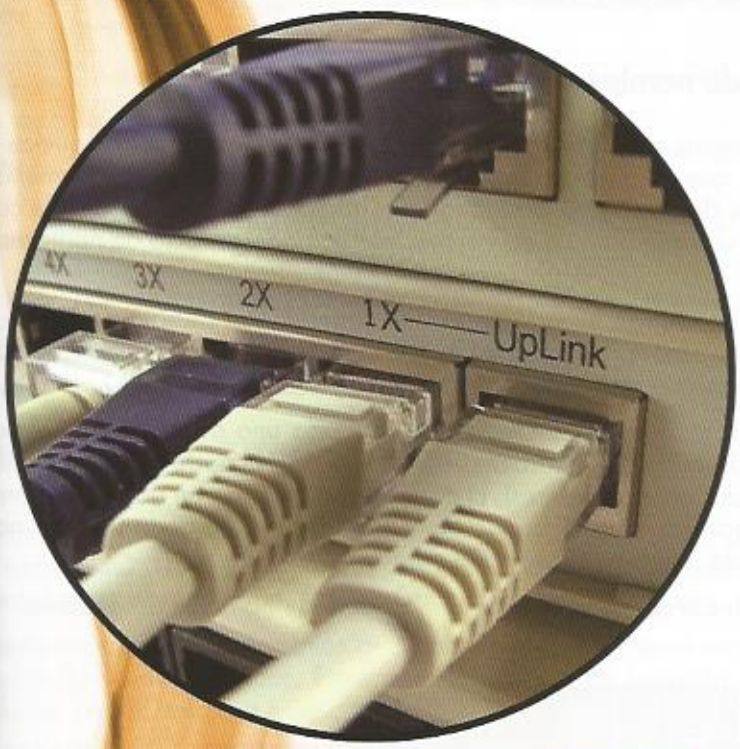
Unidad 2

Servicio de nombres de dominio (DNS)



En esta unidad aprenderemos a:

- Conocer el funcionamiento básico del servicio DNS.
- Entender y diferenciar el funcionamiento del cliente y el servidor DNS, procesos implicados y sus funciones.
- Poner en marcha un servidor DNS bajo Ubuntu GNU/Linux, comprobando su funcionamiento con diferentes parámetros de configuración.
- Poner en marcha un servidor DNS bajo Windows 2008 Server, comprobando su funcionamiento con diferentes parámetros de configuración.
- Conocer el funcionamiento básico del servicio DNS dinámico.

Y estudiaremos:

- El concepto de «resolución» de nombres.
- Los conceptos asociados necesarios para comprender los mecanismos de resolución de nombres.
- La instalación y configuración del servicio desde las perspectivas del servidor y del cliente.
- La utilización del servicio DNS proporcionado por servidores públicos.
- Los pasos necesarios para la creación de nuevas zonas.
- Las configuraciones específicas en sistemas operativos libres y propietarios.

1. ¿Qué es el servicio DNS?

Importante

El servicio DNS proporciona un mecanismo de traducción de nombres de dominio a direcciones IP únicas para localizar el servidor donde reside un sitio web.

Un dominio o nombre de dominio es el nombre que identifica un sitio web. El dominio tiene que ser único en Internet. Por ejemplo, **www.google.es** es el nombre de dominio del sitio web de Google en España.

El **servicio DNS** (Domain Name System), o sistema de nombres de dominio, gestiona y mantiene de forma distribuida las direcciones de Internet y los nombres de dominio. Se trata de un servicio de búsqueda de direcciones IP y de nombres de dominios para una red TCP/IP.

En una red TCP/IP las máquinas se identifican mediante su dirección de red o número IP. Sin embargo, para las personas resulta mucho más sencillo recordar un nombre que se asocia a una máquina concreta. Y también es más fiable, ya que la dirección IP puede cambiar, mientras que con el nombre esto es menos probable. Ello hace necesario establecer un mecanismo de traducción de nombres de máquina a direcciones IP. DNS es el servicio que proporciona este mecanismo de traducción.

1.1. El espacio de nombres de dominio

El servicio DNS se compone de una base de datos distribuida (en varias máquinas conectadas en red) en la que se almacenan las asociaciones de nombres de dominios y direcciones IP. Esta base de datos está clasificada por nombres de dominio, donde cada nombre de dominio es una rama en un árbol invertido llamado **espacio de nombres de dominio.**

El árbol comienza en el nodo raíz situado en el nivel superior. Por debajo de él pueden existir un número indeterminado de nodos de nivel inferior. Normalmente se utilizan hasta cinco niveles. Por ejemplo, **www.ite.educacion.es** tiene tres niveles.

¿Sabías que...?

La forma básica de traducción de nombres a direcciones IP (y viceversa) inicialmente era almacenando estos valores en un archivo llamado `/etc/hosts` en GNU/Linux.

El archivo `/etc/hosts` en Windows es idéntico al utilizado por GNU/Linux. Contiene la dirección IP y el nombre de la máquina a la que se refiere. Si se utilizan nombres NetBios con WINS, el archivo se llama `Lmhosts`.

Los nodos se identifican mediante nombres no nulos, cada uno de los cuales pueden contener un determinado número de caracteres (máximo 63). El nodo raíz se identifica mediante un nombre nulo (cero caracteres). El nombre completo de un nodo está formado por el conjunto de nombres que forman la trayectoria desde ese nodo hasta el nodo raíz. Como separador de nombres se utiliza el carácter punto (.).

La Figura 2.1 muestra la estructura jerárquica del espacio de nombres de dominio.

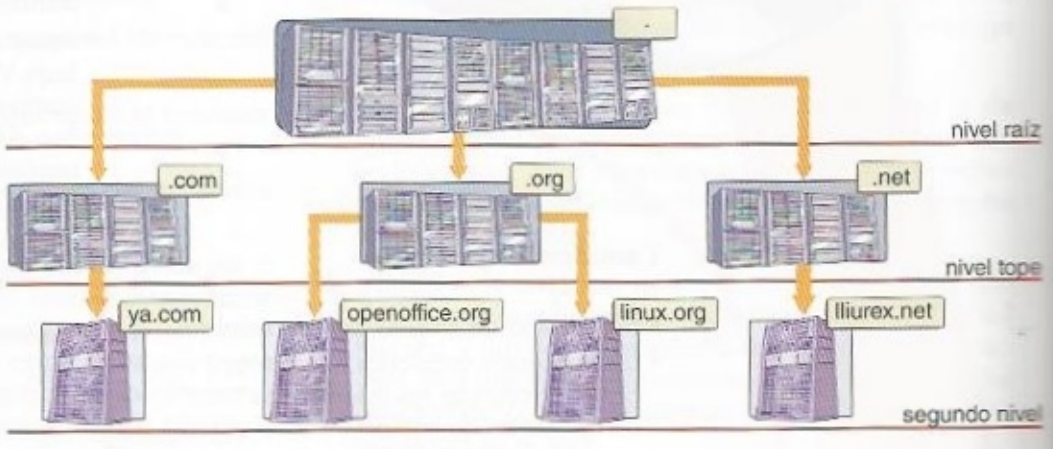


Fig. 2.1. *Estructura del árbol de nombres de dominio.*

CEO

En el CEO dispones del documento denominado *U02_SER_DNS_Historia.pdf*. El documento contiene una breve reseña histórica del protocolo DNS y sus RFCs asociados.

De esa forma, el nombre del nodo se identifica de forma única dentro de la jerarquía que genera el árbol de nombres de dominio. El nombre de dominio completo se llama **nombre de dominio completamente cualificado** (FQDN, del inglés Fully Qualified Domain Name). El FQDN de cualquier nodo del árbol siempre debe acabar con un punto, ya que el nodo raíz se identifica mediante un nombre nulo.

Por tanto, el **dominio** es cada uno de los subárboles del espacio de nombres de dominio (árbol de nombres de dominio).

Los diferentes servidores DNS que existen en la red almacenan la información relativa a los nombres de dominio DNS en los llamados **registros de recursos.** Un servidor DNS tendrá aquellos registros de recursos que le permitan responder a las peticiones de nombres relativas a la parte del espacio de nombres de dominio sobre la que tiene autoridad dicho servidor.

La organización del servicio DNS se basa en niveles según la posición del dominio. El nivel superior o primer nivel (**TLD,** Top Level Domain) lo forman aquellos dominios descendientes directos del dominio raíz. Los principales TLD genéricos son los que recoge la Tabla 2.1:

TLD	Descripción
com	Agrupa organizaciones comerciales. Ejemplos: google.com, yahoo.com, strands.com.
edu	Reúne organizaciones educativas universitarias. Ejemplos: eada.edu, ortegaygasset.edu, mit.edu.
net	Agrupa organizaciones dedicadas a Internet y a las telecomunicaciones. Ejemplos: rpmfind.net, listas.net, php.net.
org	Reúne organizaciones no comerciales. Ejemplos: linuxdoc.org, ubuntu.org, linux.org, insflug.org.
gov	Agrupa organizaciones gubernamentales de EEUU. Ejemplos: nasa.gov, nsf.gov, whitehouse.gov.
int	Se usa en organizaciones internacionales. Ejemplos: redcross.int, interpol.int, coe.int
name	Se emplea para nombres de personas.
mobi	Es propio de empresas de telefonía móvil o servicios para móvil.

Tabla 2.1. *Descripción de algunos TLD.*

Existen también dominios de primer nivel que designan zonas geográficas y que siguen la norma ISO 3166. Sus nombres representan a todos los países a través de dos letras. Ejemplos: **es** para España, **fr** para Francia, ***de*** para Alemania, etc.

Puede ocurrir que los dominios geográficos de primer nivel contengan a su vez alguno de los dominios genéricos. Estos dominios serían de segundo nivel. Ejemplos: *com.es, edu.au, org.uk, teso.org.es*, etc.

El **ICANN** (Internet Corporation for Assigned Names and Numbers) es el organismo encargado de la gestión de los dominios raíz y TLD. Su web es **http://www.icann.org.**

Los dominios asociados a cada país son registrados por las autoridades locales que, en el caso de España, es el ESNIC, actualmente integrado en Red.es (entidad pública empresarial adscrita al Ministerio de Industria, Energía y Turismo). Por tanto, para la creación de un dominio **.es** una de las opciones es solicitarlo al ESNIC o a través de alguna empresa-agente registradora de dominios española, como Acens, Arsys, Interdominios, etc. La gestión de los dominios .es se puede hacer desde **https://www.nic.es/** y en **http://www.eurid.eu/** para los dominios **.eu.**

¿Sabías que...?

El espacio de nombres de dominio es jerárquico. Internet se divide en cientos de dominios:

- Genéricos: .com, .edu, .gov, .int, .mil, .net, .org.
- De país: una entrada por país: .es, .fr, .uk, etc.
- Otros: .aero, .biz, .coop, .info, .pro, .name, .museum, .firm, .store, .nom, .arts, etc.

Cada dominio se divide en subdominios:

- máquina.subdominio.subdominio...dominio, etc.

Cada nivel va delegando autoridad en los niveles inferiores.

Importante

El servicio DNS utiliza el puerto 53/UDP para atender las consultas de nombres y el puerto 53/TCP para transferencias de zona entre servidores.

Actividades

1. Busca en Internet una definición del concepto de root server.
2. Averigua qué son los nombres NETBIOS de Windows y cuál es la diferencia con los nombres Hostname.
3. Busca la web de La Moncloa, de la Presidencia de tu Comunidad Autónoma y del Ayuntamiento al que pertenezcas. ¿Cuáles son los TLD que utilizan estos dominios?
4. ¿Dónde puedes acceder para ver todos los dominios geográficos (ccTLD) de primer nivel?
5. En la tabla de root servers (**www.root-servers.org**), busca la IPv4 e IPv6 del operador ICANN. ¿Dónde está localizado?
6. Localiza instituciones relacionadas con los dominios de Internet.

Importante

La **delegación** es la acción de cesión de la autoridad por parte del dominio padre sobre alguno de sus subdominios. El dominio padre puede retomar dicha autoridad cuando quiera.

1.2. La delegación de dominios

DNS es una base de datos distribuida y permite su administración descentralizada. La **delegación de dominios** es el mecanismo que permite llevar a cabo esa administración descentralizada. Es decir, el dominio puede ser dividido en **subdominios** por el administrador del mismo, y el control de cada subdominio puede ser delegado. La condición es que la autoridad que asume la delegación asuma también la responsabilidad de mantener actualizados los datos de ese subdominio (es decir, los registros de recursos).

Pero delegación no significa independencia, sino coordinación. Si al dominio padre se le plantean consultas acerca de nombres incluidos en uno de sus subdominios delegados puede hacer referencia a dichos subdominios, ya que mantiene enlaces con ellos para hacer efectiva la consulta.

La división de un dominio en subdominios no implica siempre la cesión de la autoridad sobre ellos. En principio, un dominio puede subdividirse en diferentes subdominios y mantener la autoridad sobre ellos. Pero también puede, si así se decide, delegar la autoridad de algunos de sus subdominios.

1.3. ¿Qué son los dominios y zonas?

El servidor de nombres almacena información acerca de algunas partes del espacio de nombres de dominio. Cada una de esas partes se llama **zona,** y se dice que el servidor de nombres tiene **autoridad sobre la zona.** Por tanto, un servidor de nombres podrá tener autoridad sobre varias zonas.

La zona en realidad es un archivo que contiene determinados registros de la base de datos del espacio de nombres de dominio. Estos registros identifican a uno o más dominios. Mediante estos registros la zona puede atender las peticiones de los clientes y por ello también se les llama zonas de autoridad. Por lo tanto, la generación de zonas se hace mediante la delegación de autoridad.

En la Figura 2.2 se observa que el dominio **nombre1.org** contiene a su vez los dominios **ftp.nombre1.org** y **www.nombre1.org** y, junto con el dominio **nombre1.org,** constituyen la **zona1** con autoridad delegada desde el dominio **org.** Lo mismo sucede con el dominio **nombre2.org.**

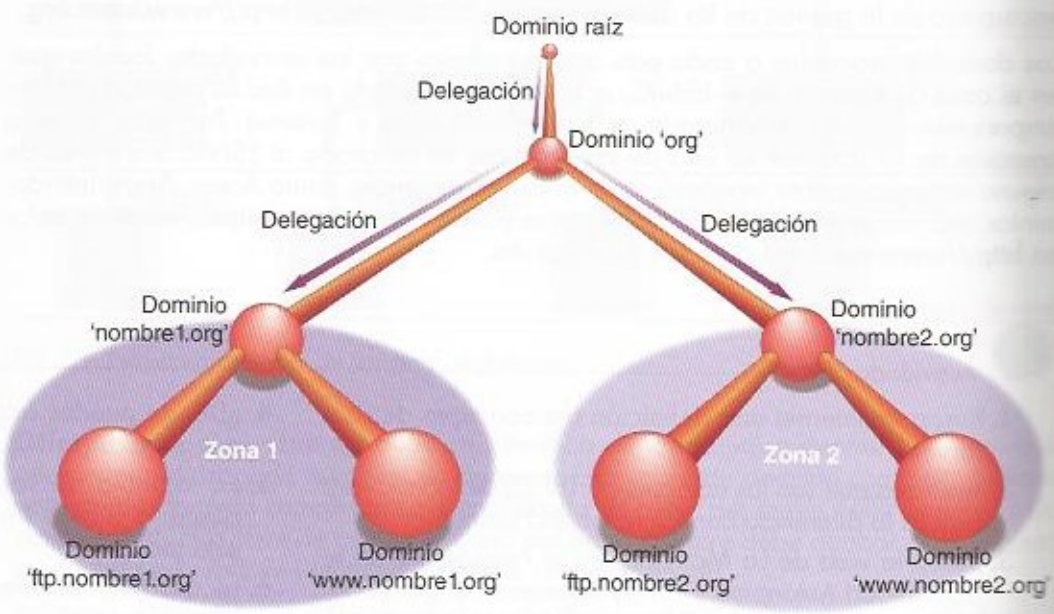


Fig. 2.2. *Zonas y dominios.*

¿Sabías que...?

Un servidor de nombres de dominio DNS es autoritario para una zona si contiene los registros de recursos para dicha zona. Para ello se utilizan los registros de recursos SOA y NS.

Para que DNS sea tolerante a fallos se recomienda utilizar dos o más servidores de nombres de dominio autoritarios por zona, donde al menos uno de ellos sea primario. El resto puede ser secundario o caché.

Los servidores de nombres se pueden clasificar en los tipos siguientes:

1. **Servidor primario** (maestro): obtiene la información de sus zonas de sus archivos locales. Todas las modificaciones sobre una zona, como añadir dominios, se llevan a cabo en el servidor primario.
2. **Servidor secundario** (esclavo): obtiene la información de sus zonas de otro servidor de nombres (generalmente, un servidor primario) que tiene autoridad sobre esas zonas. El servidor secundario contiene una copia de solo lectura de los archivos de zona.
3. **Servidor caché:** solo atiende consultas de los clientes DNS (resolvedores) sobre nombres de dominios. No contiene ningún tipo de información acerca de la zona. Se utiliza para acelerar las consultas.

Actividades

7. Averigua en qué consiste el «DNS Cache Poisoning».
8. ¿Cuál es la diferencia entre dominio y zona?

El mecanismo de obtención de la información de las zonas a través de la red se denomina **transferencia de zona** (Fig. 2.3). Los servidores de nombre secundarios solicitan esta acción con el objetivo de mantener actualizada la información acerca de la zona, y así tenerla correctamente duplicada. Este es el motivo por el que es interesante que, para cada zona, exista al menos un servidor primario y otro secundario. En el caso de fallo de alguno de ellos, el otro atiende las peticiones de resolución de nombres.

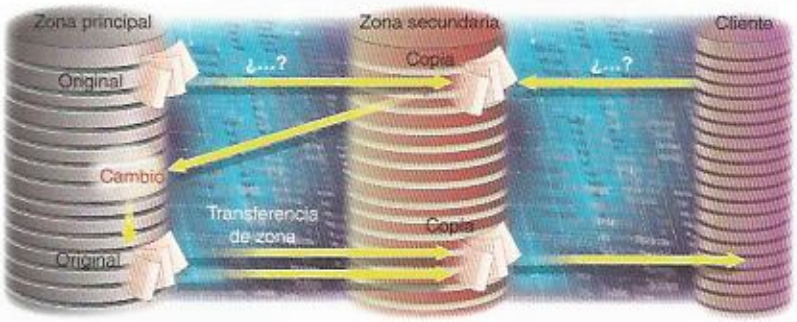


Fig. 2.3. *Transferencia de zona.*

Si un usuario de Internet quiere ofrecer a la red determinados servicios propios deberá contratar un servicio de hospedaje (hosting) junto con un dominio a una empresa proveedora de estos servicios. Este nombre de dominio es el que utilizarán el resto de internautas para acceder a su página web, portal o servicios que ofrezca.

El Caso práctico 1 muestra este proceso para Acens (acens.com), pero existen muchas otras empresas para el registro de dominios, como joker.com, arsys.es, etc.

Caso práctico 1

Registro de un dominio en Acens

- **Duración:** ◷ depende de la conexión a Internet disponible en el aula
- **Dificultad:** ☺ fácil

Objetivo: registrar un dominio para utilizar en el aula en este módulo profesional de Servicios en Red (SER). Se trata de una simulación con el fin de mostrar los pasos necesarios. Para ello hay que acceder a la página web de Acens **(www.acens.com).**

Desarrollo:

1. Verificar la disponibilidad del dominio

Nuestra intención es registrar el dominio **aulaSER.com,** pero este nombre de dominio no es aceptado (Fig. 2.4).

Fig. 2.4. *Propuesta de nombre de dominio.*

2. Selección del nombre de dominio

[illegible] el proceso y muestra los nombres de dominio disponibles que siguen el patrón de nombre dado junto con las tarifas. Selecciona **aulaser.com** y continúa el proceso.

Comprobaremos que ya está contratado este dominio, pero nos ofrece **aulaser.es** por un precio razonable (Fig. 2.5).

Contrata el dominio **aulaser.es.** Lee y acepta las condiciones del contrato.

(Continúa)

Caso práctico 1

(Continuación)

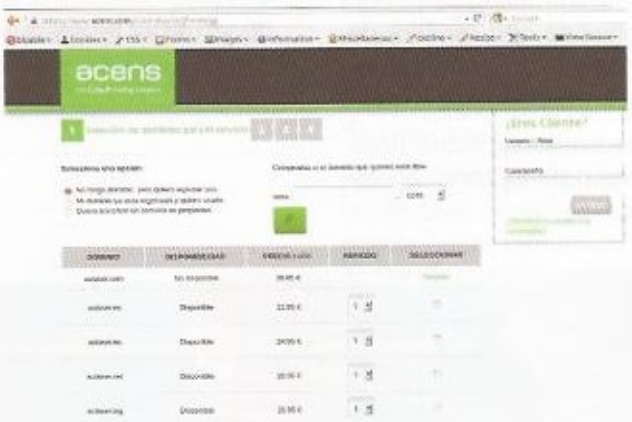


Fig. 2.5. *Selección de periodo de contratación.*

La Figura 2.6 muestra las dos opciones disponibles:

- Nuevo cliente, que requiere el registro introduciendo el NIF y pulsar el *Alta de cliente.*
- Cliente existente, que requiere únicamente introducir el nombre de usuario y contraseña y pulsar en *Continuar.*

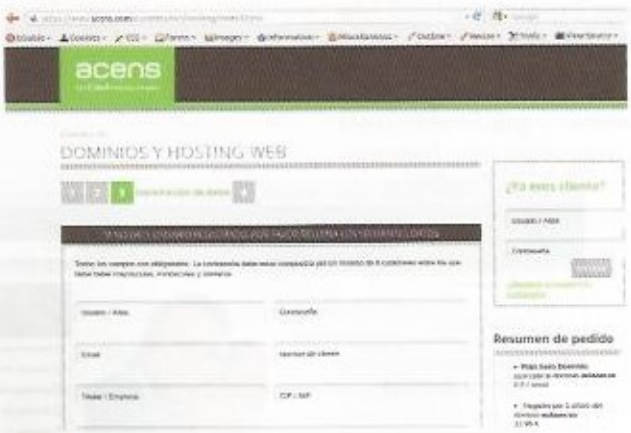


Fig. 2.6. *Contratación del dominio.*

En el caso, nuestro de cliente nuevo habría que introducir un NIF válido y continuar con el proceso.

3. Datos de contacto

Elige una contraseña con un buen nivel de seguridad y proporciona los datos de contacto y facturación. Termina el proceso.

Fig. 2.7. *Selección del método de pago.*

Es importante tener en cuenta que, una vez el dominio ha sido ya contratado, el dueño del mismo debe esperar un tiempo para que este sea reconocido en todos los servidores de Internet. Para los dominios .com y .net la demora es entre 4 y 8 horas, y para otros puede llegar a estar entre 24 y 48 horas. Durante este tiempo se registra el dominio en el ICANN y se avisa al registrador de que el dominio ha sido registrado.

El nuevo dominio funciona, y resuelve a la IP apropiada en el servidor DNS usado, pero para que lo haga en el resto de servidores DNS del mundo debe propagarse al resto de servidores, y como cada uno tiene distintos tiempos de actualización y parámetros de caché distintos, pueden pasar varias horas hasta que todos los servidores DNS del mundo conozcan cómo hacer la resolución del dominio. En este momento la página ya es accesible mediante un nombre de dominio desde cualquier máquina.

Actividades

9. Haz un estudio comparativo de precios de registro de dominios para diferentes empresas.

¿Conoces los dominios **.tk**? Busca información sobre ellos. Quizá te pueda interesar.

10. ¿Cuál es el puerto o puertos de escucha del servicio DNS por defecto?

11. ¿Cómo comprobarías que se están resolviendo nombres de ordenadores?

12. ¿Que entiendes por enrutamiento?

1.4. Red ejemplo y base para el desarrollo de la unidad

La configuración del servicio DNS se hará tomando como base el esquema de aula indicado en el esquema 2, de modo que haya un servidor DNS de aula con dos interfaces de red y el resto de ordenadores sean clientes.

Trabajamos con el dominio **aulaSER.com.** Por tanto, todos los ordenadores tendrán un nombre de dominio de la forma **nombre_ordenador.aulaSER.com.**

Los nombres de los ordenadores serán de la forma *pcXY*, donde *X* será el número de fila o grupo e *Y* será el número de equipo dentro del mismo. Por ejemplo, *pc11* es el primer equipo de la fila 1; *pc21* es el primer equipo de la fila 2, etc.

Los ordenadores forman parte de la red Ethernet definida en el aula con direcciones IP del tipo 192.168.100.XX. El ordenador servidor hace funciones de enrutamiento entre la red del aula e Internet a través de sus dos interfaces de red. La tabla de ordenadores es la indicada en el esquema 2 (Fig. 2.8). Siguiendo este esquema, el servidor está conectado al router del aula (192.168.0.1) a través de la interfaz de red eth1 con IP 192.168.0.100. La interfaz *eth0* escucha dentro del aula y hace de puerta de enlace, con IP 192.168.100.254.

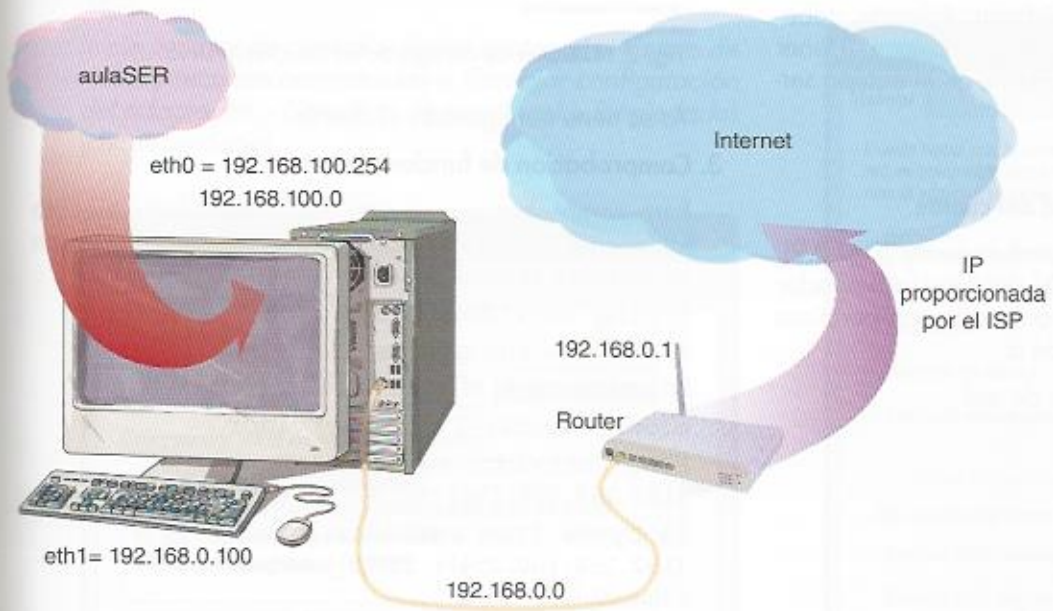


Fig. 2.8. *Estructura de la red aulaSER.com según el esquema 2.*

En los casos que se indique, se trabajará con el esquema 1, en el que cada grupo tiene dos servidores, uno Ubuntu y otro Windows 2008, y dos clientes. En este caso, dichos clientes estarán conectados a la tarjeta de red interna del servidor de grupo con IP del tipo 192.168.110.X para el grupo 1, 192.168.120.X para el grupo 2, etc.

Una forma básica de traducción de nombres a direcciones IP (y viceversa) es utilizando tablas de hosts. En GNU/Linux este archivo se llama `/etc/hosts` y su formato es una línea para cada máquina con su IP y nombres asignados (en ese orden), utilizando como separador el carácter espacio o el tabulador. El primer nombre es completo y los restantes son alias. El archivo `/etc/hosts` en Windows es idéntico al utilizado por GNU/Linux (con excepción del parámetro alias). Contiene el nodo IP y el nombre completo FQDN de la máquina a la que se refiere. Si se utilizan nombres NetBios con WINS, el archivo se llama `Lmhosts` y está en la carpeta `$WINDOWS\system32`.

A continuación entramos en la descripción del servicio DNS que sustituye este archivo, favoreciendo la administración de nombres y direcciones IP. Para ello se configurará un **servidor de DNS primario** en la red **192.168.100.0/24** en el ordenador llamado servidor.

Claves y consejos

Si se quiere cambiar el nombre del ordenador en GNU/Linux, hay que modificar el contenido del archivo `/etc/hostname` cambiando el nombre existente por el que se desee.

Para que el cambio tenga efecto inmediato se puede utilizar la orden `hostname`, pasándole como argumento el nuevo nombre. Hay que añadir dicho nombre en la línea de `/etc/hosts` correspondiente para poder resolverlo localmente.

Es importante reiniciar el sistema para que todos los servicios asuman el nuevo nombre.

Ejemplos

Archivo `/etc/resolv.conf`

```
search aulaSER.com
nameserver 192.168.100.254
127.0.0.1
```

CEO

En el CEO dispones del documento denominado *U02_SER_DNS_Caso_Practico_a.pdf*, que contiene el planteamiento y solución de la configuración del cliente DNS en modo texto.

2. Configuración del cliente DNS

CEO

En el CEO dispones del documento denominado *U02_SER_DNS_Ordenes_resolucion.pdf*, que contiene la descripción y uso de la orden `nslookup`, entre otras.

El cliente del servicio de DNS se llama **resolver.** Sus tareas son:

1. Interrogar al servidor de nombres.
2. Interpretar respuestas (que pueden ser registros RR o errores).
3. Devolver información al programa que la solicita.

Los archivos de configuración implicados para Ubuntu GNU/Linux son `/etc/resolv.conf` y `/etc/host.conf`.

Caso práctico 2

Configuración del cliente DNS en Ubuntu utilizando Webmin

Duración: 20 min **Dificultad:** fácil

Objetivo: configurar el cliente DNS en un ordenador del aula con la herramienta gráfica Webmin.

Condiciones previas: tener instalada en el cliente la herramienta de administración gráfica Webmin. Además, debemos conocer la IP del servidor y la puerta de enlace, y tener el servidor DNS configurado previamente en el equipo servidor de aula.

Desarrollo:

1. Entrar en la configuración de red del cliente

Para acceder a la configuración del cliente (Fig. 2.9), entra en **https://localhost:10000/** desde el navegador del equipo cliente, valídate como usuario con permisos de administrador (sudo) y accede a:

Webmin > Red > Configuración de red

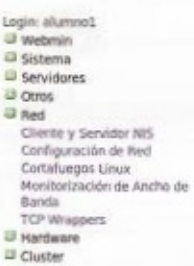


Fig. 2.9. *Acceso a la configuración del cliente DNS con Webmin.*

A continuación se abre una ventana, en la que debes seleccionar *Nombre de máquina y cliente DNS* (Fig. 2.10).

Fig. 2.10. *Acceso a la configuración de red.*

2. Indicar los datos del dominio aulaSER.com

Al entrar en esta opción (Fig. 2.11), indica el nombre del dominio de búsqueda, así como la IP del servidor DNS del aula (192.168.100.254).

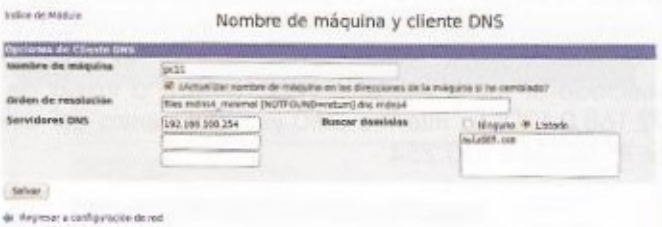


Fig. 2.11. *Datos de configuración del cliente DNS.*

Ya se tiene configurado el cliente.

3. Comprobación de funcionamiento

Para comprobar que se está resolviendo bien, ejecuta la orden `dig` sobre un dominio o simplemente la orden `ping` sobre el nombre del servidor DNS:

```
$ ping servidor.aulaSER.com
$ dig www.edu.gva.es
```

En ambos casos, el status debe ser NOERROR.

```
alumno1@pc11:~$ ping servidor
PING  servidor.aulaSER.com
(192.168.100.254)  56(84)  bytes of data.
64 bytes from servidor.local
(192.168.100.254): icmp _ seq=1 ttl=64
time=0.020 ms
--- servidor.aulaSER.com ping statistics ---
1 packets transmitted, 1 received, 0%
packet loss, time 0ms
rtt min/avg/max/mdev =
0.020/0.020/0.020/0.000 ms
```

Ejemplos

La orden `nslookup` permite resolver nombres desde el terminal en Ubuntu:

```
pc02@usuario1:~$ nslookup www.mcgraw-hill.es
Server: 62.42.63.52
Address: 62.42.63.52#53
Non-authoritative answer:
Name: www.mcgraw-hill.es
Address: 198.45.22.195
```

El Caso práctico 3 muestra el proceso de configuración del cliente DNS en Windows. No requiere Webmin, ya que la configuración por defecto es desde entorno gráfico y resulta muy sencilla.

Caso práctico 3

Configuración del cliente Windows

Duración: 5 min **Dificultad:** fácil

Objetivo general: configurar un equipo con Windows como cliente DNS.

Condiciones previas: los ordenadores tienen un nombre de host ya asignado.

Desarrollo:

1. Configuración de la conexión de red

Inicia sesión de Windows como Administrador y accede a:

Inicio > Panel de control > Redes e Internet > Centro de redes y recursos compartidos > Cambiar configuración del adaptador > Conexion de área local > Propiedades (clic secundario)

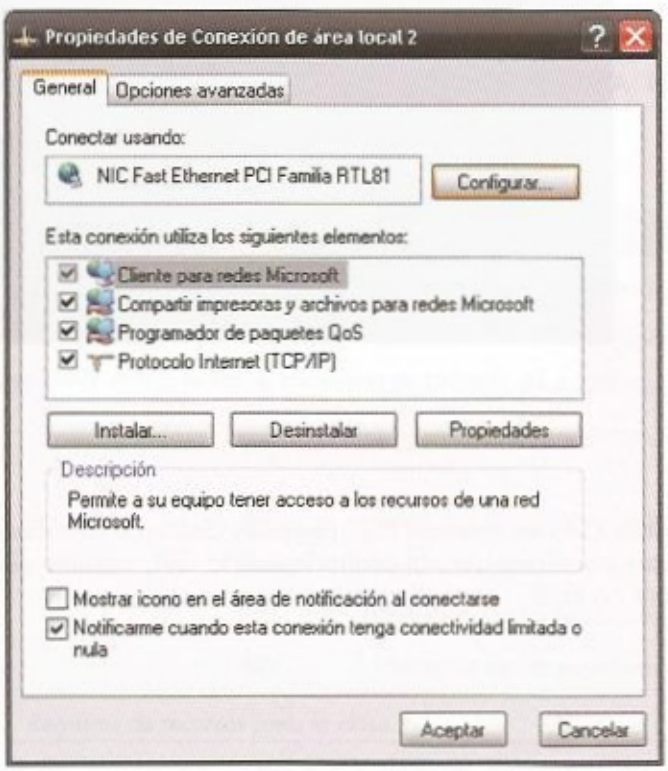


Fig. 2.12. *Propiedades de la opción Conexión de área local.*

Introduce los datos concretos del servidor DNS del aula. Si todavía no está configurado el servicio y los ordenadores salen a Internet directamente, habrá que modificar los datos y asignar los DNS del proveedor de Internet correspondiente y la puerta de enlace a la IP del router que permita el acceso.

A continuación, selecciona:

Protocolo Internet (TCP/IPv4) > Propiedades

En la ventana que aparece (Fig. 2.13), en la zona de DNS, asigna la dirección IP del servidor DNS primario. Incluye también la IP del cliente por si no se tiene configurado DHCP, así como la puerta de enlace, que es el propio servidor.

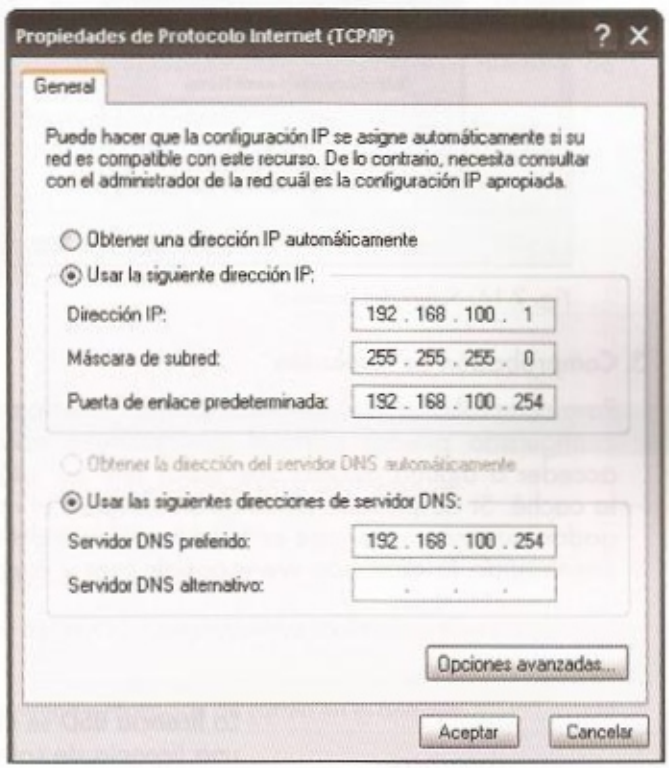


Fig. 2.13. *Propiedades de Protocolo Internet.*

2. Configuración del dominio en el cliente

Accede a *Opciones avanzadas > DNS*

Selecciona la opción *Anexar estos sufijos DNS (en este orden)*, haz clic sobre el botón *Agregar* y escribe el sufijo *aulaSER.com* (Fig. 2.14). Esta opción especifica los únicos sufijos de dominio que se van a añadir a los nombres de dominio no cualificados en el proceso de resolución de nombres.

(Continúa)

Caso práctico 3

(Continuación)

Desmarca la opción *Registrar estas direcciones de conexiones en DNS.*

Fig. 2.14. *Sufijo del dominio.*

3. Comprobación de resolución

Para comprobar que el cliente DNS está correctamente configurado puedes abrir el navegador e intentar acceder a alguna página que sepas que no está en la caché. Si después de un tiempo de espera el navegador muestra un mensaje en la barra inferior del tipo *Resolviendo la dirección* **www.google.com** y a continuación muestra el contenido de la Figura 2.15, quiere decir que no está resolviendo bien y no puede acceder a dicha página.

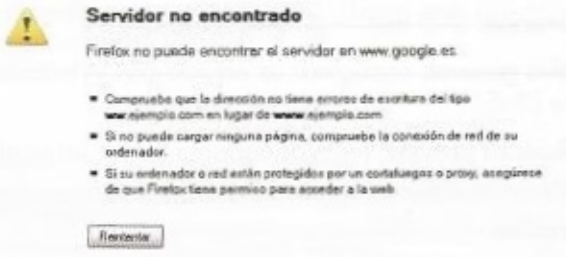


Fig. 2.15. *Fallo de resolución de nombres.*

Si todo va bien, nos mostrará información de la web solicitada.

Otra forma de comprobar la resolución es mediante la orden `nslookup` desde una consola lanzada con la orden `cmd` (Fig. 2.16).

Fig. 2.16. *Pruebas de resolución desde el cliente Windows.*

La **licencia BSD** se utiliza sobre todo en sistemas BSD *(Berkeley Software Distribution)*. Es una licencia de software libre permisiva que, al contrario que la GPL, permite el uso de su código fuente en software no libre.

Vocabulario

Resolución de nombres. Mecanismo por el que se traducen los nombres de máquinas, dados por los usuarios al conectarse a servidores remotos, a direcciones IP.

Actividades

13. ¿Existe archivo `/etc/resolv.conf` en el ordenador *pc11*? Comprueba qué líneas de configuración se han incluido.
14. ¿Cómo comprobarías los datos introducidos para el cliente DNS en la consola de Windows?
15. ¿Cómo comprobarías que el cliente resuelve correctamente desde la línea de orden? ¿Qué comando utilizarías?

3. Base de datos del protocolo DNS

Tal como se indicó en el Apartado 1.1, cada servidor de nombres de dominio mantiene una base de datos, llamada archivos de la zona, que sirve para asociar los nombres de dominio con direcciones IP, y una base de datos de resolución inversa de la zona. El formato de estas bases de datos son archivos de texto.

Para resolver nombres los servidores DNS consultan las zonas, que contienen **registros de recursos (RR),** que describen la información del dominio DNS. Por ejemplo, hay registros de recursos que asignan nombres descriptivos a direcciones IP.

Cada registro de recursos tiene este formato:

Propietario TTL Clase Tipo RDATA

La descripción de los campos de los registros de recursos (RR) es la siguiente:

- **Propietario:** nombre de máquina o dominio DNS al que pertenece el recurso. Puede contener el símbolo @, que representa el nombre de la zona descrita.
- **TTL (Time To Live):** tiempo de vida, en segundos, del registro en la caché. Es un campo opcional y se expresa en días (d), horas (h), minutos (m) y segundos (s). El cero (0) no se almacena en caché.
- **Clase:** familia de protocolos en uso. Suele tomar el valor «IN» de Internet, que representa una red TCP/IP.
- **Tipo:** varía en función del campo *Clase*. En la Tabla 2.2 se indican tipos de registros para la clase IN.
- **RDATA:** información específica del tipo de recurso. Por ejemplo, para un registro de clase IN y tipo A este campo especifica una dirección IP.

Los principales **tipos** de registros de recursos RR son: **SOA, NS, A, PTR, CNAME, MX** y **SRV** (Tabla 2.2).

CEO

En el CEO dispones del documento *U02_SER_DNS_Registros_Recursos.pdf*, que contiene una descripción detallada de los registros de recursos.

Ejemplos

Registro SOA del modelo de aula:

```
aulaSER.com. IN SOA servidor.aulaSER.com.
(2009051701; número de serie
10800; actualización
3600; reintentos
604800; caducidad
86400; valor TTL
)
```

Nombre de recurso	Tipo de registro	Función
Inicio de autoridad	**SOA**	Identifica al servidor autoritario de una zona y sus parámetros de configuración.
Servidor de nombres	**NS**	Identifica servidores de nombres autorizados para una zona.
Dirección	**A**	Asocia un nombre de dominio FQDN con una dirección IP.
Puntero	**PTR**	Asigna una dirección IP a un nombre de dominio completamente cualificado. Para las búsquedas inversas.
Registro de correo	**MX**	Indica máquinas encargadas de la entrega y recepción de correo en el dominio.
Nombre canónico	**CNAME**	Permite asignar uno o más nombres a una máquina.
Text	**TXT**	Almacena cualquier información.
Servicio	**SRV**	Ubicación de los servidores para un servicio.

Tabla 2.2. *Registros de recursos para la clase IN.*

En el ejemplo, los valores están dados en segundos, aunque también se pueden utilizar letras para representar a las unidades de tiempo. Por ejemplo, para especificar un intervalo de tiempo de una semana (Week), dos días (Day), cinco horas (Hour) y diez minutos (Minute) se escribe 1W2D5H10M. Según el ejemplo anterior, y haciendo las correspondientes transformaciones en las cantidades dadas, el registro SOA se escribe de la forma:

```
aulaSER.com. IN SOA servidor.aulaSER.com. (2009051701 3H 1H 1W 1D)
```

4. Servidores de nombres de dominio

Existen varias aplicaciones de servidores de nombres de dominio. La más conocida y utilizada en Internet es **BIND** con licencia **BSD.**

La ejecución de un servidor DNS en una máquina implica la ejecución en el sistema del proceso **named,** cuyo archivo de configuración es `/etc/bind/named.conf`. Este archivo es el lugar donde se le dice a BIND qué hacer, dónde y cómo.

La primera línea del archivo es una declaración include, que incluye el archivo `named.conf.options`, donde se encuentran las opciones globales del servidor. La última línea del archivo vuelve a ser otra declaración include, esta vez del archivo `named.conf.local`, que es donde se definen las zonas locales.

Las principales sentencias del archivo `named.conf.options` son:

- `acl`: define listas de direcciones IP para permitir o denegar el acceso al servidor de nombres. La sintaxis sería la que se muestra en el ejemplo siguiente:

Queremos definir la lista de control de acceso *redes* que incluya todas las máquinas de las redes 192.168.100.0/24 y 192.168.0.0/16, y la máquina independiente 192.168.110.5. Para ello, especificaremos:

```
acl redes { { 192.168.100/24; 192.168/16; 192.168.110.5; } };
```

  Por defecto, existen tres `acl` predefinidas:
  - **`any/none`:** acceso permitido/denegado a todas las máquinas.
  - **`localhost`:** acceso permitido solo a las direcciones IP locales.
- **`options`:** controla las opciones de configuración del servidor y de otras sentencias. Solo debe aparecer una vez en el archivo de configuración. En `options` se pueden encontrar declaraciones *directory, allow-query, blackhole, forwarders* y otras. Algunos ejemplos de uso de estas declaraciones son los siguientes:

  `options { directory /var/cache/bind; };`

  Muestra el directorio que almacenará archivos temporales generados por `named`.

  `allow-query {192.168.110/24;};`

  Indica que se permiten las consultas de todos las máquinas con direcciones que comiencen por 192.168.110.

  `blackhole { redes;};`

  Advierte que no se responda a ninguna consulta de las máquinas de `acl` 'redes'.

  `forwarders { 192.144.104.4; };`

  Señala que las peticiones de resolución no solucionadas en el servidor DNS local se reenvíen al servidor 192.144.104.4. Es necesario incluir esta opción para que los ordenadores de la red local salgan a Internet.

Las principales sentencias del archivo `named.conf` son:

- **`zone`:** define las zonas y describe sus configuraciones. Existen cuatro tipos de zonas:
  - **Zona maestra** (master zone): aquí el servidor tiene la copia principal de los datos de la zona.
  - **Zona esclava** (slave zone): contiene datos que se obtienen como resultado de la duplicación de la información de una zona maestra.
  - **Zona oculta** (hint zone): cuando se hacen peticiones a una zona que no se conoce, ofrece información relativa a servidores del dominio raíz.
  - **Zona de reenvío** (forward zone): indica al servidor de nombres que redirija las peticiones de información sobre la zona hacia otros servidores.
- **`include`:** se utiliza para incluir archivos que contienen las opciones y las zonas locales. Su sintaxis es:

```
include "/etc/bind/named.conf.local";
```

Vocabulario

BIND. Berkeley Internet Name Domain **http://www.isc.org/products/BIND/.**

BSD. Berkeley Software Distribution.

www.opensource.org/licenses/bsd-license.php.

Ejemplos

Si nuestro proveedor de Internet (ISP) es ONO, sus servidores DNS son: 62.42.230.24 y 62.42.63.52. Habría que indicar:

```
options {
  forwarders {
      62.42.63.52;
      62.42.230.24; };
};
```

CEO

En el CEO dispones de dos archivos relacionados con la materia.

El documento *U02_SER_DNS_Busquedas.pdf* contiene una descripción de los dos tipos de búsquedas más importantes.

El documento *U02_SER_DNS_Ordenes_resolucion.pdf* contiene una descripción de las órdenes mas utilizadas en la resolución de nombres.

¿Sabías que...?

Se pueden consultar más sentencias en la página de manual correspondiente (`$ man named.conf`).

Importante

El servidor BIND 9 incluye dos herramientas software, **named-checkzone** y **named-checkconf,** que permiten comprobar la sintaxis y semántica de los archivos que describen las zonas y el archivo de configuración `named.conf`.

Comprobamos la sintaxis del archivo `named.conf` ejecutando como administrador:

```
$sudo named-checkconf
```

La salida generada indica los errores que detecta. Si no genera salida, todo está correcto.

En el caso de los archivos de zona, hay que ejecutar:

```
$sudo named-checkzone aulaSER.com /etc/bind/db.aulaSER.com
```

A continuación, la interfaz muestra la siguiente salida:

```
zone aulaSER.com/IN: loaded serial 1
```

4.1. Resolución inversa

El servicio DNS es capaz de realizar la resolución en los dos sentidos. Es decir, dado un nombre de máquina, puede obtener su dirección IP correspondiente y, dada una dirección IP, es capaz de obtener el nombre de la máquina.

De la misma forma que los nombres de dominio se resuelven efectuando consultas para cada componente de derecha a izquierda, y el punto final indica el dominio raíz, las direcciones IP siguen el mismo esquema, y su dominio raíz se llama **in-addr.arpa.**

Por ejemplo, tenemos la dirección IP (192.168.100.1) de un ordenador. El servidor de nombres buscará los servidores *arpa.*, luego los servidores *in-addr.arpa.*, los *192.in-addr.arpa.*, los *168.192.in-addr.arpa.* y, por último, los servidores *100.168.192.in-addr.arpa.* En este último encontrará el registro buscado: *1.100.168.192.in-addr.arpa.*

Por tanto, las direcciones IP están escritas en orden inverso en el dominio **in-addr.arpa.**, es decir, utilizan una notación de puntos invertida.

Fig. 2.17. *Búsqueda inversa.*

El registro de recurso (RR) que define la resolución inversa se llama registro PTR (véase Tabla 2.2). Por ejemplo, para el caso anterior en el archivo `/etc/named.conf.local` debe existir la declaración de la zona correspondiente al dominio de *in-addr.arpa*, que sería *100.168.192.in-addr.arpa:*

```
zone "100.168.192.in-addr.arpa" {
type master;
file "/etc/bind/db.192.168.100"; };
```

En `/etc/bind/db.192.168.100` están todos los registros PTR definidos para esa red:

```
$ttl 38400
0.100.168.192.in-addr.arpa. IN SOA servidor.aulaSER.com. ser-admin.
aulaSER.com. ( 1242760444  10800  ..... )
0.100.168.192.in-addr.arpa.     IN NS servidor.aulaSER.com.
254.100.168.192.in-addr.arpa.   IN PTR servidor.aulaSER.com.
1.100.168.192.in-addr.arpa.     IN PTR pc11.aulaSER.com.
2.100.168.192.in-addr.arpa.     IN PTR pc12.aulaSER.com.
3.100.168.192.in-addr.arpa.     IN PTR pc13.aulaSER.com.
```

Para comprobar la resolución inversa, se ejecuta la orden `host` o `dig` con el parámetro -x:

```
# host 192.168.100.254
254.100.168.192.in-addr.arpa domain name pointer servidor.aulaSER.com.
```

Importante

¿Cómo se resuelve un nombre?

El usuario hace una petición de una URL desde su navegador, y el cliente DNS (resolvedor) lanza la siguiente consulta a un servidor DNS local:

Vocabulario

Resolución inversa. Es el proceso por el cual, dada una dirección IP, se obtiene el nombre de un dominio. Es utilizada por algunas aplicaciones para comprobar la identidad del cliente, sobre todo por temas de seguridad.

¿Sabías que...?

El número de serie no tiene por qué ser la fecha necesariamente. Puede ser cualquier número secuencial que vaya cambiando en el servidor primario a medida que se produzcan cambios en la base de datos de DNS. Así los servidores secundarios, al comparar su valor con este, saben que deben llevar a cabo una transferencia de zona.

CEO

En el CEO dispones del documento *U02_DNS_SER_Caso_Practico_b.pdf*, que contiene el planteamiento y solución de la configuración del servidor DNS en Ubuntu en modo texto.

5. Instalación y configuración del servicio DNS en un servidor GNU/Linux

Importante

La instalación de paquetes *.deb* se realiza desde el Centro de Software de Ubuntu, pero otra forma de instalar paquetes es desde una terminal, utilizando la forma `apt-get install`.

Para instalar el servicio DNS BIND 9 hay que abrir el Centro de Software de Ubuntu (Fig. 2.18), buscar BIND 9 y pulsar *Instalar*. Comprobamos que existe un paquete para la administración gráfica de DNS llamado Gadmin-Bind.

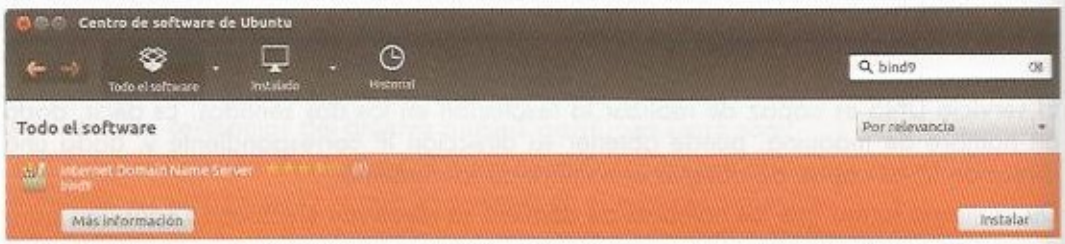


Fig. 2.18. *Instalación de BIND 9.*

El servicio DNS está compuesto por dos programas:

- El demonio **named:** este servidor de nombres de dominio contiene la base de datos con información relativa a un segmento de la red y responde a las peticiones.
- El **resolver** (cliente): genera las peticiones. Es un conjunto de rutinas que permiten que los clientes accedan a los servidores de nombres para resolver la búsqueda de una dirección IP asociada a un nombre.

En el directorio `/etc/bind/` se encuentra `named.conf`, y también el resto de archivos de configuración relacionados con BIND, como los archivos de datos de las zonas para los servidores raíz y las zonas de traducción de direcciones y de traducción inversa para localhost.

El archivo `named.conf` no se suele modificar. Las zonas específicas del servidor DNS que se configuran se definen en `/etc/bin/named.conf.local` y se incluyen al final de este archivo con un `include`.

El directorio de trabajo de named es `/var/cache/bind/`. Para lanzar el servicio, debemos ejecutar la orden siguiente, tras lo cual se lanza el proceso demonio named:

```
# /etc/init.d/Bind9 start
```

¿Sabías que...?

Los parámetros generales de configuración del servicio se pueden establecer de forma genérica mediante la opción de Wembin *Valores por defecto de zona.*

De esa forma no se tendrán que modificar en cada acción, si varían respecto a los valores por defecto, por ejemplo, los tiempos del registro SOA, utilización de plantillas, nombre del servidor, dirección de correo, etc.

Caso práctico 4

Instalación y configuración de un servidor DNS en Ubuntu GNU/Linux utilizando Webmin

Duración: 30 min **Dificultad:** media

Objetivo: instalar y configurar el servicio DNS en Ubuntu GNU/Linux utilizando la herramienta gráfica Webmin.

Consideraciones: el proceso se realiza sobre el servidor de aula llamado *servidor* con IP 192.168.100.254. Como práctica para reproducir los mismos pasos, se puede realizar en el servidor Ubuntu que hay en cada una de las filas según el esquema 2 del aula. Lógicamente, los valores de IP deberían adaptarse.

Desarrollo:

1. **Acceso a la interfaz de configuración del servidor DNS**

   Accede mediante el navegador a **https://localhost:10000.** Webmin mostrará la pantalla de conexión y podrás validarte con el usuario y contraseña establecidos en la instalación.

(Continúa)

Actividades

16. ¿Cómo comprobarías que el servicio DNS está funcionando correctamente?
17. Averigua el PID que tiene asignado el proceso named.
18. En ocasiones ocurre que al intentar resolver con *servidor* no hay éxito, y sí con *servidor.aulaSER.com*. ¿Por qué crees que puede suceder esto?

Caso práctico 4

(Continuación)

Al abrir Webmin es posible que ocasionalmente muestre un mensaje de problema relacionado con módulos. La propia herramienta da la opción de resolver el problema actualizando el módulo correspondiente. Por ejemplo, el módulo *File Manager*. La interfaz de trabajo dispone de un botón de *Refresco de módulos*.

Cuando se accede a Webmin, en la zona de servidores aparece la entrada *Servidor de DNS BIND*. Al pulsar sobre ella se mostrará la interfaz de configuración del servicio (Fig. 2.19).

Fig. 2.19. *Interfaz de administración del servicio DNS con Webmin.*

En primer lugar, configura la zona *aulaSER.com*. El archivo en el que se define la zona es `/etc/bind/named.conf.local`. Asociado a la zona está el archivo `/etc/bind/db.aulaSER.com`, que incluye los datos específicos para la zona definida. Para crear la zona, accede en Webmin a:

Zona DNS existentes > Crear una nueva zona maestra

2. Creación de la zona maestra

Introducir los datos de la zona según se han ido describiendo en apartados anteriores. Queda como indica la Fig. 2.20:

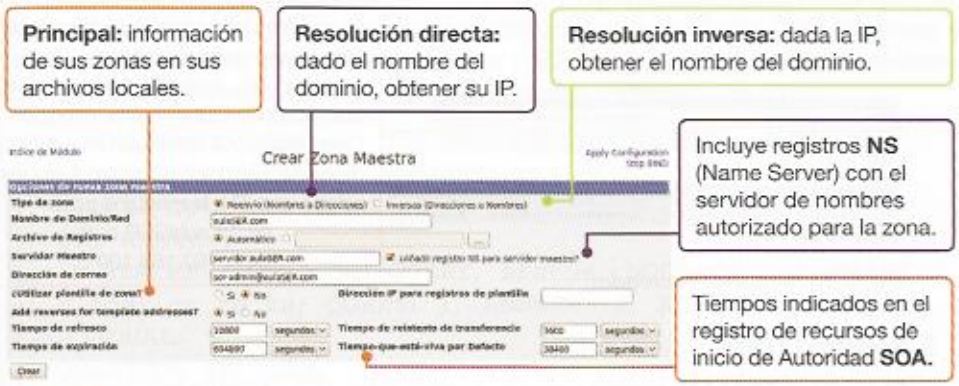


Fig. 2.20. *Creación de la zona maestra.*

En el archivo `/etc/bind/named.conf.local` se ha incluido el siguiente código:

```
zone "aulaSER.com" {
    type master;
    file "/var/lib/bind/aulaSER.
com.hosts";
    };
```

Se ha creado un nuevo archivo `aulaSER.com.hosts`, cuyo contenido son datos de la zona definida y que habrá que completar.

Ya creada la zona maestra, Webmin muestra su ventana de configuración (Fig. 2.21).

Fig. 2.21. *Opciones disponibles de configuración de la zona maestra.*

(Continúa)

¿Sabías que...?

En Ubuntu, el archivo `bind.keys` se utiliza cuando se implementa DNS seguro (`dnssec`). Mediante claves criptográficas, garantiza que los servidores son los que están autorizados, y no otros que intentan suplantarlos al hacer las consultas.

Importante

Para crear una nueva zona se debe utilizar el archivo de configuración `named.cof.local` indicando el nombre de la zona, su tipo y el archivo de zona.

Caso práctico 4

(Continuación)

3. Registro NS

El registro de recurso NS (servidor de nombres) establece los servidores de nombres autorizados para la zona. Cada zona debe contener registros, indicando tanto los servidores primarios como los secundarios. Por tanto, cada zona debe contener, como mínimo, un registro NS.

Además, dado que estos registros también se utilizan para indicar quiénes son los servidores de nombres con autoridad en los subdominios delegados, la zona ha de incluir, al menos, un registro NS por cada subdominio que haya delegado.

Pulsa en el icono *Servidor de Nombres;* se mostrará lo siguiente (Fig. 2.22):

Fig. 2.22. *Contenido del registro NS.*

4. Registros de dirección A

Accede a la opción de configuración de los registros de direcciones Dirección (0). Añade, a modo de ejemplo, registros de dirección para el dominio, el propio ordenador que hace de servidor DNS y para cuatro ordenadores del aula (Fig. 1.23).

Fig. 2.23. *Registros A creados.*

5. Registro CNAME

El registro CNAME permite que un ordenador sea identificado por uno o más nombres de host. Debe existir primero un registro de dirección (A) llamado nombre canónico u oficial. Por ejemplo, se quiere identificar el ordenador servidor por otros nombres. Ya se tiene el registro A correspondiente. Ahora, con esta opción de Webmin se crean alias (Fig. 2.24).

Fig. 2.24. *Registros CNAME.*

(Continúa)

¿Sabías que...?

Por medio del registro CNAME www hacemos posible escribir navegador desde el navegador **www.aulaSER.com** en lugar de **servidor.aulaSER.com.**

Caso práctico 4

(Continuación)

El archivo de configuración `aulaSER.com.hosts` debe quedar de la forma siguiente:

```
$ttl 38400
aulaSER.com. IN SOA servidor.aulaSER.com. ser-admin.aulaSER.
com. (
        1242759044
              10800
              3600
              604800
              38400 )
aulaSER.com.          IN    NS     servidor.aulaSER.com.
aulaSER.com.          IN    A      192.168.100.254
servidor              IN    A      192.168.100.254
pc11.aulaSER.com.     IN    A      192.168.100.1
pc12.aulaSER.com.     IN    A      192.168.100.2
pc13.aulaSER.com.     IN    A      192.168.100.3
pc14.aulaSER.com.     IN    A      192.168.100.4
www                   IN    CNAME  servidor
ftp                   IN    CNAME  servidor
mail                  IN    CNAME  servidor
```

Los registros CNAME indican que, por ejemplo, www puede ser utilizado como alias de servidor, o lo que es lo mismo, **aulaSER.com.**

Ahora puedes comprobar si el servidor DNS atiende peticiones de resolución tomando como cliente el propio ordenador. Hay que tener en cuenta que, en la configuración de red, se deben desactivar otros servidores DNS externos y dejar solo el que se acaba de configurar (192.168.100.254) junto con el dominio de búsqueda aulaSER.com. Ejecuta la orden `nslookup` o `dig`:

```
ser-admin@servidor:~$  dig www.edu.gva.es
; <<>> DiG 9.8.1-P1 <<>> www.edu.gva.es
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43689
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0,
ADDITIONAL: 0
;; QUESTION SECTION:
;www.edu.gva.es.                    IN    A
;; ANSWER SECTION:
www.edu.gva.es.       5     IN    A     193.144.125.18
www.edu.gva.es.       5     IN    A     195.77.17.148
;; Query time: 30 msec
;; SERVER: 62.42.63.52#53(62.42.63.52)
;; WHEN: Wed Jul  4 17:24:04 2012
;; MSG SIZE  rcvd: 64
```

Comprueba que en la salida aparece el status NOERROR, indicando que está resolviendo.

6. Registro PTR

A la hora de configurar de la resolución inversa hay que crear, en primer lugar, una zona de resolución inversa. En *Crear zona maestra* activa el tipo de zona inversa e introduce los datos de la red y el dominio (Fig. 2.25).

(Continúa)

CEO

En el CEO dispones del documento denominado *U02_SER_DNS_Registros_Recursos.pdf*, que contiene la descripción de los registros de recursos disponibles.

También dispones del documento denominado *U02_SER_DNS_Servidor_Autoritario.pdf*, que ofrece la definición detallada de este concepto.

¿Sabías que...?

Para hacer las pruebas y comprobar que se resuelve dentro del aula, puede ser importante desconectar la segunda tarjeta de red del equipo servidor de aula.

Caso práctico 4

(Continuación)

Fig. 2.25. *Creación de la zona maestra para la resolución inversa.*

La interpretación de los valores es similar que en la Figura 2.20, salvo que en este caso se ha seleccionado *Tipo de zona > Inversas* (de direcciones a nombres).

Fig. 2.26. *Registros PTR creados para la resolución inversa.*

Comprueba que en el archivo de configuración que contiene las zonas definidas (`/etc/bind/named.conf.local`) se ha añadido el código siguiente:

```
zone "0.100.168.192.in-addr.arpa" {
type master;
file "/var/lib/bind/192.168.100.0.rev";
};
```

La interfaz de Webmin muestra ahora las opciones de edición de la nueva zona maestra creada para la resolución inversa.

Ya puedes crear los registros de recurso PTR definidos para esa red. Ir a *Dirección inversa* y dar de alta registros PTR para el servidor y un grupo de cuatro ordenadores del aula.

Comprueba que se ha generado un archivo de configuración `/var/lib/bind/192.168.100.0.rev` para la resolución inversa. Debe contener los siguientes registros de recursos PTR:

```
$ttl 38400
0.100.168.192.in-addr.arpa. IN SOA servidor.aulaSER.com. ser-
admin.aulaSER.com. (
                1242760444
                     10800
                  3600
                  604800
                    38400 )
```

(Continúa)

Importante

Se puede comprobar en cualquier momento cómo se van introduciendo los diferentes registros de recursos en el archivo de configuración, accediendo a la opción *Edición de archivos de configuración* de Webmin para cada zona.

Caso práctico 4

(Continuación)

```
0.100.168.192.in-addr.arpa.   IN   NS    servidor.aulaSER.com.
254.100.168.192.in-addr.arpa. IN   PTR   servidor.aulaSER.com.
1.100.168.192.in-addr.arpa.   IN   PTR   pc11.aulaSER.com.
2.100.168.192.in-addr.arpa.   IN   PTR   pc12.aulaSER.com.
3.100.168.192.in-addr.arpa.   IN   PTR   pc13.aulaSER.com.
```

7. Registro de recurso MX (Mail eXchange)

El **registro de recurso MX** (intercambio de correo) es un registro de correo e indica una o varias máquinas encargadas de la entrega de correo en el dominio. Si el dominio tiene varias máquinas como registros MX, se puede señalar, mediante un valor numérico, el orden de preferencia de máquina que seguirá el servidor que envía el correo para hacer su entrega.

El ejemplo siguiente define la máquina *mail.aulaSER.com* como el servidor de correo del dominio *aulaSER.com*:

```
aulaSER.com.  IN  MX 10 mail.aulaSER.com.
```

El «0» está indicando que la máquina *mail.aulaSER.com* es la primera a contactar.

La configuración en Webmin es la siguiente (Fig. 2.27):

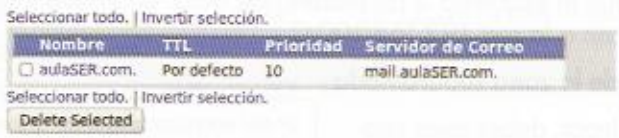


Fig. 2.27. *Registro MX creado para el servidor de correo.*

Una vez finalizada la configuración, se pueden ver todos los registros generados a través de la opción *Todo Registros* en una zona determinada. En nuestro caso, si te sitúas en la zona **aulaSER.com,** verás lo siguiente (Fig. 2.28):

Fig. 2.28. *Todos los registros creados.*

8. Comprobación de servicio DNS activo

Para comprobar que el servicio DNS está activo y escuchando peticiones de resolución de nombres, ejecuta esta orden:

```
$sudo netstat -atunp |grep 53
```

Comprueba si existe una entrada para el puerto 53 con el atributo ESCUCHAR.

La orden `netstat` permite conocer para una máquina dada qué servicios en general están activos y cuáles son los puertos de escucha de cada uno de ellos.

¿Sabías que...?

Se puede utilizar la opción *Generadores de registro* cuando se quieren dar de alta un número elevado de registros; de este modo no hay que hacerlo uno a uno.

A menor número, mayor prioridad en la recepción de correo.

Vocabulario

Servidor DNS secundario. Obtiene la información de sus zonas de otro servidor de nombres (generalmente, un servidor primario) que tiene autoridad sobre esas zonas. El servidor secundario contiene una copia de solo lectura de los archivos de zona.

6. Configuración de un servidor DNS secundario en Ubuntu GNU/Linux

Actividades

19. ¿Qué diferencia existe entre la transferencia de zona completa y la transferencia incremental?

Los servidores secundarios son necesarios por dos razones. En primer lugar, porque permiten descargar el tráfico de consultas DNS en redes en las que se consulta a menudo una zona. En segundo lugar, si el servidor primario o maestro está inactivo por algún motivo, el servidor secundario ofrecerá resolución de nombres en esa zona mientras el primario no esté disponible.

El servidor secundario debe estar físicamente en una máquina diferente y debidamente actualizado para ofrecer el servicio en condiciones. Es decir todos los cambios que se realizan en la zona del maestro deberán replicarse en el secundario de la zona a través de la transferencia de zona.

Caso práctico 5

Configuración de un servidor DNS secundario con Ubuntu GNU/Linux en el aula

- **Duración:** 20 min
- **Dificultad:** fácil

Objetivo: configurar la máquina del aula *pc11* como servidor DNS secundario dentro del dominio **aulaSER.com** con Ubuntu GNU/Linux.

Desarrollo:

Se transformará el equipo *pc11* en servidor secundario del servidor del aula (equipo profesor). Sigue el esquema 2 de modelo de aula, en el que todos los equipos del aula pertenecen a la red 192.168.100.0.

1. Creación de la zona subordinada

En primer lugar, debes crear una zona esclava alojada en el servidor de nombres secundario; su función será «redundar» la zona master del dominio primario.

Desde Webmin acceder a *Crear una nueva zona subordinada*.

Fig. 2.29. *Creación de la zona secundaria.*

En el archivo `/etc/bind/named.conf.local` del servidor, añade las líneas de la zona esclava y el servidor donde está alojada la zona maestra:

```
zone "aulaSER.com" {
type master;
file "/var/lib/bind/aulaSER.com.hosts";
masters { 192.168.100.254; };
};
zone "0.100.168.192.in-addr.arpa" {
type master;
file "/var/lib/bind/192.168.100.0.rev";
};
zone "pc11" {
    type slave;
    masters {
          192.168.100.254;
          };
    file "/var/lib/bind/pc11.hosts";
};
```

(Continúa)

CEO

En el CEO dispones del documento denominado *U02_SER_DNS_Busquedas.pdf*, que contiene la descripción de los métodos de búsquedas DNS.

Caso práctico 5

(Continuación)

Aparecerá una nueva zona en Webmin llamada *pc11* (Fig. 2.30).

Fig. 2.30. *Zona secundaria* pc11.

2. Registro NS de la zona secundaria

A continuación, incluye un registro NS en el servidor primario para la zona secundaria (Fig. 2.31).

Si editas el archivo `/var/lib/bind/aulaSER.com.hosts` del servidor primario, comprobarás que se ha incluido el registro NS y, por lo tanto, *pc11* es un servidor autorizado para **aulaSER.com:**

Fig. 2.31. *Registro NS para la nueva zona secundaria.*

Si editas el archivo `/var/lib/bind/aulaSER.com.hosts` del servidor primario, comprobarás que se ha incluido el registro NS y, por lo tanto, *pc11* es un servidor autorizado para **aulaSER.com:**

```
$ttl 38400
aulaSER.com. IN SOA servidor.aulaSER.com.  ser-admin.aulaSER.com.
( 1242759047  10800  3600  604800  38400 )
; registros de autoridad
aulaSER.com.          IN    NS     servidor.aulaSER.com.
aulaSER.com.          IN    NS     pc11.aulaSER.com.
;registro de correo
aulaSER.com.          IN    MX 10       mail.aulaSER.com.
;registros de dirección
aulaSER.com.          IN    A      192.168.100.254
servidor              IN    A      192.168.100.254
pc11.aulaSER.com.     IN    A      192.168.100.1
pc12.aulaSER.com.     IN    A      192.168.100.2
pc13.aulaSER.com.     IN    A      192.168.100.3
pc14.aulaSER.com.     IN    A      192.168.100.4
;registros de alias
www                   IN    CNAME servidor
ftp                   IN    CNAME servidor
mail                  IN    CNAME servidor
```

Si configuras la resolución inversa, debes añadir también este registro NS en el archivo `/etc/bind/db.192.168.100`.

3. Permitir las transferencias de zona desde este servidor

Para ello, comprueba la sentencia `allow-transfer` en el archivo `/etc/bind/named.conf.options`, y verifica que este nuevo servidor secundario está incluido en la lista. De esta forma, el servidor primario permitirá transferencias de zona desde el secundario.

Deberás añadir la siguiente línea en `/etc/bind/named.conf.options`:

```
allow-transfer  { 192.168.100.1; };
masters { 192.168.100.254; };
```

La transferencia se hará desde el servidor DNS primario.

Por último, relanza el servicio BIND para que reconozca las modificaciones:

```
$ sudo /etc/init.d/bind9 reload
```

¿Sabías que...?

DNSChanger es un virus que modifica la configuración DNS del equipo infectado.

Para comprobar si tu ordenador está infectado por el virus DNS Changer puedes hacerlo a través de la web **www.dns-changer.eu** o comprobando manualmente si los servidores DNS configurados en tu PC son maliciosos.

Para más información puedes vistar INTECO **(http://cert.inteco.es/Actualidad/Actualidad_Virus/DNSChanger/)** y la Oficina de Seguridad del Internauta **(https://www.facebook.com/osiseguridad).**

7. Configuración del servidor DNS con Windows 2008 Server

Web

En **http://www.youtube.com/watch?v=qrCszcfJtsw** dispones de un sencillo videotutorial que describe los pasos necesarios para la instalación de Active Directory en Windows 2008 Server.

Hasta la aparición de Windows 2000 se utilizaba WINS (Windows Internet Naming Service) como servicio de resolución de nombres. WINS es un servicio que convierte los nombres de máquina NetBIOS a direcciones IP. En la actualidad se utiliza el servicio DNS, aunque se mantiene la compatibilidad con WINS y, en ocasiones, se utilizan ambos conjuntamente.

En Windows 2008 se trabaja con el servicio DNS integrado en Active Directory. Las funciones que lleva a cabo dicho servicio son:

- Resolución de nombres, tanto directa como inversa, siguiendo el esquema de funcionamiento explicado al inicio de la unidad.
- Integración de los nombres de dominio asignados por Active Directory y los nombres de dominio de DNS. Ambos siguen la misma estructura jerárquica de nombres, aunque representan dos espacios de nombres distintos, ya que almacenan distinta información. Pero las máquinas y dominios DNS son los mismos que los de Active Directory.

Windows 2008 Server incorpora un asistente que facilita la configuración de un servidor DNS en una red, aunque se puede hacer también de forma manual.

En este apartado se va a configurar el servicio DNS desde Active Directory utilizando su asistente correspondiente.

Con la instalación de Active Directory tenemos ya definido el dominio raíz, que es **aulaSER.com**. y tenemos instalado un controlador de dominio local.

Al utilizar el asistente para la instalación de los servicios de dominio de Active Directory, no hay que seleccionar la opción adicional de Servidor DNS, aunque dé error de diagnóstico DNS. El asistente avisa de que se necesita la compatibilidad con el servidor DNS para que los servicios de dominio de Active Directory funcionen correctamente.

El servidor se configura como el primer controlador de dominio de Active Directory de un nuevo bosque. Tanto el dominio como el bosque se llaman **aulaSER.com,** el nombre de la máquina es *servidorWIN* y el nombre NetBIOS asignado es SERVIDOR_WIN.

Antes de instalar y configurar el servicio DNS, hay que revisar las conexiones de red. En nuestro caso, el servidor dispone de dos tarjetas de red. Es preferible que ambas tengan direcciones IP estáticas. Pero en nuestro caso dejaremos estática la interfaz de red que atiende peticiones dentro del aula para configurar como dinámica la que se conecta al router del aula, dentro de la red 192.168.0.0. El router será la puerta de enlace con la IP interna 192.168.0.100 (Figs. 2.32 y 2.33):

Panel de control > Centro de redes y recursos compartidos > Administrar conexiones de red

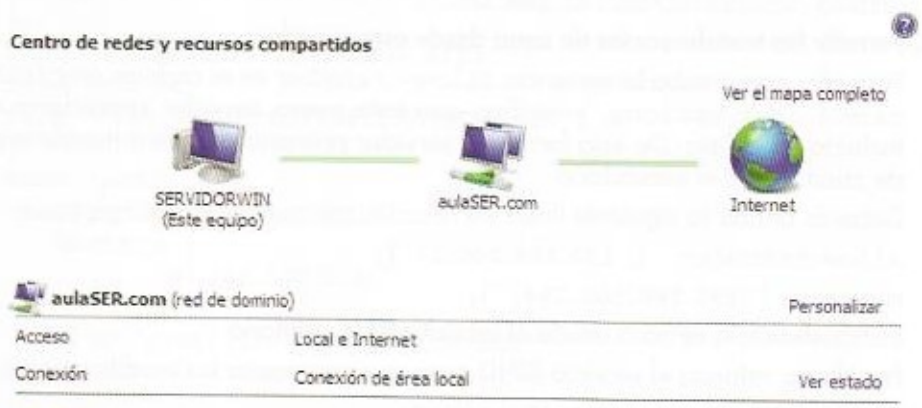


Fig. 2.32. *Conexiones de red del aula.*

Claves y consejos

Para hacer las pruebas dentro del aula se recomienda desactivar el servicio DHCP del router y asignar direcciones estáticas al equipo en el que se configura el servicio DNS.

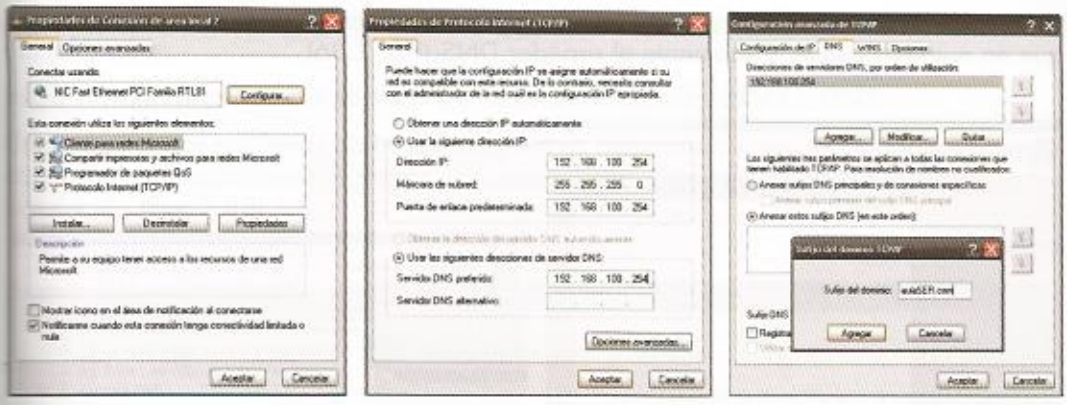


Fig. 2.33. *Acceso a la configuración de las propiedades de la conexión de red.*

Después, sobre el controlador de dominio aulaSER creado debe instalarse y configurarse el servidor DNS. A continuación se describen todos los pasos del proceso. Accedemos a *Inicio > Administración del servidor > Agregar funciones > Asistente para agregar funciones* (Fig. 2.34).

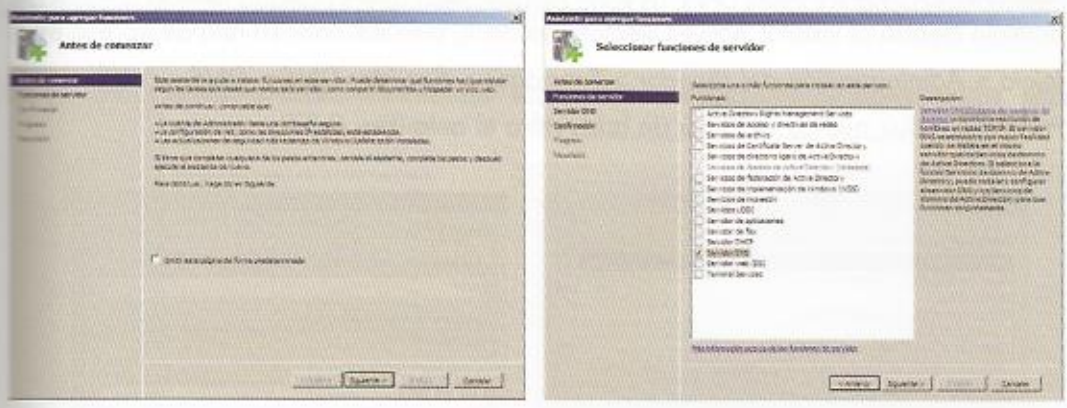


Fig. 2.34. *Asistente para agregar funciones de Windows 2008.*

Para instalar el servicio DNS conviene tener una IP estática, que en nuestro caso será la tarjeta de red que atiende al aula, con IP 192.168.100.254.

Seleccionaremos el Servidor DNS y comprobaremos que los servicios de dominio de Active Directory están ya instalados (Fig. 2.35).

Fig. 2.35. *Asistente para agregar funciones de Windows 2008.*

¿Sabias que...?

En Windows Server 2008 existen varios procedimientos para iniciar y detener el servicio DNS. Por ejemplo, desde la línea de orden *Inicio > Ejecutar >* `cmd` se puede utilizar la orden `NER opción DNS`, donde `opción` puede ser `START`, `STOP` o `RESTART`.

También desde la herramienta gráfica de administración de servicios:

Inicio > Herramientas administrativas > Servicios

Por último, usando la herramienta gráfica de administración y configuración de DNS desde *Inicio > Herramientas Administrativas > DNS.*

Importante

Al finalizar la instalación y activación del servicio DNS en Windows 2008 Server, se muestra un montaje de advertencia que indica que las actualizaciones automáticas no están disponibles.

Es importante no activar las actualizaciones automáticas, ya que estas podrían generar problemas y comprometer el servicio. Las actualizaciones deben hacerse siempre bajo nuestro control.

Continuaremos con la instalación y confirmaremos la selección de funciones realizada, que en nuestro caso es únicamente el servidor DNS (Fig. 2.36).

Fig. 2.36. *Finalización de la instalación del servicio DNS.*

Por último, comprobamos que la instalación se ha realizado correctamente.

Una vez instalado el servicio, hay que comprobar los registros de dirección creados, así como otras configuraciones DNS. La zona de búsqueda directa creada tiene el nombre del dominio creado al instalar Active Directory, es decir, aulaSER.com. La ruta de acceso es:

Inicio > Administración del servidor > Funciones > Servidor DNS > DNS

Podemos incluir nuevos registros de hosts para el aula (Fig. 2.37):

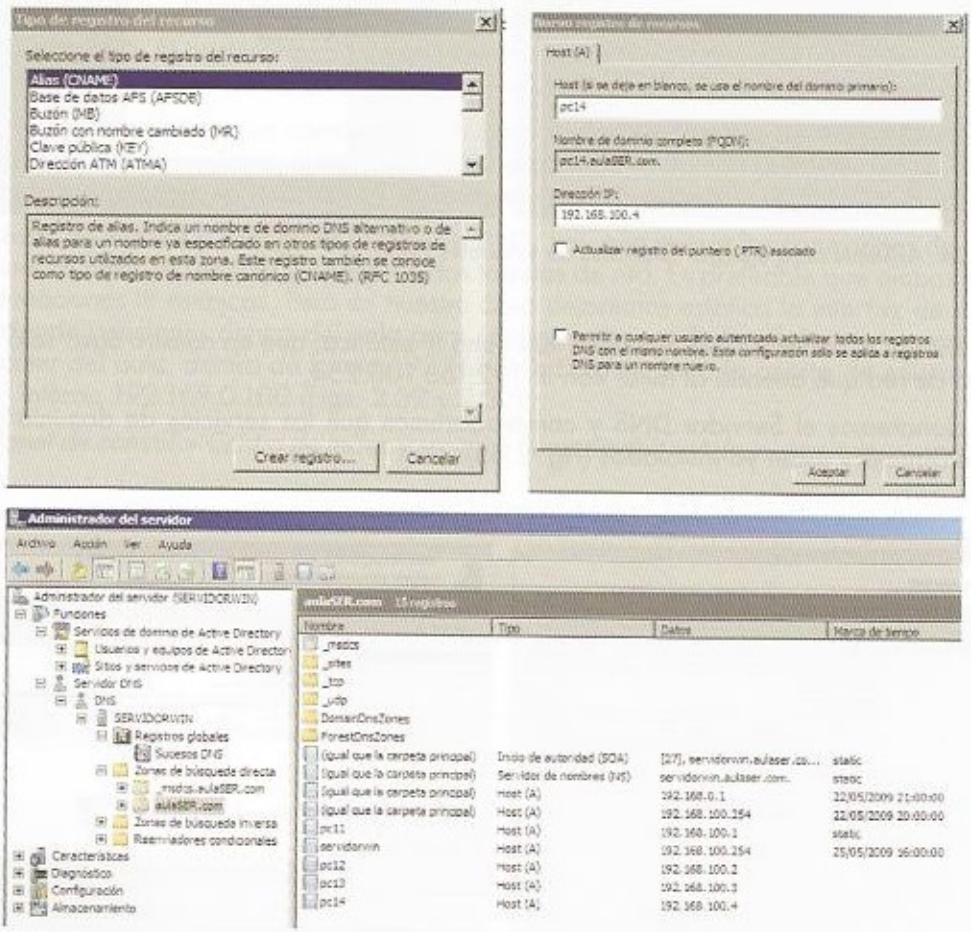


Fig. 2.37. *Creación de nuevos registros de hosts.*

¿Sabías que...?

Se puede comprobar la respuesta de un servidor DNS utilizando la orden `nslookup`. Para ello, desde un terminal de Windows escribiremos:

`nslookup IP:servidor`
`1237.0.0.1`

Si el servidor DNS resuelve, devolverá «`localhost`».

A continuación, creamos la zona de búsqueda inversa en el servidor DNS. Para ello accedemos a:

Inicio > Administración del servidor > Funciones > Servidor DNS > DNS

Una vez situados en *Zonas de búsqueda inversa*, hacemos clic secundario y, en el menú contextual, seleccionamos *Agregar una nueva zona*. Con ello, se lanza el asistente de instalación (Fig. 2.38).

Fig. 2.38. *Creación de una zona inversa.*

A continuación, se ejecuta el asistente para la creación de una zona inversa (Fig. 2.39):

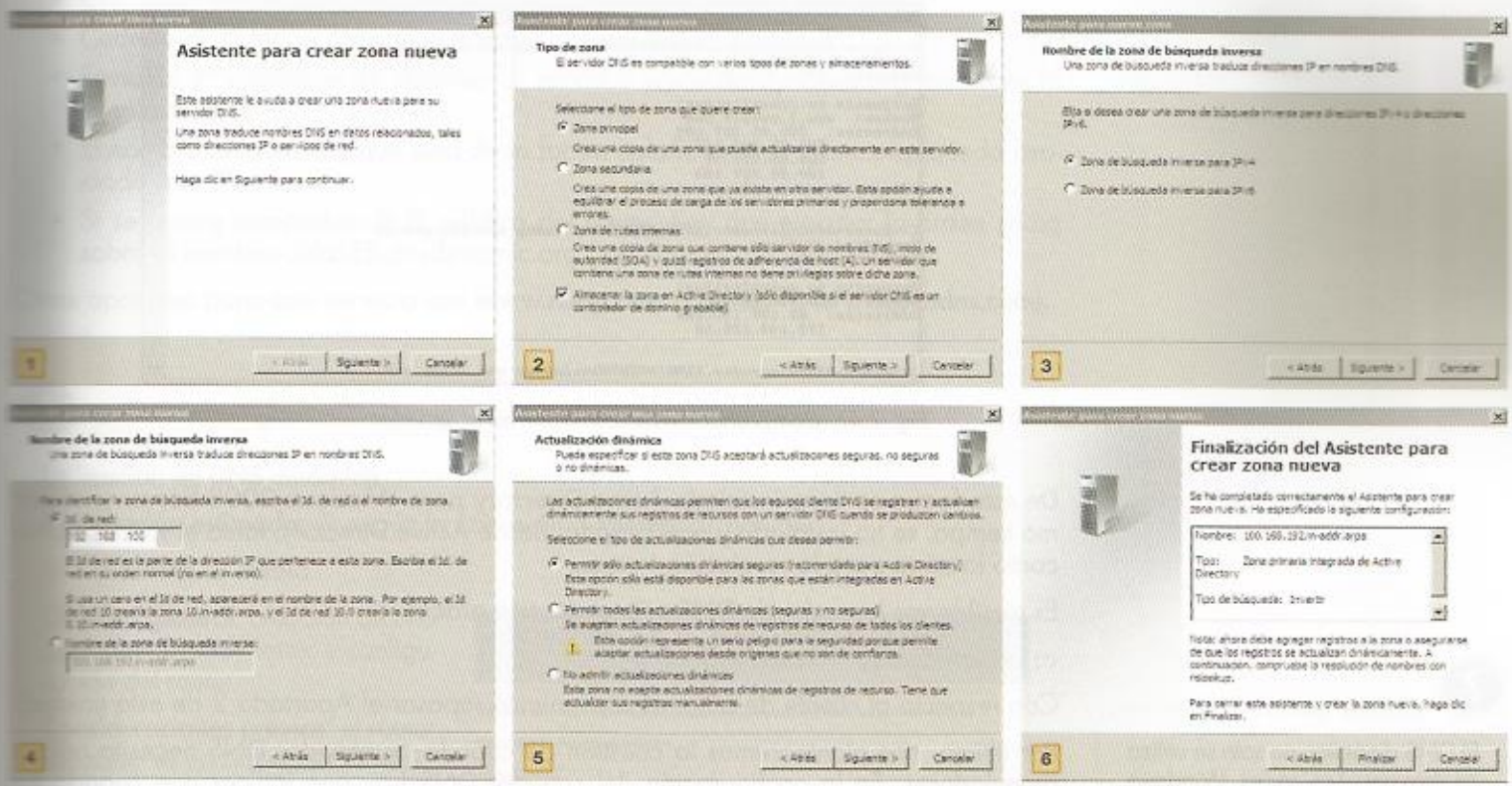


Fig. 2.39. *Asistente para la creación de una zona inversa.*

Ámbito de replicación de la zona de Active Directory: para todos los controladores de dominio en el dominio aulaSER.com de Active Directory.

Nombre de la zona de búsqueda inversa: introducir el ID de la red (192.168.100.).

Actualización dinámica: permitir solo actualizaciones dinámicas seguras (recomendado para Active Directory).

Vocabulario

Reenviador. Es un servidor DNS de una red que se utiliza para realizar consultas de nombres DNS externos a servidores DNS que se encuentran fuera de la red.

A continuación, comprobamos que la zona inversa ha sido creada (Fig. 2.40).

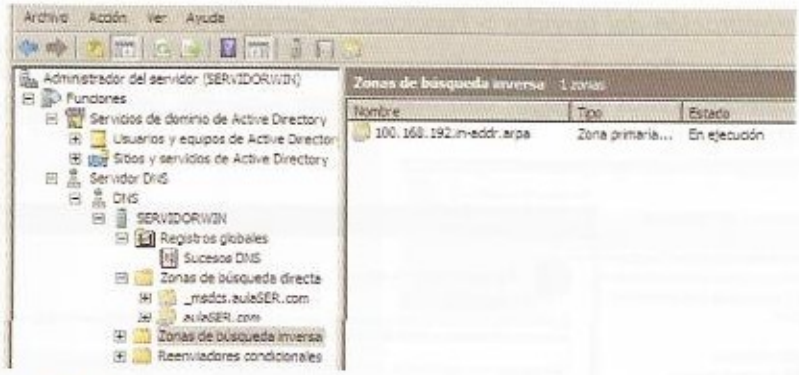


Fig. 2.40. *Comprobación de la zona inversa.*

Para comprobar que el servidor DNS esta funcionando, abriremos el navegador web Internet Explorer y, en la URL, escribiremos `\\servidor.aulaSER.com`. Aparecerá la información del servidor DNS.

Comprobamos que desde el servidor se resuelven los nombres ejecutando la orden `nslookup` (Fig. 2.41):

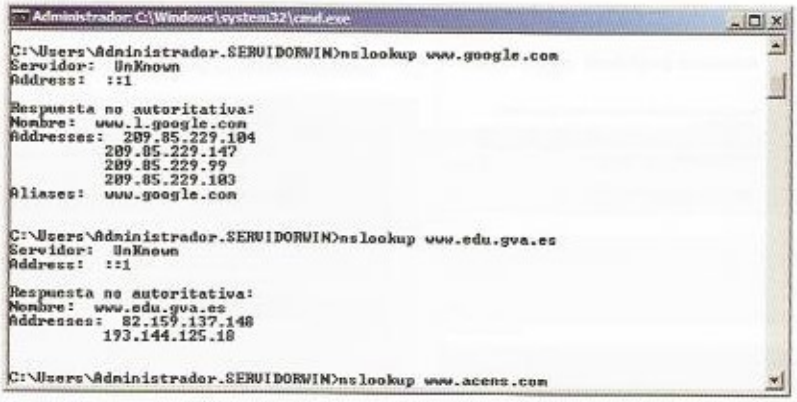


Fig. 2.41. *Comprobación de resolución en el servidor.*

De esta forma se tiene instalado Active Directory para Windows 2008 Server y, al mismo tiempo, se ha instalado y configurado, desde Active Directory, tanto el servidor DNS como la zona para la resolución inversa.

Es posible ver la caché de DNS utilizando esta orden:

```
c:\> ipconfig /displaydns
```

Con respecto al cliente de aula, es conveniente repasar el Apartado 2 de esta unidad.

Por último, nos plantearemos la cuestión de cuándo un servidor DNS necesita utilizar **reenviadores.** En la configuración del servidor DNS hay que indicar que cuando los ordenadores del aula intenten resolver URL que no pertenezcan a la red local y, por lo tanto, el servidor DNS no sea capaz de resolver, reenvía estas peticiones a otros servidores DNS públicos que puedan resolverlas.

Para ello, una vez situados sobre el nombre del servidor DNS *(SERVIDOR),* hacemos clic secundario y seleccionamos la opción *Propiedades.*

En la ventana que aparece a continuación, seleccionaremos la pestaña *Reenviadores* y, una vez allí, activaremos la casilla *Habilitar reenviador(es).* A continuación añadimos las IP de servidores DNS públicos.

¿Sabías que...?

El DNS dinámico no solo se utiliza en Internet. Las redes Windows con Active Directory integran este servicio, de forma que un equipo que arranca y recibe su IP por DHCP puede ser accedido mediante su nombre, a pesar de haber recibido una IP dinámica, una vez que se integra en un dominio Windows o grupo de trabajo.

8. DNS dinámico (DDNS)

Las siglas **DDNS** significan el **sistema dinámico de nombres de dominio,** que permite la asignación de un nombre de dominio a una máquina con dirección IP dinámica.

A menudo, el proveedor de Internet proporciona a nuestro ordenador una IP pública dinámica, es decir, que cambia de valor cada vez que nos conectamos. De esta forma se está impidiendo que nuestra máquina se transforme en un servidor DNS. Sin embargo, utilizando DNS dinámico es posible configurar un sitio web doméstico sin necesidad de utilizar un hosting externo a cambio de tener conectado nuestro servidor 24 horas al día. Es decir, si se quiere montar un servidor web, con FTP o servicios de escritorio remoto, se necesita que se pueda acceder desde Internet al router, para lo cual hay que configurar el router y asociarlo a una IP mediante un nombre de dominio.

Hay varios proveedores que ofrecen gratuitamente servicio DDNS. Uno de ellos es DNSdynamic. Para configurar un DDNS con él seguiremos estos pasos:

1. Activamos la opción DDNS en el router.

   La forma de acceso al router suele ser a través del navegador web y la IP interna del mismo. Es necesario validarse como usuario administrador en la interfaz del router e ir a las opciones de *Setup*, pestaña *DDNS*. La ubicación del servicio puede cambiar en cada tipo de router, por lo que es conveniente leer las instrucciones del mismo.

2. Creación de una cuenta DDNS en el servidor DNSdynamic:
   - Crear una cuenta en un servidor DDNS **(www.dnsdynamic.org).**
   - Cuando el router se conecta a Internet obtiene una dirección IP.
   - Envía su IP y nombre de dominio al servidor **www.dnsdynamic.org** mediante la cuenta creada.
   - El nombre de dominio, que será de la forma aulaSER.dnsdynamic.org, queda asociado a la IP.
   - Si se quiere comprobar la IP pública del router, hay que ejecutar la orden `ping` sobre el nombre aulaSER.dnsdynamic.org.

Otras opciones para este servicio son **www.no-ip.com** o DynDNS **(www.dyndns.com).**

Actividades

20. ¿En qué consiste la actualización dinámica de DNS?

Caso práctico 6

Utilización de DNS dinámica

- **Duración estimada:** ◷ según la conexión a Internet disponible
- **Dificultad:** 😐 media

Objetivo general: creación de una cuenta en DNSdynamic y configuración del router.

Consideraciones previas: el router utilizado es un Linksys WRT54G.

Desarrollo:

1. **Obtención de una cuenta en www.dnsdynamic.org**

   Entra en la web indicada y accede a la zona *Sign up* (Fig. 2.42):

Fig. 2.42. *Acceso al portal de DNSdynamic.*

(Continúa)

¿Sabías que...?

El servicio DNS dinámico va destinado a los usuarios con IP dinámica, es decir, a usuarios que no tienen IP estática o fija, y cambia cada vez que se conectan a Internet a través de su ISP.

Con DNS dinámica el usuario redirige su dominio a su IP, aunque no sea estática.

Caso práctico 6

(Continuación)

Introduce el nombre del dominio deseado para comprobar su disponibilidad (Fig. 2.43). A continuación, crea una cuenta introduciendo los datos requeridos y rellenando el campo *camptcha* (Fig. 2.44).

Fig. 2.43. *Disponibilidad del dominio aulaser.dnsdynamic.org.*

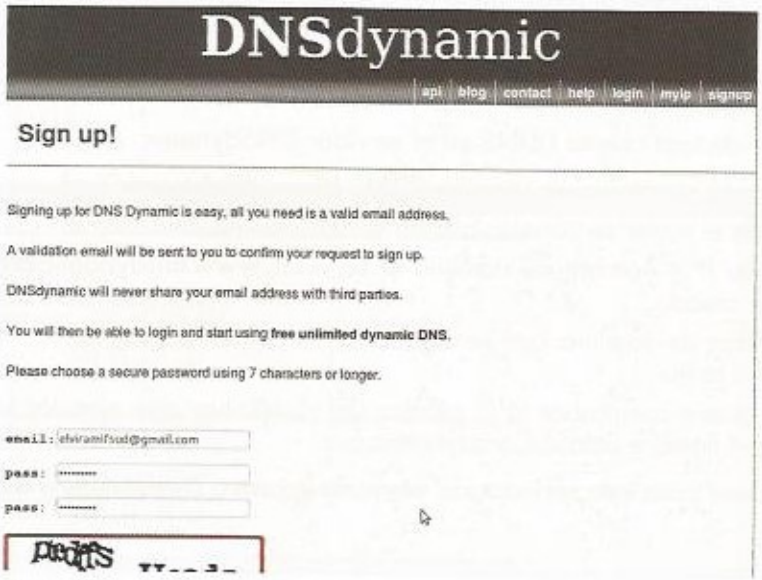


Fig. 2.44. *Creación de una cuenta en DNSdynamic.org.*

Recibirás un correo en la cuenta de correo dada que te avisará de que tu cuenta en DNSdynamic está activa. Accede a la dirección referida para validar la acción (Fig. 2.45).

Fig. 2.45. *Correo recibido.*

(Continúa)

Caso práctico 6

(Continuación)

A continuación, entra en esta cuenta; se te indicará cuál es la IP detectada para ese dominio (Fig. 2.46):

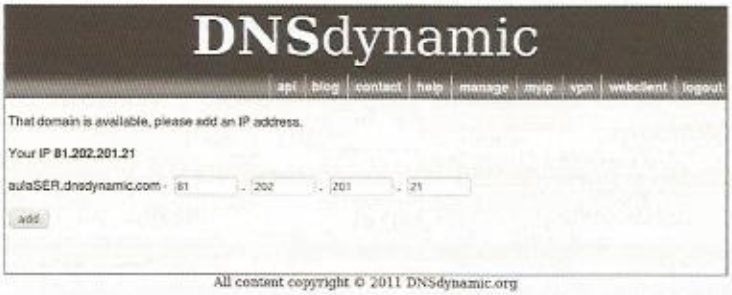


Fig. 2.46. *Dirección IP para el dominio.*

El servicio permite añadir mas dominios pulsando en *add*.

2. Configuración del router para soportar DNS dinámico

Desde el navegador web, accede a la URL de tu router, valida tu nombre de usuario y contraseña (Fig. 2.47); se mostrará la interfaz de administración del mismo:

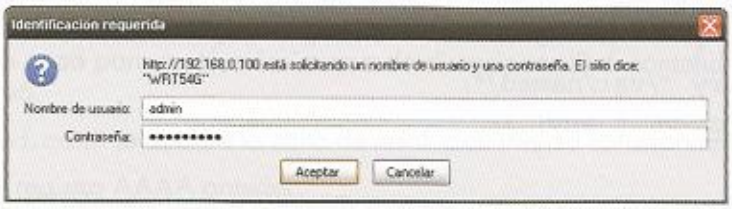


Fig. 2.47. *Acceso al router para activar DNSdynamic.*

En la ventana *Setup*, accede a la pestaña DDNS. En principio, este servicio aparece desactivado. En función del tipo de router aparecerá una serie de opciones para DNS dinámico (Fig. 2.48); selecciona la correspondiente a DNSdynamic e introduce los datos correspondientes a la cuenta creada en la web **www.dnsdynamic.org:** usuario, contraseña y nombre del dominio. De esta forma se valida el dominio para el router.

Si tienes un servidor web instalado en el servidor, puedes acceder a él desde la dirección **http://aulaser.dnsdynamic.org.**

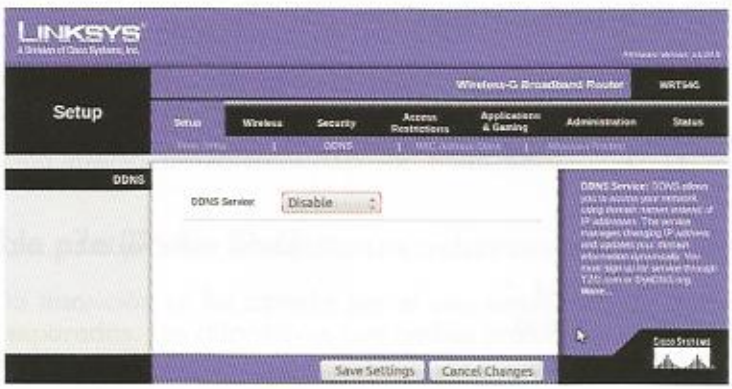


Fig. 2.48. *Activación de DNSdynamic.*

¿Sabías que...?

Cuando entras en un sitio web sin utilizar una dirección IP, en realidad estás preguntando al servidor DNS cuál es la IP correspondiente a este dominio. Luego, con este dato se realiza la conexión.

Como la IP no cambia cada día, si entrases varias veces en un sitio web estarías haciendo la misma pregunta cada vez.

Un DNS caché evita esto, ya que guarda un listado de las peticiones para no tener que estar preguntando cada vez.

Además, si el servidor DNS cae, puedes seguir entrando en los sitios que ya habías visitado.

Para conseguir este efecto hay que instalar el paquete Dnsmasq en Ubuntu.

Es recomendable repasar la Actividad 7 para dominios .com.

9. DNS con IPv6

El sistema DNS tiene la función de traductor de nombres de dominio a direcciones de red tanto del tipo IPv4 como del tipo IPv6. Es importante que los servidores DNS sean capaces de hacer peticiones de resolución de nombres sobre ambos tipos, ya que no toda la infraestructura de DNS soporta IPv6, y debe asegurarse la compatibilidad con los servidores ya existentes.

Al ser DNS independiente del protocolo de transporte, las peticiones y respuestas pueden ser transmitidas sobre IPv6 o IPv4, independientemente del tipo de información transportada.

El servidor DNS BIND soporta IPv6 para GNU/Linux, y Windows DNS Server para plataformas Windows.

En este apartado, a partir de una instalación de BIND 9.8.1, veremos cómo hacer lo siguiente:

1. Atender peticiones sobre IPv6 (escuchar IPv6).
2. Asociar direcciones IPv6 a nombres de dominio (Registros AAAA).
3. Realizar la resolución inversa de direcciones IPv6 a nombres de dominio (registro PTR).

Las especificaciones para DNS sobre IPv6 están recogidas en el RFC 1886 (Extensiones DNS para soportar IPv6).

9.1. Habilitar la escucha del servidor por IPv6

Para habilitar la escucha por IPv6 hay que editar el archivo `/etc/named.conf` y añadir a la sección `options` la directiva `listen-on-v6`. El código quedará así:

```
options {
directory "/var/named/";
listen-on-v6 { any; };
};
```

Con `listen-on-v6 { any; }` estamos diciendo que el servidor DNS escuchará en todas las direcciones IPv6 que posea el servidor.

9.2. Registros AAAA

Las direcciones IPv6 se almacenan en registros de tipo AAAA en el DNS.

Como vimos, en BIND el archivo `/etc/bind/named.conf.local` contiene las zonas de las que se encarga el servidor. Comprobamos que existe la zona de nuestro dominio `/var/lib/bind/aulaSER.com.hosts`, que es el master:

```
zone "aulaSER.com" {
type master;
file "/var/lib/bind/aulaSER.com.hosts";
};
```

Los ficheros de zona para resolución directa pueden contener registros con direcciones IPv4 e IPv6 a la vez. En nuestro caso editamos `/var/lib/bind/aulaSER.com.hosts` y añadimos:

```
$ttl 38400
aulaSER.com. IN SOA servidor.aulaSER.com. ser-admin.aulaSER.com. (
            1242759044
                  10800
                  3600
                  604800
                  38400 )
```

¿Sabías que...?

Los túneles proporcionan un mecanismo para utilizar las infraestructuras IPv4 mientras la red IPv6 está siendo implantada.

Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4.

Estos túneles se pueden utilizar en tres configuraciones:

1. **Router a router:** varios routers con doble pila (IPv6/IPv4) se conectan mediante una infraestructura IPv4 y transmiten tráfico en IPv6. El túnel comprende un segmento que incluye la ruta completa, extremo a extremo, que siguen los paquetes IPv6.
2. **Host a router:** varios hosts con doble pila se conectan a un router intermedio (también con doble pila), alcanzable mediante una infraestructura IPv4. El túnel comprende el primer segmento de la ruta seguida por los paquetes.
3. **Host a host:** varios hosts con doble pila interconectados por una infraestructura IPv4. El túnel comprende la ruta completa que siguen los paquetes.
4. **Router a host:** routers con doble pila que se conectan a hosts también con doble pila. El túnel comprende el último segmento de la ruta.

Actividades

21. ¿Qué son los servidores DNS de doble pila?

```
aulaSER.com.            IN    NS     servidor.aulaSER.com.
aulaSER.com.            IN    A      192.168.100.254
                        IN    AAAA   fdda:5cc1:23:4::1f
ipv4-ipv6               IN    A      192.168.100.254
                        IN    AAAA   fdda:5cc1:23:4::1f
ipv6                    IN    AAAA   fdda:5cc1:23:4::1f
ipv4                    IN    A      192.168.100.254
servidor                IN    A      192.168.100.254
pc11.aulaSER.com.       IN    A      192.168.100.1
pc12.aulaSER.com.       IN    A      192.168.100.2
pc13.aulaSER.com.       IN    A      192.168.100.3
pc14.aulaSER.com.       IN    A      192.168.100.4
```

A partir de estas acciones hemos configurado lo siguiente:

- `ipv4.aulaSER.com` resolverá solamente a una dirección ipv4 192.168.100.254.
- `ipv6.aulaSER.com` resolverá solamente a una dirección IPv6 fdda:5cc1:23:4::1f
- `ipv4-ipv6. aulaSER.com` resolverá una dirección IPv4 y una dirección IPv6 a la vez.

9.3. Registros PTR

Los registros PTR son los mismos que se utilizan para la resolución inversa de direcciones IPv4 a nombres de dominio. La diferencia con IPv6 está en la notación utilizada para representar las direcciones IPv6 (nibbles) y en el nombre de dominio utilizado (IP6 ARPA).

Los ficheros de zona para resolución inversa de direcciones IPv6 contendrán solamente direcciones IPv6.

En `/etc/named.conf` se declara la zona de resolución inversa correspondiente al prefijo.

En el caso del registro AAAA anterior:

```
aulaSER.com.        IN      AAAA        fdda:5cc1:23:4::1f
```

Su registro PTR en IPv6 sería:

```
f.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.3.2.0.0.1.c.c.5.a.d.d.f.ip6.arpa.
IN   PTR    aulaSER.com.
```

9.4. Comprobación

Con el fin de realizar la comprobación deberemos reiniciar el servidor DNS con `/etc/init.d/named restart`.

Comprobaremos que el servidor está escuchando en las direcciones IPv6 e IPv4 en el puerto 53 de DNS con la orden `netstat -atunp`.

Haremos consultas al servidor utilizando la orden `dig any ipv6.aulaSER.com` o por medio de la orden `dig any ipv4-ipv6. aulaSER.com`.

Para la resolución inversa, utilizaremos `dig -x fdda:5cc1:23:4::1f`

9.5. Doble pila (IPv4 e IPv6)

Para facilitar la transición se ha optado por el uso simultáneo de ambos protocolos, pero en pilas separadas. Los dispositivos con ambos protocolos también se denominan «nodos IPv6/IPv4».

De esta forma, un dispositivo con ambas pilas pueden recibir y enviar tráfico a nodos que solo soportan uno de los dos protocolos (nodos solo IPv4 o solo IPv6).

Importante

Un nibble son cuatro bits (medio byte), por lo que se suele representar en formato hexadecimal (0, 1, 2,..., 9, A, B, C, D, E, F).

Actividades

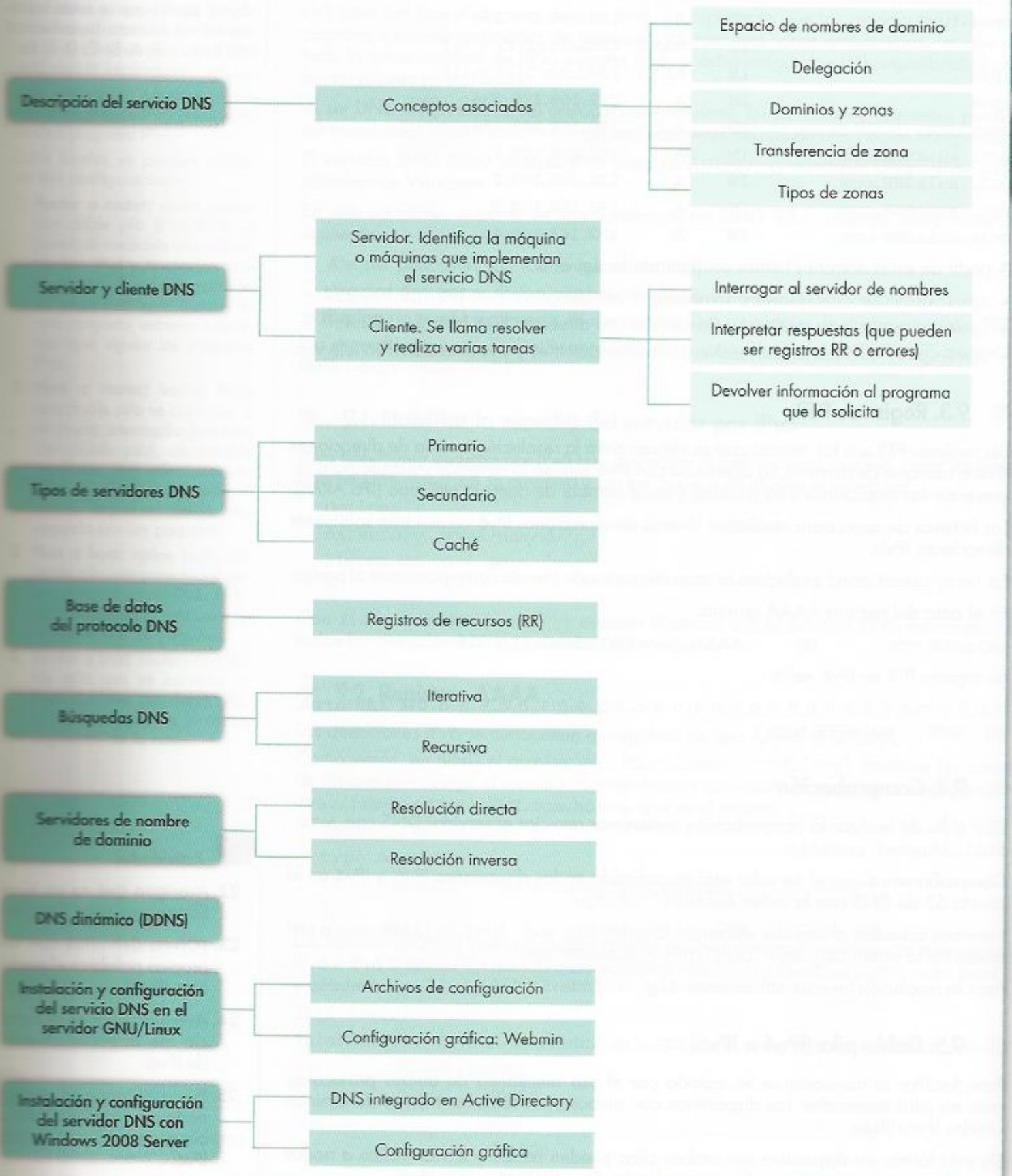
22. Averigua qué es un túnel Server y un túnel Brocker.

23. ¿Cómo definirías con tus propias palabras el protocolo IPv6?

24. Averigua cuál es el espacio de direccionamiento de IPv6.

25. Busca información relacionada con los tipos de direccionamiento disponible con IPv6.

Síntesis


Descripción del servicio DNS
Conceptos asociados
Espacio de nombres de dominio
Delegación
Dominios y zonas
Transferencia de zona
Tipos de zonas
Servidor y cliente DNS
Servidor. Identifica la máquina o máquinas que implementan el servicio DNS
Cliente. Se llama resolver y realiza varias tareas
Interrogar al servidor de nombres
Interpretar respuestas (que pueden ser registros RR o errores)
Devolver información al programa que la solicita
Tipos de servidores DNS
Primario
Secundario
Caché
Base de datos del protocolo DNS
Registros de recursos (RR)
Búsquedas DNS
Iterativa
Recursiva
Servidores de nombre de dominio
Resolución directa
Resolución inversa
DNS dinámico (DDNS)
Instalación y configuración del servicio DNS en el servidor GNU/Linux
Archivos de configuración
Configuración gráfica: Webmin
Instalación y configuración del servidor DNS con Windows 2008 Server
DNS integrado en Active Directory
Configuración gráfica