia.com, whois.net, etc.) para recopilar el máximo de información de los siguientes dominios:

a) google.com	c) yahoo.com	e) facebook.com	g) live.com
b) msn.com	d) blogger.com	f) youtube.com	h) red.es

ACTIVIDADES FINALES

- 1. Busca en internet servidores DNS de otros ISP que no sean los que utilizas. Configúralos en Windows. Prueba uno que permita que te conectes a internet (ISP pequeños) y otro que no (ISP de Telefónica). ¿Cómo crees que lo hacen? ¿Por qué crees que pasa que los grandes sí y los pequeños no?
- 2. El archivo hosts (/etc/hosts) puede estar vacío, pero lo normal es que contenga esta línea: inicialmente: 127.0.0.1. localhost.localdomain. ¿Qué significa o qué hace esta línea?
- 3. El archivo por defecto de BIND tiene:

```
options {
    allow-query { 127/8; } ;
} ;
zone "localhost" in {
    type master;
    file "db.localhost";
} ;
zone "0.0.127.in-addr.arpa" in {
    type master;
    file "db.127.0.0";
} ;
zone "." in {
    type hint;
    file "root.hint";
} ;
```

¿Qué consigue esta configuración?

¿Cómo ampliarías la configuración para que soporte la red local 192.168.0.0/24?

- 4. Identifica los servicios, prioridades y pesos del siguiente fragmento del archivo db.aula.inf:

ftp.tcp	SRV 0 0 21	ftp.aula-inf.org.
ssh.tcp	SRV 0 0 22	aula-inf.org.
telnet.tcp	SRV 0 0 23	aula-inf.org.
smtp.tcp	SRV 0 0 25	smtp.aula-inf.org.
http.tcp	SRV 0 3 80	aula-inf.org.
http.tcp.ww	SRV 0 1 80	ns2.aula-inf.org.
http.tcp.ww	SRV 0 3 80	aula-inf.org.
https.tcp	SRV 0 1 80	ns2.aula-inf.org.
https.tcp	SRV 1 0 443	aula-inf.org.
https.tcp.ww	SRV 2 0 4443	ns2.aula-inf.org.
https.tcp.ww	SRV 1 0 443	aula-inf.org.
pop3s.tcp	SRV 2 0 443	ns2.aula-inf.org.
* .tcp	SRV 0 0 995	pop3.aula-inf.org.
* .udp	SRV 0 0 0	.

■ 5. /var/named/root.hints // Renuévalo con dig:

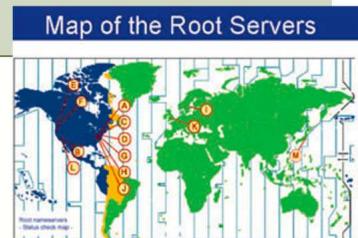
```

6D IN NS A.ROOT-SERVERS.NET.
6D IN NS B.ROOT-SERVERS.NET.
6D IN NS C.ROOT-SERVERS.NET.
6D IN NS D.ROOT-SERVERS.NET.
6D IN NS E.ROOT-SERVERS.NET.
6D IN NS F.ROOT-SERVERS.NET.
6D IN NS G.ROOT-SERVERS.NET.
6D IN NS H.ROOT-SERVERS.NET.
6D IN NS I.ROOT-SERVERS.NET.

A.ROOT-SERVERS.NET. 6D IN A 198.41.0.4      //com, US
B.ROOT-SERVERS.NET. 6D IN A 128.9.0.107     //edu, US
C.ROOT-SERVERS.NET. 6D IN A 192.33.4.12     //com existe slave en MAD
D.ROOT-SERVERS.NET. 6D IN A 128.8.10.90     //edu, US
E.ROOT-SERVERS.NET. 6D IN A 192.203.230.10  //*, US
F.ROOT-SERVERS.NET. 6D IN A 192.5.5.241     //com existe slave en MAD y BCN
G.ROOT-SERVERS.NET. 6D IN A 192.112.36.4    //*, US
H.ROOT-SERVERS.NET. 6D IN A 128.63.2.53     //*, US
I.ROOT-SERVERS.NET. 6D IN A 192.36.148.17   //int, SE

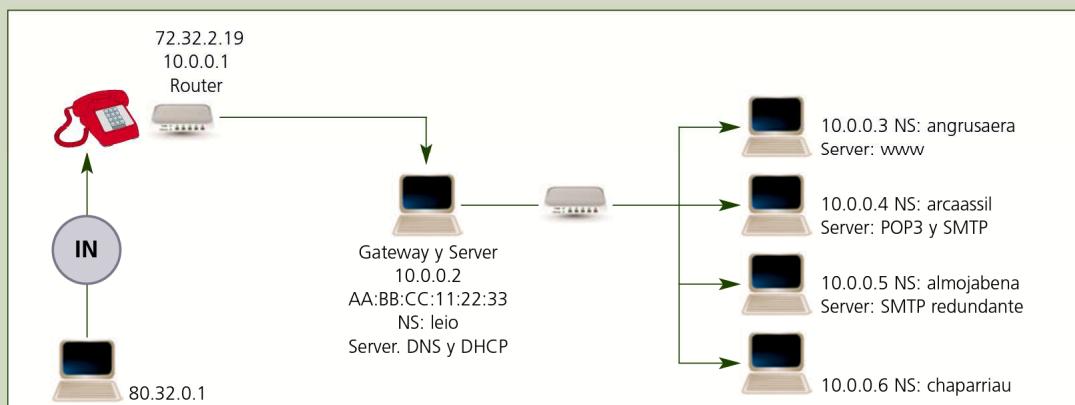
```





¿Qué hace este fragmento de archivo?

■ 6. Realiza los archivos de configuración necesarios para el servidor DNS:



- Hemos alquilado el DNS pancho.int y nuestro ISP nos autoriza para administrarlo.
 - Nuestra LAN tiene la máscara de red 255.255.0.0.
 - En un site nos regalan la gestión de un servidor secundario (que no podemos modificar) en la IP 80.32.0.1.
 - No olvides filtrar los paquetes del tipo tcp.

PRÁCTICA PROFESIONAL

material

- PC con Linux Ubuntu, última versión (o máquina virtual, mínimo Ubuntu con kernel 2.6).
- Ordenadores con Windows.
- Conexión a internet.

Instalación y configuración de un servidor DNS (BIND) en Linux y dos clientes en Windows

Objetivo:

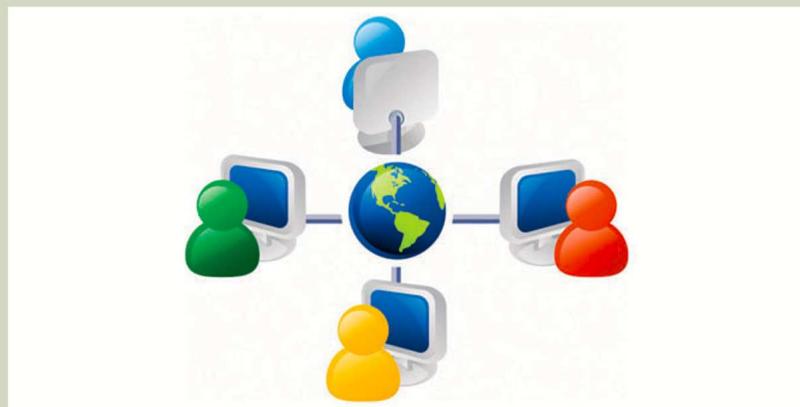
Instalar un servidor DNS con las técnicas que hemos estudiado en la unidad.

Desarrollo:

1. Instala el servidor DNS en el equipo con Linux. Usa el CD de Ubuntu o hazlo desde internet (paquete bind9).

2. Configura el servidor DNS, editando el archivo named.conf y:

Nombra servidor a tu equipo, llama pc01, pc02, etc., al menos hasta cinco equipos del aula de prácticas. Invéntate un dominio o usa aula-inf.



Si suponemos que en clase de prácticas la red es una 192.168.0.0/24 y tu equipo es el 192.168.0.2, el archivo debería quedar más o menos así:

//192.168.0.2/etc/bind9/named.conf

```
zone "aula-inf" {
    type master;
    file "db.aula-inf";
} ;
zone "0.168.192.in-addr.arpa" {
    type master;
    file "db.192.168.0";
} ;
allow-query {192.168.0.0/24;} ;
allow-transfer {none;} ;
```

```
//192.168.0.2/etc/bind9/db.aula-inf
```

```
$TTL 604800
@ IN SOA aula-inf hostmaster.aula-inf (20090517001;
10800; 7200; 1296000; 172800 );

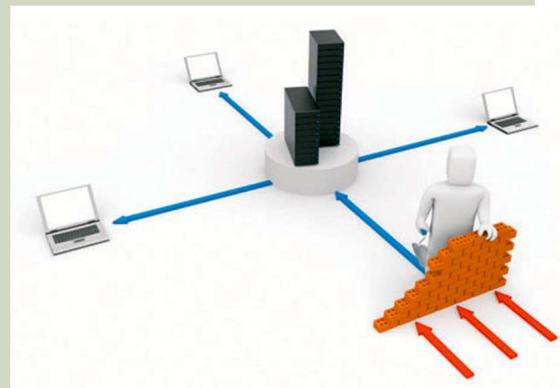
localhost.aula-inf A 127.0.0.1
servidor.aula-inf A 192.168.0.2
pc01.aula-inf A 192.168.0.1
pc02.aula-inf A 192.168.0.2
pc03.aula-inf A 192.168.0.3
pc04.aula-inf A 192.168.0.4
pc05.aula-inf A 192.168.0.5
*.tcp SRV 0 0 0 .
```

```
//192.168.0.2/etc/bind9/ db.192.168.0
```

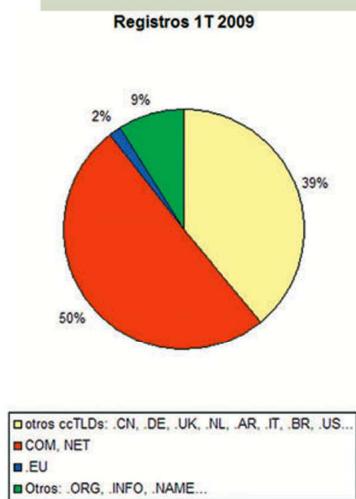
```
$TTL 604800
@ IN SOA aula-inf hostmaster.aula-inf (
20090517001 ; 10800 ; 7200 ; 1296000 ; 172800);

@ IN NS aula-inf
1 IN PTR pc01.aula-inf
2 IN PTR pc02.aula-inf
3 IN PTR pc03.aula-inf
4 IN PTR pc04.aula-inf
5 IN PTR pc05.aula-inf
```

3. Arranca el servidor para hacer efectiva la nueva configuración.
4. Configura los dos equipos-cliente para que funcionen con este servidor DNS (con la IP del servidor DNS).
5. Reinicia los equipos-cliente.
6. Comprueba:
 - que funciona internet en los equipos-cliente;
 - con un ping, si funciona servidor.aula-inf;
 - al menos dos equipos de tu LAN.
7. Pruébalo desde los clientes.



MUNDO LABORAL



Los nombres de dominio superan los 180 millones

Internet incorpora más de 180 millones de nombres de dominios, según el resumen de la industria de nombres de dominios en internet para el primer trimestre del 2009, publicado por VeriSign.

El primer trimestre del 2009 finalizó con una base total de alrededor de **183 millones de nombres de dominios** registrados entre todos los Dominios de Primer Nivel (**TLD**). Esto significa un crecimiento del 3% con respecto al cuarto trimestre de 2008 y un crecimiento del 12% con respecto al mismo trimestre del año pasado.

Los dominios de primer nivel con código de país (**ccTLD**) alcanzaron **74.1 millones** durante el primer trimestre, un aumento del 4% con respecto al trimestre anterior y un incremento del 18% año tras año. De acuerdo con los registros totales, **.com** permanece como el TLD más popular, seguido por los **.cn** (China), **.de** (Alemania) y **.net**. Esta composición permanece sin cambios desde el cuarto trimestre de 2008. [...]

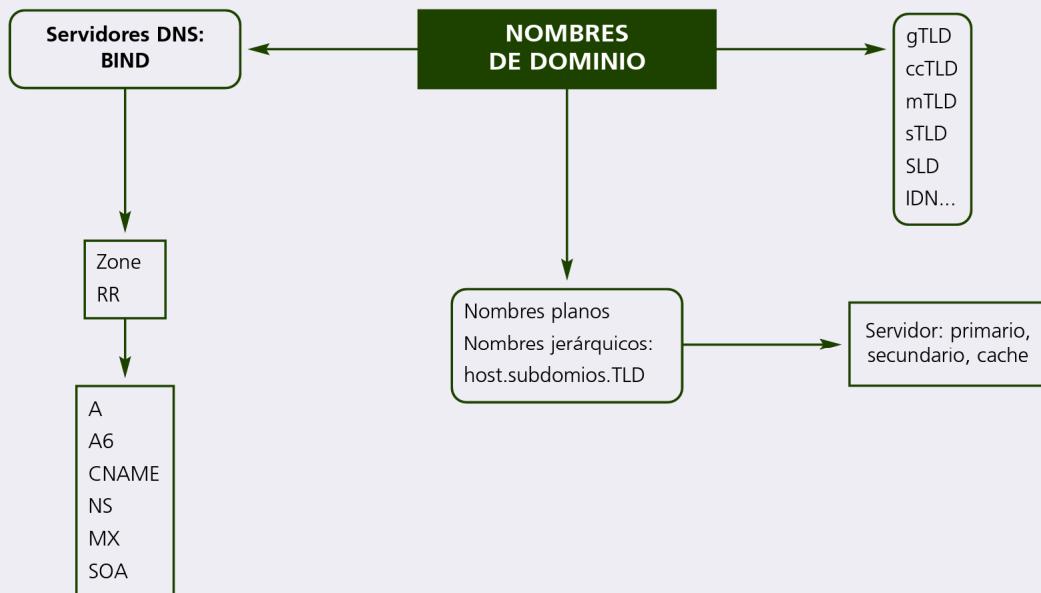
«En su carácter de operador de registro autoritativo para los nombres de dominios .com y .net, VeriSign cuenta con una visión única del pulso de internet», dijo Jill Corso McNabb, vicepresidente de Servicios de Registro de Dominios de VeriSign. «La resolución del DNS realmente es el eje de lo que hace que internet opere en todo el mundo. **El DNS se vuelve aún más crítico para la infraestructura general de internet, no solo por el creciente uso de internet, sino también por la proliferación de productos y servicios innovadores relacionados** con el DNS.»

Publicado el primer trimestre de 2009 por diarioti.com.
[<http://www.infonortedigital.com/index.php?id=47091&sección=24>](http://www.infonortedigital.com/index.php?id=47091&sección=24).

Actividades

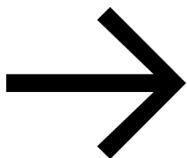
1. Contesta a las siguientes preguntas:
 - ¿Te ha pasado alguna vez agregar al Messenger a un amigo, con correo, por ejemplo, pepe@hotmail.es y haber puesto en su lugar pepe@hotmail.com?
 - ¿Crees que son útiles los dominios que no son .com?
 - ¿Crees más útil un dominio terminado en .ea, .es, .eu o en .com?
2. Discutid en grupos de cuatro la conveniencia de los TLD lingüísticos (tipo .cat y el que se está proponiendo para el gallego) sobre dominios internacionales en países con varias lenguas.
3. ¿Conoces algún TLD que se esté proponiendo ahora? ¿Cuál? ¿Lo ves interesante?
4. Busca en internet y compara los precios de alquiler bianual de los siguientes TLD: .com, .es, .tv, .fm, .eu, .uk, .cat, .info, .name, .ru y .mobi.

EN RESUMEN



EVALÚA TUS CONOCIMIENTOS

1. Para configurar un servidor DNS en una LAN:
 - a) Necesito BIND.
 - b) Necesito el archivo hosts.
 - c) Las opciones a) y b) son válidas.
 - d) Ninguna de las anteriores.
2. ¿Qué dirección no es una FQDN?
 - a) Informatica.uam.es
 - b) http://www.Informatica.uam.es/misdocumentos/index.htm
 - c) 3.14159.org
 - d) del.icio.us
3. ¿Qué nombre de dominio es menos aconsejable?
 - a) cocacola.com.co
 - b) cocacola.φ
 - c) barça.eu
 - d) estaeslapaginamaslargaquepodrasencontrardedicadaamotos.com
4. Completa en tu cuaderno de prácticas las siguientes frases:
 - Los TLD _____ pueden alquilarse por todo el mundo.
 - Los TLD _____ pueden alquilarse si se cumplen una serie de restricciones.
 - Los ccTLD más registrados son _____.
 - El mTLD es _____.
 - El único TLD lingüístico patrocinado es _____ aunque otras lenguas, como por ejemplo el gallego, ya están pidiendo su propio TLD.
5. Los registros (RR), en direccionamiento inverso, pueden ser:
 - a) A para IPv4 o A6 IPv6.
 - b) NS, MX y PTR.
 - c) Obligatorios A, NS, SOA y PTR; y optativos CNAME, MX.
 - d) Ninguna es correcta.



Redacción y selección de contenidos: Joaquín Andreu

Edición: Montserrat Sánchez

Diseño de cubierta: Paso de Zebra

Fotocomposición, maquetación

y realización de gráficos: MT Color & Diseño, S. L.

Fotografías: Microsoft Corporation; Canonical Ltd.; Apple Inc.; Bind, licencia BSD; ICANN; PuTTY, Simon Tatham; OpenSSH, OpenBSD; Webmin; TeamViewer GMBH; RealVNC Limited; Medialogic; Google; Google Inc.; Mozilla Foundation; Filezilla-project.org; gFTP, Brian Masney ; GNU.org; OpenSight Software, LLC; cPanel Inc.; Cuerpo Nacional de Policía, Ministerio del Interior, Gobierno de España; Fábrica Nacional de Moneda y Timbre, Ministerio de Economía y Hacienda, Gobierno de España; Conselleria de Justicia i Administracions Públiques, Generalitat Valenciana; Agència Catalana de Certificació, Generalitat de Catalunya; Yahoo!; Adobe Systems Incorporated; Romain Bourdon; The Apache Software Foundation; Oracle Corporation; The PHP Group; GNU; 3Com Corporation; PLANET Technology Corporation; GSMA; Telefónica Móviles España, SAU; France Télécom; The Information Technology & Innovation Foundation; TeleAtlas; HISPAKSAT, SA; SES ASTRA, Grupo SES; NEO-SKY 2002, SA; Euskaltel, SA; Xfera Móviles, SA; EDIMAX Technology Co.; Check Point Software Technologies Ltd.; Agnitum Ltd.; Bluetooth SIG.; Wi-Fi Alliance; IEEE; D-LINK Europe Ltd.; Jinx, Inc.; Medion Iberia, SL; Sony Computer Entertainment Europe; Symantec Corporation; Bratel Co., Ltd.; Technicolor; Koninklijke Philips Electronics N.V.; Accton Technology Corporation; Skype Limited; Cisco System, Inc.; ITU; ISOC; Digium, Inc.; Peoplecall the callshop Co.; Vonage Marketing LLC; AOL Inc.; Telefonica USA Inc.; Jajah, Inc.; CounterPath Corporation; Internap Network Services Corporation; iDATE FR; Getty Images (Photos.com) y archivo Editex

Dibujos: Ángel Ovejero

Dirección producción: Teresa del Arco

Preimpresión: José Ciria

Producción editorial: Francisco Antón

Dirección editorial: Carlos Rodríguez

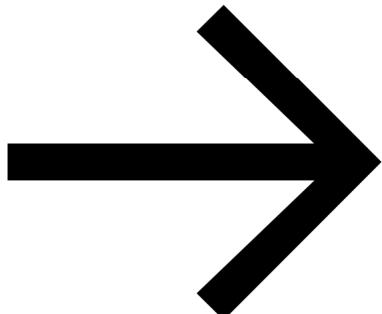
Editorial Editex, S. A. ha puesto todos los medios a su alcance para reconocer en citas y referencias los eventuales derechos de terceros y cumplir todos los requisitos establecidos por la Ley de Propiedad Intelectual. Por las posibles omisiones o errores, se excusa anticipadamente y está dispuesta a introducir las correcciones precisas en posteriores ediciones o reimpresiones de esta obra.



El presente material didáctico ha sido creado por iniciativa y bajo la coordinación de **Editorial Editex, S. A.**, conforme a su propio proyecto editorial.

© **Editorial Editex, S. A.**

Vía Dos Castillas, 33. C.E. Ática 7, edificio 3, planta 3^a, oficina B
28224 Pozuelo de Alarcón (Madrid)



Cualquier forma de reproducción, distribución, comunicación pública o transformación de esta obra solo puede ser realizada con la autorización de sus titulares, salvo excepción prevista por la ley. Diríjase a CEDRO (Centro Español de Derechos Reprográficos, www.cedro.org) si necesita fotocopiar o escanear algún fragmento de esta obra.