Tema 2. Servicio de Nombres de Dominio. DNS

Tema 2. Servicio de nombres de dominio. DNS.

El servicio de resolución de nombres usado en las redes TCP/IP es el servicio DNS *Domain Name System* o Sistema de Nombres de Dominio. Este servicio permite identificar de una forma más sencilla a un equipo mediante un nombre, en lugar de usar la identificación numérica de la dirección IP.

1. Características.

Para facilitar el uso de los servicios, recursos y equipos de una red se creó un sistema de nombres que mediante un servicio de resolución de nombres permite asociar nombres con direcciones numéricas. De forma simplificada podemos decir que un servicio de nombres almacena direcciones y sus nombres correspondientes.

La operación que hay que realizar para conocer la dirección IP de un equipo a través de su nombre se denomina *resolución de nombre*.

El servicio DNS es un servicio de registro y consulta de información, la cual se almacena en una base de datos distribuida en numerosos equipos. Estos equipos que almacenan una parte de la información de denominan *servidores de nombres*.

La información a la hora de distribuirla entre los diversos servidores de nombres se organiza mediante un esquema de nombres jerárquico. Este esquema jerárquico es lo que se denomina *espacio de nombres de dominio*. Así cada servidor de nombre gestiona sólo una parte de todo el espacio de nombres de dominio. Dicha parte se denomina *dominio* y es un subárbol del espacio de nombres de dominio.

Los clientes DNS se dedican a preguntar a los servidores de nombres, los cuales responden usando para la comunicación entre ellos el protocolo DNS.

El servicio DNS no sólo permite asociar un nombre de dominio con una dirección IP, además permite almacenar otras informaciones, como por ejemplo qué equipos ofrecen un determinado servicio, cuál es el servidor de correo del dominio, o qué equipos son fuentes de *malware* o de *spam*.

2. Componentes.

El servicio DNS se basa en el modelo cliente-servidor y está formado por los componentes siguientes:

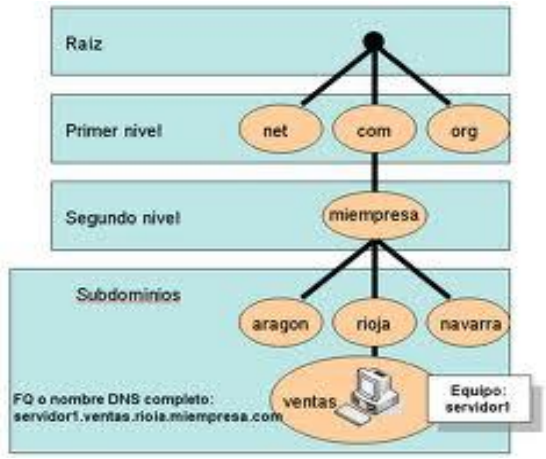
- Espacio de nombres de dominio. Lo forma la totalidad del conjunto de nombres, estructurados de forma jerárquica que permite identificar equipos o servicios de red.
- Base de datos DNS. Es una base de datos distribuida que contiene la información del espacio de nombres del dominio. La base de datos se organiza en *zonas*, en las cuales los datos se registran mediante los llamados *registros de recursos (RR)*.
- Servidores de nombres. También llamados servidores DNS. Guardan parte de la base de datos DNS en las llamadas *zonas* y son capaces de responder a las preguntas relativas a la información que almacena en sus zonas. Normalmente un servidor de nombres guarda información de una sola zona, (la información correspondiente a esa parte del espacio de nombres o dominio), pero también puede registrar la información de varios dominios que el servidor almacenará en varias zonas.
- Clientes DNS o resolvedores. Son los encargados de realizar las preguntas a los servidores de nombres y ofrecer las respuestas a los clientes o aplicaciones que las solicitan.
- Protocolo DNS. Conjunto de reglas y normas que usan los servidores y clientes DNS para dialogar.

3. Espacio de nombres de dominio.

Como hemos comentado, el espacio de nombres de dominio lo forma el conjunto de nombres que permite identificar equipos o servicios de red, estructurados de forma jerárquica.

Estos nombres se denominan *nombres de dominio* y están formados por una serie de caracteres separados por puntos. Por ejemplo: *google.es., info., servidor.aula.izv.*

El espacio de nombres de dominio se puede representar mediante una estructura jerárquica arborescente, donde cada nodo del árbol se separa de otro mediante un punto.



Los nombres de dominio no pueden superar los 255 caracteres distribuidos en como máximo 127 niveles, los cuales pueden contener como máximo 63 caracteres.

Los nombres de dominio siempre terminan con un punto, ya que el árbol de nombres de dominio empieza en el dominio "." o dominio *raíz*. Los dominios que cuelgan del dominio raíz se denominan *dominios de primer nivel* o *dominios de nivel superior* (TLD, Top Level Domains). Los que cuelgan de los dominios de primer nivel se denominan *dominios de segundo nivel*. Normalmente a los dominios de tercer nivel e inferiores se les suelen denominar *subdominios*, aunque sólo es cuestión de nomenclatura.

3.1. Nombres de dominio.

Los nombres de dominio no sólo sirven para hacer referencia a un equipo en el espacio de nombres de dominio. También sirven para hacer referencia a un subárbol del espacio de nombres del dominio, es decir para hacer referencia a un nodo, y a todos los nodos que cuelgan de éste.

Por ejemplo, el dominio *es.* hace referencia a todos los nodos (subdominios y equipos) que cuelgan del dominio de primer nivel *es.* El dominio *aula.izv.* hace referencia a todos los nodos que cuelgan del domino de segundo nivel *aula.izv.*

Por lo tanto un dominio permite hacer referencia a un conjunto de equipos y subdominios que se agrupan según un criterio. Uno de los criterios más usados, y que suele causar confusión, es el de los equipos que pertenecen a una misma red. Por ejemplo, en nuestro caso el dominio *aula.izv.* agrupa a todos los equipos del aula, los cuales están en la misma red (192.168.110.0/24), pero esto no quiere decir que todos los equipos que pertenezcan a una misma red deben pertenecer al mismo dominio. De hecho se pueden usar otros criterios de agrupación: equipos de una misma empresa (aunque los equipos estén en redes distintas…), equipos que prestan servicios, equipos que estén en una misma ubicación física, etc.

Un *nombre de dominio perfectamente cualificado* (FQDN, Fully Qualified Domain Name) es un nombre de dominio absoluto o completo, en el sentido de que el nombre de equipo o host refleja su localización exacta en el espacio de nombres de dominio. Se debe especificar todos los niveles de dominio, incluido el dominio raíz. Por ejemplo: *puesto5.aula.izv.*

3.2. Administración de nombres de dominio.

En Internet, la administración y la organización del espacio de nombres de dominio se realiza a través de diversas empresas y organizaciones coordinadas por la ICANN (*Internet Corporation for Assigned Names and Numbers* http://www.icann.org/).

El ICANN tiene la misión de que Internet sea funcional y entre otras cosas, de administrar el dominio raíz y de mantener un registro de los dominios de primer nivel o superior (TLD).

Por otra parte, InterNIC, (http://www.internic.net/) organización asociada al ICANN, es la encargada de registrar los dominios de primer nivel (TLD).

Los dominios de primer nivel (TLD) se clasifican por parte de la ICANN en:

- Genéricos. Usan un nombre relacionado con el propósito o el tipo de organización que lo va a utilizar. Éstos a su vez se clasifican en:
  - Patrocinados. Existe una organización que lo patrocina. Ejemplos: "info", "asia", "edu", etc.
  - No patrocinados. Operan con unas reglas comunes establecidas por el ICANN. Por ejemplo:"com", "net", "org", etc.
- Geográficos. Usan dos letras en función del país. La gestión del estos dominios es delegada por el ICANN a organizaciones propias de cada uno de los países denominadas *operadoras de registro*. Ejemplo de dominios geográficos son: "es", "uk", "fr". En España Red.es

(http://www.red.es) es la organización delegada por el ICANN para la gestión del dominio "es", y del registro de dominios de segundo nivel dentro de "es".

- arpa. El dominio "arpa" lo gestiona directamente la ICANN y sirve a través de los subdominios "in-addr.arpa" y "ip6.arpa" para efectuar la resolución inversa de direcciones.
- Reservados. Son dominios de primer nivel reservados sólo para pruebas y documentación. Por ejemplo: "test", "example" y "localhost".

3.3. Delegación de dominios.

La delegación permite que una organización que administra un dominio, ceda la administración de sus subdominios (de uno, de varios o de todos) a otras organizaciones. Por ejemplo la ICANN, administradora del dominio raíz, delega en Red.es la administración del dominio de primer nivel "es", y ésta a su vez delega a otras organizaciones los dominios de segundo nivel.

Por ejemplo, el dominio "ugr.es." es delegado por Red.es a la Universidad de Granada, la cual puede a su vez delegar o no sus subdominios a otras organizaciones. Así el subdominio "etsiit.ugr.es." es delegado por la Universidad de Granada a la ETS de Informática y Telecomunicaciones.

El hecho de que un dominio se divida en subdominios no implica que tenga que ser delegado. Por ejemplo la UGR puede crear el subdominio "derecho.ugr.es." pero no delegar su administración.

3.4. Registros de dominio.

El registro de un dominio consiste en reservarle un nombre durante un tiempo, para poder crear subdominios y asociar al dominio y a sus subdominios direcciones IP.

El registro de nombres de segundo nivel lo realizan empresas u organizaciones acreditadas denominadas *agentes registradores* las cuales asesoran a los clientes que quieren registrar un dominio. Además tramitan las solicitudes operando como intermediarios entre los clientes y las operadoras de registro de primer nivel.

Red.es puede registrar directamente dominios de segundo nivel, pero los clientes utilizan normalmente los servicios de los agentes registradores debido a que suelen ofrecer otros servicios complementarios (alojamiento web, servidores de correo, etc,) y a precios más competitivos.

En los sitios web pertenecientes a ICANN e InterNIC podemos obtener la lista de empresas registradoras acreditadas que ofrecen servicios de registro de dominios genéricos, y en Red.es las acreditadas para el dominio "es".

4. Servidores de nombres.

Los servidores de nombres o servidores DNS almacenan una parte de la base de datos DNS guardando información sobre nombres de dominio y respondiendo a los clientes DNS u otros servidores DNS. Los servidores escuchan las peticiones por defecto en los puertos 53/TCP y 53/UDP.

La parte de información del espacio de nombres de dominio que mantienen los servidores de nombres se denomina zona. Cuando un servidor de nombres contiene información de una zona se dice que es *autorizado para esa zona*. La información de una zona se almacena en archivos de texto o en bases de datos, dependiendo de la implementación software de servidor.

Los ficheros de zona almacenan básicamente sus datos mediante registros de recursos (RR). Según el tipo de información que se asocie con un nombre de dominio se utiliza un tipo de RR u otro.

Por ejemplo un servidor DNS para los equipos del aula almacenaría la información de la zona "*aula.izv."* definiéndose los nombres que cuelgan de "*aula.izv."* como por ejemplo "*puesto1.aula.izv."*, "*puesto2.aula.izv."*, "*www.aula.izv."* etc.

Aunque posteriormente lo examinaremos con más detalle, el servidor **BIND** (*Berkeley Internet Name Domain*), es el servidor DNS más comúnmente usado en Internet y un estándar de facto. Registra los datos en formato texto. Los registros de recursos más usuales son:

- NS. Indica cuales son los servidores de nombres de dominio DNS que tienen autoridad para una zona.
- A. Permite asociar un nombre de dominio con su dirección IP.

- CNAME. Asigna otro nombre o alias a un nombre de dominio previamente definido.

Por ejemplo, un archivo de zona de resolución directa para el dominio *aula.izv*, podría ser:

```
. . .
aula.izv.              IN      NS      puesto1.aula.izv.
puesto1.aula.izv.      IN      A       192.168.110.1
puesto2.aula.izv.      IN      A       192.168.110.2
puesto3.aula.izv.      IN      A       192.168.110.3
www.aula.izv.          IN      CNAME   puesto2.aula.izv.

;subdominio sri.aula.izv.      delegado
sri.aula.izv.          IN      NS      puesto10.sri.aula.izv.
puesto10.sri.aula.izv. IN      A       192.168.110.10

;subdominio bd.aula.izv.   no delegado
puesto15.bd.aula.izv.  IN      A       192.168.110.15
puesto16.bd.aula.izv.  IN      A       192.168.110.16
puesto17.bd.aula.izv.  IN      A       192.168.110.17
. . .
```

El archivo de zona del dominio *aula.izv.* nos indica que se almacena en un servidor DNS que está en el equipo con dirección IP 192.168.110.1 y cuyo nombre es *puesto1.aula.izv*. A continuación los registros tipo "A" asocian un nombre de dominio con una dirección IP, y con CNAME indicamos otro nombre de dominio (un alias) para *puesto2.aula.izv*.

También podemos comprobar cómo se ha delegado el subdominio *sri.aula.izv.* a otro servidor DNS con dirección IP 192.168.110.10 y cuyo nombre es *puesto10.sri.aula.izv*. Este servidor será autorizado para el dominio *sri.aula.izv.* y deberá almacenar el archivo de zona de dicho subdominio.

Este archivo de zona del dominio delegado *sri.aula.izv.* podría ser:

```
. . .
sri.aula.izv.          IN      NS      puesto10.sri.aula.izv.
puesto10.sri.aula.izv. IN      A       192.168.110.10
puesto11.sri.aula.izv. IN      A       192.168.110.11
puesto12.sri.aula.izv. IN      A       192.168.110.12
. . .
```

Por otro lado, el subdominio *bd.aula.izv.* no se ha delegado ya que la zona también almacena los RR del subdominio. Por lo tanto el servidor DNS es autorizado para los dominios *aula.izv* y *bd.aula.izv.*

Es común el error de considerar los términos zona y dominio como sinónimos. Un dominio es un subárbol del espacio de nombres del dominio cuyos nombre de dominio puede estar almacenados en una o varias zonas, las cuales pueden estar distribuidas en uno o varios servidores DNS. (El servicio de búsquedas de Google no iría tan rápido si solo hubiera un único servidor autorizado para el dominio *google.com*.)

En nuestro ejemplo anterior podemos comprobar como los nombres de dominio *aula.izv.* se distribuyen en dos archivos de zona, el fichero de la zona *aula.izv.* y el fichero de la zona *sri.aula.izv.*

Además, un servidor de nombres puede tener autoridad sobre varias zonas. Por ejemplo, un mismo servidor puede ser autorizado para las zonas *aula.izv* y *taller.izv*.

4.1. Tipos de servidores de nombres.

Según la función que realizan los servidores de nombres se pueden clasificar en:

- **Servidor maestro (*master*)**. Define una o varias zonas para las que es autorizado. El administrador es el responsable de los archivos de zona, añadiendo, modificando o borrando nombres de dominio.

  Si un cliente DNS le pregunta por un nombre de dominio para el que está autorizado, consultará en los archivos de su zona y le responderá. Si no está autorizado, buscará la información en otros servidores DNS si así está configurado, o responderá que no sabe la respuesta.

- **Servidor esclavo (*slave*).** Define una o varias zonas para las que es autorizado, pero obtiene los archivos de zona de otro servidor autorizado para la zona (maestro o esclavo), realizando lo que se denomina *transferencia de zona*. Los archivos de zona del servidor esclavo no se pueden editar, por lo que las modificaciones deben realizarse en el servidor que realiza la transferencia.

  Un servidor DNS puede ser maestro para una o varias zonas y a la vez esclavo de otras. Además pueden existir varios servidores esclavos para una misma zona.

  Con los servidores esclavos se puede repartir la carga de trabajo entre varios servidores y disminuir los fallos que se puedan producir en el servicio.

- **Servidor caché**. Si un servidor DNS recibe una pregunta sobre un nombre de dominio para la que no está autorizado, podrá preguntar, si está configurado así, a otros servidores DNS. Si el servidor actúa como caché, las respuestas obtenidas de los otros servidores las podrá almacenar durante un tiempo (TTL, *Time To Live*). De esta forma, cuando un cliente u otro servidor DNS le formule una pregunta, consultará primero en su memoria caché, por si ya tuviera la respuesta.

  Los servidores llamados *solo caché*, son los que no tienen autoridad sobre ningún dominio y siempre tienen que realizar las preguntas a otros servidores para resolver las peticiones, guardando las respuestas en su memoria caché. En redes extensas y con muchos equipos, es adecuado tener un servidor DNS que actúe de esta forma ya que se logra disminuir significativamente el tráfico en la red.

- **Servidor reenviador (*forwarding*).** Cuando un servidor DNS no tiene respuesta a una petición de resolución, puede si así está configurado, realizar la pregunta a otros servidores en un orden que luego explicaremos, o bien puede trasladar directamente la pregunta a otros servidores DNS (*forwarders*), para que sean éstos los que se encarguen de resolverla.

  Con esto se consigue disminuir el tráfico de peticiones DNS generado por los equipos de una red a Internet (se encargan de resolver los *forwarders*) y además se comparte la caché de los servidores DNS a los que se le reenvían las consultas.

  Lógicamente, las consultas que se reenvían son sólo aquellas para las que el servidor no está autorizado, ni cacheadas previamente.

- **Servidor sólo autorizado**. Son los servidores que son autorizados para una zona pero que no responden a peticiones que no sean para su zona. Esto implica que no preguntan a otros servidores, no hacen de reenviador, ni tampoco actúan como caché.

En Internet existen una serie de servidores DNS denominados servidores raíz (*root servers*) autorizados para el dominio raíz "." Estos servidores contienen el archivo de la zona "." en donde se delega a otros servidores DNS autorizados los dominios de primer nivel.

El ICANN es responsable de estos servidores raíz, en concreto 13, de los cuales existen copias repartidas mundialmente. Cada uno de ellos, y sus copias, se identifica con una misma dirección IP, de forma que cuando un cliente u otro servidor DNS les realiza una pregunta, responde la copia más cercana.

Como luego veremos, estos servidores raíz deben ser conocidos por todos los servidores DNS para poder responder a preguntas sobre nombres de dominio para los que no están autorizados.

En la web http://root-servers.org/ podemos ver cuáles son los servidores raíz, sus nombres, ubicaciones y las empresas que los administran; y en http://www.iana.org/domains/root/db los servidores de nombres y las empresas u organizaciones responsable de los dominios de primer nivel.

5. Clientes DNS (resolvedores).

Antes de que existieran servidores DNS que resolvieran los dominios, se usaba un archivo de texto (denominado *hosts*) donde se guardan las correspondencias entre nombres de dominio y direcciones IP. Este mecanismo se dejó de utilizar cuando Internet empezó a crecer en nombres de dominio, pasándose a usar servidores DNS.

Muchos sistemas operativos están configurados para usar este método antes de usar el servicio DNS. Si mediante la tabla de *hosts* no se puede resolver, se usa el servicio DNS. En una red local con pocos equipos y que mantengan direcciones fijas puede ser efectivo mantener la tabla de *hosts*, en otro caso, mantener actualizado y sincronizado el archivo *hosts* en todos los equipos es muy complicado y genera errores. En la actualidad también se usa para bloquear contenidos de Internet como la publicidad web.

El formato del archivo *hosts* es el siguiente:

- En cada línea se debe introducir la dirección IP a la que resolverá, uno o más espacios o tabulaciones y el dominio a resolver.
- Se pueden introducir más de un dominio a resolver en la misma línea separados por uno o más espacios o tabulaciones.
- Cada correspondencia de dirección IP y dominio debe ir en una línea distinta.
- Las líneas que comienzan por # se consideran comentarios y no se computan.

Un ejemplo válido de archivo *hosts* podría ser este:

```
#Definición de localhost
127.0.0.1       localhost

#Correspondencia para equipos de la red local
192.168.110.1       puesto1.aula.izv
192.168.110.222     ns1.aula.izv

#Correspondencia para una página web
209.85.229.104      www.google.es

#Dominios de Internet bloqueados mediante un IP inválida (usando por ejemplo un máscara de subred…)
255.255.255.0       www.fantomas.com    www.petardas.com    www.justinbieber.com
```

La única entrada obligatoria y que aparece siempre por defecto es la del dispositivo de red loopback. Las direcciones del rango 127.0.0.0/8 son direcciones de loopback, de la cual la que se utiliza de forma mayoritaria es la 127.0.0.1 por ser la primera de dicho rango. A pesar de se suele usar la dirección 127.0.0.1, se reservan las direcciones 127.0.0.0 a 127.255.255.255. Cualquier dirección dentro de este bloque producirá un loopback dentro del equipo local.

Esta dirección especial se suele utilizar cuando una transmisión de datos tiene como destino el propio equipo de forma que éstos la utilizan para dirigir el tráfico hacia ellos mismos. También es posible hacer ping a la dirección de loopback para probar la configuración de TCP/IP en el host local.

Ojo. En algunas distribuciones Linux de Debian o basadas en ésta, se añade otra entrada asociada al loopback, en concreto la 127.0.1.1. Esto realmente es un apaño para resolver un bug del escritorio gnome. Se puede sustituir esta dirección por la que tenga el equipo en la red, siempre que dicha dirección se mantenga y no cambie de forma dinámica mediante DHCP.

Un resolvedor (*resolver*) es cualquier software que realiza preguntas a un servidor DNS y entiende las respuestas recibidas. Los sistemas operativos incluyen un conjunto de librerías que realizan estas operaciones y que son invocadas por las aplicaciones cuando usan un nombre de dominio.

Normalmente, se puede configurar si el resolvedor deberá buscar primero en el archivo de *hosts* antes de hacer la resolución del nombre mediante el servicio DNS.

Así, en general los pasos que realiza el resolver cuando una aplicación quiere resolver un nombre son:

1. Consulta la memoria caché de resolución de nombres, si está configurada.
2. Si la respuesta no es positiva, realiza la búsqueda en el archivo *hosts* del equipo.
3. Si el nombre de dominio tampoco existe en el archivo *hosts*, se realizará una consulta *recursiva* al servidor DNS que se tenga configurado y éste suministrará la respuesta a la aplicación.

6. Mecanismo de resolución.

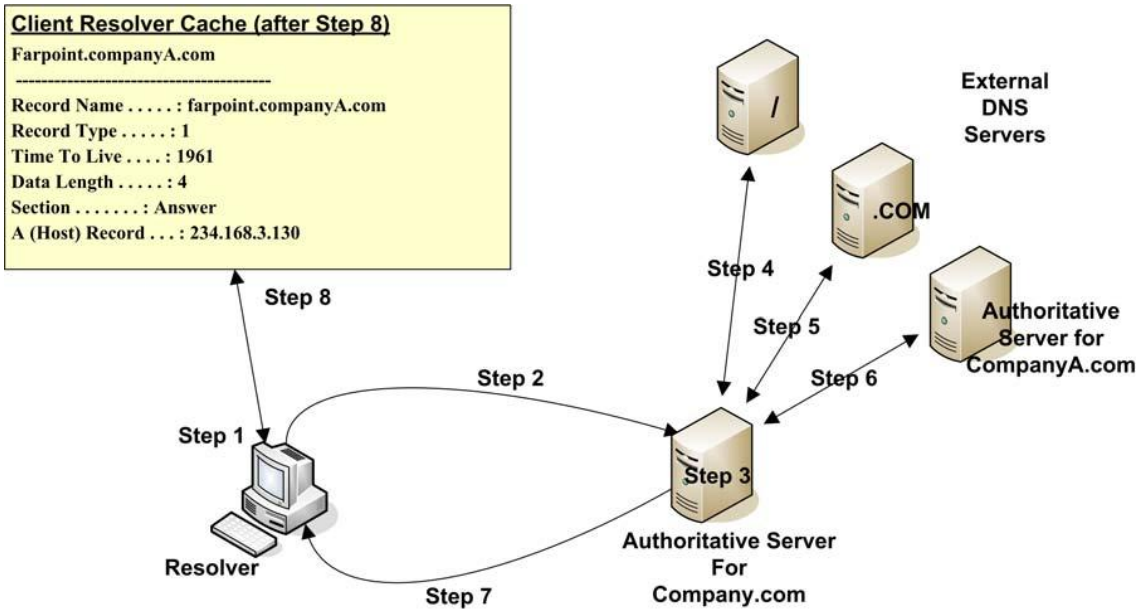
Las consultas a un servidor DNS pueden ser *recursivas* o *iterativas* (también llamadas no recursivas). Como veremos a continuación, a la hora de resolver un nombre, el resolvedor realiza una consulta recursiva, la cual podrá generar o no en una serie de consultas iterativas.

Una consulta *recursiva* es aquella en la que el servidor debe dar siempre una respuesta completa. Esta respuesta podrá ser: positiva indicándose si ésta es autorizada o no, negativa (si no se pudo resolver) o de error (por ejemplo por fallo en la red).

Una consulta *iterativa* es aquella en la que el servidor DNS puede proporcionar una respuesta parcial. Es decir, a parte de las respuestas positivas, negativas o de error, puede dar una respuesta incompleta que indique una referencia a otros servidores a los que se les puede preguntar para resolver la pregunta.

Una consulta recursiva la inicia un cliente DNS a través del resolvedor o bien un servidor DNS que la traslada a otro servidor DNS que esté actuando como reenviador. El proceso de resolución cuando un servidor recibe una consulta recursiva es el siguiente:

1. Si el servidor es autorizado para alguna zona, comprueba sus archivos de zona, y si encuentra la respuesta, responde indicando que la respuesta es *autoritativa*.
2. Si no encuentra la respuesta, o no es autorizado y actúa como caché, consulta su caché de respuesta anteriores, y si la encuentra responde que la respuesta es *no autoritativa*.
3. Si en el paso anterior no se encontró respuesta positiva, y tiene configurados reenviadores, entonces reenvía la consulta recursiva a otro servidor DNS y la respuesta que reciba de ese otro servidor DNS la traslada al cliente o al servidor que le preguntó.
4. Si no tiene configurados reenviadores entonces:
    a. Inicia una serie de consultas *iterativas* a otros servidores DNS empezando la primera de ellas por un servidor raíz.
    b. Los servidores consultados devuelven *referencias* a otros servidores DNS que se usan para realizarles la pregunta. Este proceso de preguntas iterativas a distintos servidores finaliza cuando un servidor autorizado proporciona una respuesta positiva o negativa.



La figura muestra los pasos cuando un cliente realiza una pregunta recursiva por el dominio "*farpoint.companyA.com*" a un servidor que tiene activada la recursividad (tiene que dar una respuesta completa). Como el servidor DNS no está autorizado para la zona "companyA.com", no tendrá en sus archivos de zona el nombre de dominio por el que se le ha preguntado.

Como debe dar una respuesta, empezará una serie de consultas iterativas empezando por uno de los servidores raíz. El servidor raíz responde con una referencia al servidor autorizado para el dominio "com". El servidor DNS envía una consulta iterativa al servidor autorizado del dominio "com", y éste le responde con una referencia al servidor autorizado para el dominio "companyA.com". Posteriormente el servidor DNS envía una consulta iterativa al servidor autorizado del dominio "companyA.com".

El servidor autorizado del dominio "companyA.com" consulta en sus ficheros de zona y como existe el nombre de dominio "farpoint.companyA.com" responde con la información asociada a él, en este caso con la dirección IP. (Si no existiera el nombre de dominio en los archivos de zona respondería de forma negativa).

El servidor que recibió la respuesta recursiva entrega al resolver la información por la que preguntó (la dirección IP) y la guarda en su caché disponible para futuras consultas.

Por lo tanto, las consultas iterativas son iniciadas por un servidor DNS a otro servidor DNS, cuando en una consulta recursiva no ha encontrado la respuesta en sus archivos de zona o en la caché.

En este proceso de resolución es muy importante la caché. Por ejemplo si el resolvedor pregunta primero por el dominio www.granada.es y luego por www.alomartes.es no tendrá que preguntar de nuevo a un servidor raíz, ya que tendrá almacenada en la caché las direcciones de los servidores DNS autorizados para el dominio "es".

Como hemos podido comprobar, las consultas recursivas son costosas para los servidores DNS ya que deben dar siempre una respuesta; de hecho los servidores DNS raíz y los de primer nivel no responden a consultas recursivas.

6.1. Respuestas en caché.

Las respuestas almacenadas en cache pueden ser positivas o negativas. Es decir se puede almacenar los registros de recursos de nombres de dominio resueltos, y la información de que no existe un registro de recursos para el nombre de dominio consultado. En este último caso se impide la repetición de preguntas para nombres que no existen.

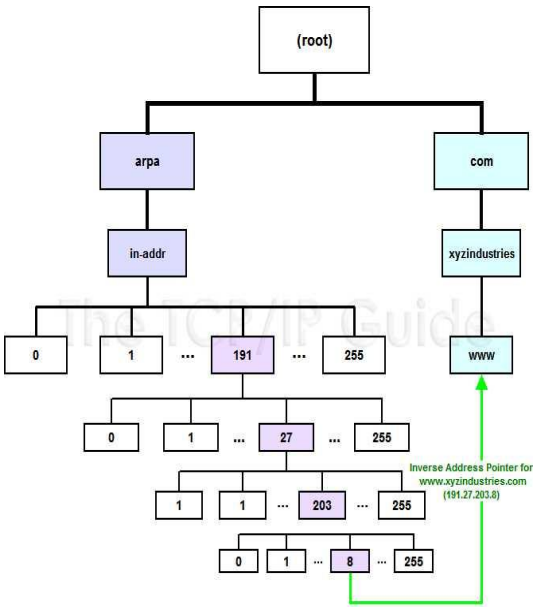
Los archivos de zona almacenan los tiempos máximos que se guardan las respuestas en caché (TTL), de forma que habrá TTL para las respuestas positivas y TTL para las negativas. Se recomienda que el TTL para las respuestas positivas sea mayor de un día, incluso semanas, y que el TTL para las respuestas negativas sea menor de 3 horas.

7. Correspondencias inversas.

Las resoluciones de nombre de dominio que hemos comentado hasta ahora se denominan de *resolución directa*. Las resoluciones inversas consisten en preguntar por una dirección IP para obtener el nombre o nombres de dominio como respuesta.

Uno de los principales motivos por el que se realiza una resolución inversa está ligado a la seguridad. Si al realizar una resolución directa para un nombre de dominio obtenemos una dirección IP, la cual se usa para realizar una resolución inversa, se debería obtener el nombre de dominio por el que preguntamos. Si no es así, posiblemente un intruso esté resolviendo nombres a direcciones IP no válidas con fines maliciosos. Los servidores DNS pueden configurarse para que actúen de esta forma para asegurarse de las respuestas recibidas.

También se suelen usar para detectar errores en la configuración de los servidores y equipos, *spam* en los servidores de correo, o seguir la traza de un ataque.



En la resolución inversa, las direcciones IP se tratan como nombres en donde cada byte de la IP es un dominio que cuelga del dominio "in-addr.arpa". Así cuando realizamos una pregunta inversa del tipo ¿cuál es el nombre de dominio para la IP 191.27.203.8?, lo que realmente estamos preguntando es por el nombre de dominio de "8.203.27.191.in-addr.arpa". Como vemos, la estructura jerárquica de la dirección IP tratada como nombre de dominio es de izquierda a derecha comenzando por el dominio "in-addr.arpa".

Para la resolución inversa los servidores de nombres deben almacenar zonas de resolución inversa que podrán ser maestras o esclavas.

Las zonas directas e inversas son independientes, y el administrador debe mantener la información de ambas sin discrepancias. Si se administra una zona directa no es obligatorio administrar la zona inversa correspondiente. De hecho si administramos un dominio asociado a una IP pública contratada a un ISP éste no incluirá nuestro dominio en su zona inversa salvo que se lo pidamos expresamente.

El proceso de resolución inversa es análogo al directo. Por ejemplo una consulta recursiva de la IP 191.27.203.8 a un servidor DNS, empezaría en buscar en la caché, y si no tiene la respuesta comenzaría una serie de consultas iterativas a los servidores DNS raíz, a los servidores autorizados para el dominio "191.in-addr.arpa", a los autorizados para el dominio "27.191.in-ddr.arpa" y así sucesivamente.

Los archivos de zona de resolución inversa usan registros de recursos de tipo NS y PTR. Por ejemplo para el siguiente archivo de zona de resolución directa:

```
aula.izv.          IN    NS      puesto1.aula.izv.
puesto1.aula.izv.  IN    A       192.168.110.1
puesto2.aula.izv.  IN    A       192.168.110.2
puesto3.aula.izv.  IN    A       192.168.110.3
www.aula.izv.      IN    CNAME   puesto2.aula.izv.
```

el siguiente archivo de zona de resolución inversa "110.168.192.in-addr.arpa." nos permitiría resolver las consultas inversas sobre direcciones IP de la red 192.168.110.0/24.

```
110.168.192.in-addr.arpa.    IN    NS    puesto1.aula.izv.
1.110.168.192.in-addr.arpa.  IN    PTR   puesto1.aula.izv.
2.110.168.192.in-addr.arpa.  IN    PTR   puesto2.aula.izv.
3.110.168.192.in-addr.arpa.  IN    PTR   puesto3.aula.izv.
```

8. Registros de recursos.

Los archivos de zona almacenan la información sobre nombres de dominio mediante *registros de recursos* (RR, Resource Records). Estos RR son los que se envían entre los clientes y servidores DNS en las preguntas y respuestas.

Los RR se representan en los archivos de zona en formato texto, y de forma binaria en los mensajes que se envían mediante el protocolo DNS. El formato en modo texto es:

```
Nombre de Dominio   [TTL]   Clase   Tipo   Dato
```

Por ejemplo:

```
puesto1.aula.izv.   3600    IN      A      192.168.110.1
```

Lo primero es el nombre de dominio que se asocia al recurso, opcionalmente aparece el tiempo de vida medio (TTL) que indica en segundos el tiempo que puede estar el registro en caché antes de ser descartado. (Veremos que se puede especificar un tiempo global para todos los registros de la zona).

La clase define el tipo de protocolo usado. Aunque se pueden usar otras arquitecturas la habitual es Internet (IN). A continuación el tipo indica el tipo de dato asociado al nombre de dominio y por último se especifica el dato asociado al nombre de dominio.

8.1. Tipos de registros.

Comentaremos sólo los tipos de registros de recursos más usados, ya que el protocolo define más de una treintena. En el sitio web del IANA (http://www.iana.org/assignments/dns-parameters) se pueden consultar todos ellos.

- Registro SOA (Star of Authority). Es el primer registro de una zona y permite definir el tipo de servidor y las opciones generales de la zona.

  El registro tipo SOA comienza con el nombre del dominio de la zona, opcionalmente un TTL (lo normal es establecerlo aquí de forma global para toda la zona) y continua con la clase IN, el tipo SOA y finaliza con los datos asociados. Estos datos asociados son:

  - FQDN del servidor de nombres maestro para el dominio
  - Contacto. Dirección de correo del responsable del dominio. (La arroba se sustituye por ".")
  - Número de serie (serial). Indica la versión del archivo de zona que se irá incrementando cada vez que el archivo se modifique. De esta forma los servidores secundarios conocen si el archivo de zona ha cambiado y deben actualizarse mediante una transferencia de zona.
  - Actualización (refresh). Indica cada cuanto tiempo deben contactar los servidores secundarios con el servidor maestro para comprobar si ha habido cambios en la zona. Dependiendo de la

frecuencia de actualización de la zona primaria se usará más o menos tiempo. Se recomiendan valores entre 12 y 24 horas.

- Reintentos (retry). Indica cada cuanto tiempo deben reintentar los servidores secundarios contactar con el servidor maestro si éste no responde a una actualización.
- Caducidad (expire). Tiempo durante el cual un servidor secundario puede estar sin contactar con el primario para comprobar la zona. Si se supera este tiempo, el secundario descarta los datos que tenía sobre la zona y se declara no autorizado para la zona.
- TTL negativo. Es el tiempo mínimo en que se almacena las respuestas negativas sobre la zona.

Por ejemplo, nuestro dominio aula.izv podría tener el siguiente registro SOA

```
aula.izv.  IN  SOA  puesto1.aula.izv. carlos.aula.izv. (
                    2012041401      ; nº de versión del archivo de zona
                    604800          ; tiempo de refresco
                    86400           ; tiempo de reintento
                    2419200         ; tiempo de expiración
                    38400 )         ; TTL negativo
```

- Registro NS (Name Server). Permite indicar los servidores de nombres autorizados para una zona. (Cada zona debe contener al menos un registro NS, por ejemplo un maestro, y puede tener uno o más esclavos). Este registro también permite indicar los nombres de los servidores con autoridad en los subdominios que hayan sido delegados. (Ver ejemplo de la página 6).
- Registro A. (Address). Establece una correspondencia entre un nombre de dominio FDQN y una dirección IP (IPv4).
- Registro AAAA. (Address). Establece una correspondencia entre un nombre de dominio FDQN y una dirección IP (IPv6).
- Registro CNAME (Canonical Name). Indican un alias o sobrenombre para los nombres de dominio especificados en registros A y AAAA. Un alias puede apuntar a otro dominio, pero no se pueden usar en la parte derecha de registros MX y NS. Estos dos tipos de registros necesitan usar en su parte derecha nombres que aparezcan en registros de tipo A o AAAA.
- Registro MX (Mail Exchange). Define los equipos encargados de correo en el dominio para que los agentes de transporte de correo sepan a que equipo deben entregar el correo. Se pueden definir varios servidores de correo donde en el registro de recursos de cada uno se indican mediante un número el orden de preferencia de cada uno de ellos; a número menor le corresponde mayor preferencia.
- Registro SRV (Services Record). Permite definir equipos que actúan como servidores de algún servicio particular en el dominio. Por ejemplo servidores LDAP, servidores de mensajería, etc.
- Registro PTR (Pointer Record). Establecen correspondencias entre direcciones IP y nombres de dominio en las zonas de resolución inversas. Si se usan direcciones tipo IPv4 y IPv6 deben aparecer en zonas separadas.
- Registro TXT (Texto). Permite registrar cualquier texto que tenga relación con un equipo.

8.2. Registros pegamento (Glue Record).

Sabemos que un servidor de nombres se puede configurar para delegar o no algunos de sus dominios en otros servidores de nombres.

En el caso de que el servidor de nombres autorizado para el subdominio delegado se encuentre en el mismo dominio es necesario añadir:

1. Un registro NS en el dominio que delega, para indicar cuál es el servidor de nombres para la zona delegada.
2. Un registro A que indique la IP del servidor de nombres del subdominio delegado. Este tipo de registro se denomina *glue record* porque que de alguna forma relaciona o pega la zona hija con la zona padre.

Por lo tanto, los servidores de un dominio deben conocer la dirección IP de los servidores de nombres de los subdominios delegados para que los clientes puedan dirigirse a ellos en las consultas.

En el caso de que el servidor de nombres autorizado para el subdominio delegado no se encuentre en el mismo dominio, sólo es necesario añadir el registro NS que indique el servidor de nombres de la zona delegada. En este caso no necesita un registro tipo A, por que los clientes podrán resolver el nombre de dominio de la zona delegada normalmente.

Finalizamos con un ejemplo más completo de una zona de resolución directa para el dominio aula.izv.

```
 aula.izv.  IN  SOA  puesto1.aula.izv. carlos.aula.izv. (
                2012041401      ; nº de versión del archivo de zona
                604800          ; tiempo de refresco
                86400           ; tiempo de reintento
                2419200         ; tiempo de expiración
                38400 )         ; TTL negativo
aula.izv.               IN      NS      puesto1.aula.izv.
puesto1.aula.izv.       IN      A       192.168.110.1
puesto2.aula.izv.       IN      A       192.168.110.2
puesto3.aula.izv.       IN      A       192.168.110.3
www.aula.izv.           IN      CNAME   puesto2.aula.izv.
ftp.aula.izv.           IN      CNAME   puesto2.aula.izv.
aula.izv.               IN      MX      10      puesto3.aula.izv.
smtp.aula.izv.          IN      CNAME   puesto3.aula.izv.
_ldap._tcp.aula.izv.    SRV     0  0  389  puesto3.aula.izv.
;subdominio sri.aula.izv.       delegado en un subdominio propio
sri.aula.izv.           IN      NS      puesto10.sri.aula.izv.
puesto10.sri.aula.izv.  IN      A       192.168.110.10          ; (Glue Record)
;subdominio bd.aula.izv.        delegado en un subdominio ajeno
bd.aula.izv.            IN      NS      ns1.informatica.izv.
```

9. Transferencias de zona.

Los servidores en los que se declaran zonas esclavas, deben obtener los archivos de zonas, es decir los registros de recursos, de otros servidores (maestros o esclavos) autorizados para dichas zonas.

Este proceso se denomina transferencia de zona y hay que configurar los servidores para que las realicen. Los servidores maestros usan el puerto 53/TCP para realizar el intercambio de zona la cual puede ser de dos tipos: *completa* e *incremental*.

En las transferencias de zonas completas, el servidor maestro envía al esclavo todos los datos de la zona sustituyendo a los datos anteriores. En las transferencias de tipo incremental, el maestro sólo envía los datos que han cambiado desde la última transferencia de zona.

Las transferencias de zona puede comenzar por una pregunta del servidor esclavo al maestro para comprobar si hay algún cambio en la zona. La primera vez que se inicia el servidor esclavo realiza esta pregunta, y luego la repite cada cierto tiempo (especificado en el campo *refresh* del registro SOA).

Por otro lado el servidor maestro puede ser el encargado de notificar a los servidores esclavos de las modificaciones producidas en sus zonas. De esta manera, si se produce una modificación en la zona del maestro, el esclavo queda enterado de forma inmediata y puede comenzar el proceso de transferencia.

En el proceso de transferencia, el servidor maestro envía su registro SOA al esclavo, de forma que éste obtiene su número de serie y lo compara con el que tiene almacenado en su zona. Si el número de serie que obtiene es superior al suyo, entiende que sus datos no están actualizados y se realiza la transferencia.

El que la transferencia sea de tipo completa o incremental depende del tipo de petición que envíe el servidor maestro al esclavo empleando mensajes de tipo AXFR o IXFR respectivamente.

10. DNS dinámico (DDNS, Dynamic DNS)

Hasta ahora hemos comentado que es responsabilidad del administrador mantener actualizada la zona de los servidores de nombres. Esta tarea puede ser muy costosa si la organización dispone de varios dominios o múltiples servidores DNS. Si además si se usan servidores DHCP para asignar direcciones a

los equipos, el mantenimiento manual de las zonas no es una opción. Además cada vez que se realizara una modificación, se tendría que parar y reiniciar el servicio DNS.

Para aliviar esta situación, el RFC 2162 define los procesos para que de forma automática, los registros de recursos de una zona se puedan actualizar de forma externa, sin que el administrador tenga que editar manualmente los archivos de zona y sin necesidad de reiniciar el servicio DNS.

Normalmente las actualizaciones dinámicas de los registros de una zona las pueden realizar los propios equipos clientes o bien servidores DHCP. En ambos casos hay que configurar el servidor DNS y el servidor DHCP o los propios clientes para habilitar las actualizaciones dinámicas.

Otro problema para los usuarios que usan el servicio DNS para acceso a Internet, es cuando quieren acceder a un servicio (servidor web, ftp, corro, etc.) en un dominio que no tiene una IP fija en Internet.

Actualmente, la mayoría de los ISP proporcionan direcciones IP públicas por DHCP al *router* que nos conecta a la red. Esto implica que la IP cambiará cada cierto tiempo y por lo tanto no podemos asignarle un nombre de dominio estable a esta dirección IP.

Los llamados DNS dinámicos que ofrecen algunos sitios web en Internet permiten registrar un nombre de dominio actualizándolo con la dirección IP que realmente se tenga en el momento. Lo más habitual es que sea el propio *router* el que tenga la posibilidad de actualizar el servidor DNS cuando cambie su dirección IP, aunque también podría ser un programa instalado en algún equipo de la red.

Varias web, como DynDNS o No-ip ofrecen estos servicios de forma gratuita sobre un dominio de segundo nivel de su propiedad. Por ejemplo podríamos configurar un servidor web con IP dinámica con el nombre de dominio “micasa.dynds.org”.

11. Seguridad DNS.

El servicio DNS es fundamental para el funcionamiento de una red e imprescindible en Internet, por ello suele ser un objetivo para los atacantes. El hecho de que el protocolo DNS se diseñara inicialmente sin tener en cuenta la seguridad (al igual que otros servicios de red) y que el servicio al ser distribuido depende de muchos equipos, implica dificultades para su administración.

Las principales amenazas para un servicio DNS son:

- Ataques al servidor DNS usando *exploits* aprovechando agujeros en la seguridad.
- Modificaciones de los archivos de zonas aprovechando una mala configuración de los permisos de usuarios que puedan acceder al equipo servidor de forma remota.
- Ataques DoS (*Denail of Service*) mediante inundación de múltiples peticiones UDP.
- Suplantación del servidor DNS, enviando RR incorrectos y envenenando la caché del cliente.
- Envenenamiento de la caché de un servidor DNS al preguntar a otro DNS suplantado.
- Suplantaciones del servidor maestro en las transferencias de zona.
- Suplantaciones de los orígenes externos que envían actualizaciones a los DNS dinámicos.

Los mecanismos de seguridad que se pueden establecer son:

1. En los servidores DNS. Actualización a las últimas versiones software, instalación de parches de seguridad, enjaular el servidor en un entorno seguro, configuración de los privilegios de acceso a los archivos de zona, distribuir los servidores DNS en distintas redes y ubicaciones.
2. En las transferencias de zona y actualizaciones dinámicas.
   - Establecer listas de control de acceso por IP o nombres de dominios con los servidores desde los que se permiten las transferencias de zona y las actualizaciones dinámicas.
   - Utilizar cortafuegos para controlar las transferencias y actualizaciones de zona.
   - Mecanismos de autentificación de servidores mediante generación de claves del tipo TSIG o TKEY.
3. En las consultas DNS.
   - Configurar los servidores para minimizar las consultas iterativas.
   - Limitar por dirección IP los equipos que pueden preguntar a un servidor.
   - Implantación de DNSSEC (DNS Security) basado en algoritmos de cifrado asimétricos para garantizar la autenticidad e integridad en las consultas y respuestas DNS.

12. Servidores DNS en Linux.

El servidor DNS más extendido en sistemas operativos basados en UNIX, y de facto un estándar, se llama **bind** (*Berkeley Internet Name Domain*), y actualmente lo desarrolla la organización ISC (*Internet Systems Consortium*).

Antes de realizar la instalación, siempre se debe tener la capacidad de resolver el nombre de nuestro servidor independientemente de que tengamos un servidor DNS. El motivo es que cuando se inicia el sistema, puede que sea necesario resolver el nombre del equipo, pero todavía no esté operativa la red, o que no podamos acceder al servicio DNS. Para ello, se comprueba que el nombre del servidor esté correctamente establecido en los ficheros /etc/hostname y /etc/hosts.

Por ejemplo, el contenido de un fichero /etc/hostname podría ser el siguiente:

```
ubup
```

Y el contenido del fichero /etc/hosts:

```
127.0.0.1       localhost
127.0.1.1       ubup.aula.izv ubup

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Es importante, como suele suceder en la mayoría de los servicios, que el servidor tenga una IP fija.

El servidor bind se instala mediante el paquete *bind9*, sus archivos de configuración se ubican en el directorio /etc/bind, el demonio del proceso servidor se denomina *named*, y el script que permite arrancar, parar y reiniciar el servicio es /etc/init.d/bind9 {start|stop|reload|restart|force-reload|status}.

Terminada la instalación debemos comprobar que *named* está en ejecución, y que el servicio está a la escucha en los puertos 53 TCP y UDP. Para ello ejecutamos:

```
$ ps –ef | grep named
```

```
$ netstat –ltun
```

Cuando se instala bind, se generan unos archivos con una configuración básica con unas zonas ya preconfiguradas:

- /etc/bind/named.conf. Es el archivo de configuración principal con los las diferentes zonas generadas por defecto. Incluye, mediante la directiva "include", a los tres archivos siguientes:
  - /etc/bind/named.conf.options. Contiene opciones de configuración generales del servidor. Entre otras opciones desde aquí se permite configurar el servidor como reenviador.
  - /etc/bind/named.conf.local. Es el archivo de configuración de zonas donde se declaran las zonas de resolución tanto directas como inversas.
  - /etc/bind/named.conf.default-zones. Contiene la declaración de las zonas creadas por defecto. Los archivos de zonas creados por defecto, y referenciados desde /etc/bind/named.conf.default-zones son:
    - /etc/bind/db.root Servidores raíz.
    - /etc/bind/db.local Resolución directa del bucle local.
    - /etc/bind/db.127 Resolución inversa del bucle local.
    - /etc/bind/db.0 Resolución inversa *broadcast*.
    - /etc/bind/db.255 Resolución inversa *broadcast*.

Siempre que se cambie la configuración del servidor hay que reiniciar el servicio para que tengan efecto los cambios. Es muy conveniente examinar el archivo de *logs* (/var/log/syslog) del sistema para comprobar que no se hayan producido fallos en el arranque del servidor.

El contenido del archivo de configuración /etc/bind/named.conf.options que se genera por defecto es muy simple. Le vamos a añadir algunas opciones más cuyo significado aparecen como comentarios.

```
options {
        // Directorio de trabajo por defecto
        directory "/var/cache/bind";
        // Para aceptar sólo peticiones de resolución de ciertos equipos.
        allow-query { 127.0.0.1; 192.168.110.0/24;};
        // Por defecto se permiten consultas recursivas (  recursion yes;) pero podemos limitar dichas consultas
        // recursivas solo a los equipos que indiquemos
        allow-recursion {127.0.0.1; 192.168.110.0/24;};
        // En principio no se permite enviar notificaciones de actualización de zonas a otros servidores
        notify no;
        // Servidores DNS a los que hacer peticiones de información de otras zonas (normalmente a los servidores
        // públicos de los ISP)
        // forwarders {80.58.61.250;};
        // No se responderá autoritativamente a peticiones de dominio inexistentes
        auth-nxdomain no;    # conform to RFC1035
        // Direcciones y puertos en los que realizar la escucha de peticiones de resolución.
        // (Por si hay varias interfaces de red…)
        listen-on port 53 { 127.0.0.1; 192.168.110.211;};
        // también escucha en Ipv6 (además por cualquier interfaz)
        listen-on-v6 { any; };
};
```

- Servidor DNS como solo caché.

Por defecto, el servidor *bind* está configurado como *solo caché* (no es autorizado para ninguna zona) y es capaz de responder a consultas recursivas (*recursión yes*).

Podemos probarlo configurando un cliente con dicho servidor DNS y preguntar por cualquier nombre de dominio en Internet. Además las consultas repetidas se aceleran al estar resueltas en la caché.

- Servidor DNS para que reenvíe las consultas a reenviadores

Para configurar un servidor que reenvíe las consultas a otros servidores (*forwading*) se edita el archivo named.conf.options y mediante el atributo *forwarders* se indican las direcciones IP separadas por punto y coma de los DNS que actuarán como reenviadores (*forwarders*).

Recordemos que las consultas que se reenvían son sólo aquellas para las que el servidor no está autorizado y sus respuestas no están en caché.

Si el servidor está configurado como reenviador, cabe la posibilidad de usar la opción *forward* la cual ya tiene como valor por defecto el valor *first*. Con *first* el servidor consultará a los servidores indicados con *forwarders* en primer lugar, y si no obtiene la respuesta, entonces intentará buscarla por sí mismo. Si se usa *forward only*, entonces el servidor sólo consultará a los reenviadores.

- Servidor DNS como maestro para una zona de resolución directa y una zona de resolución inversa

Para configurar el servidor DNS como maestro para una zona de resolución directa y una zona de resolución inversa se debe editar el archivo named.conf.local e indicar entre otras opciones el nombre de la zona, el tipo de zona y el archivo donde se almacenarán los registros de recursos de la zona.

Por ejemplo, si queremos que el servidor tenga autoridad para el dominio aula.izv y para la zona de resolución inversa de la red 192.168.110.0/24 editaríamos el archivo named.conf.local y le añadimos las zonas directa e inversa

```
zone "aula.izv" {
        type master;
        file "/etc/bind/db.aula.izv";
        };
zone "110.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192.168.110";
        };
```

A continuación deberíamos crear los archivos con los registros de recursos de ambas zonas. Los archivos a crear son los que hemos indicado anteriormente en el parámetro *file*. Si no hubiéramos especificado la ruta absoluta de los archivos, se toma el directorio de trabajo por defecto (/var/cache/bind).

La creación de los archivos de registros de recursos editándolos manualmente suele causar problemas, ya que la sintaxis es algo complicada. Es más cómodo usar alguna herramienta que nos ayude en esta tarea como es "Webmin". Además podemos indicarle que a medida que vayamos registrando registros de recursos de la zona directa, vaya creando automáticamente los correspondientes PTR de la zona inversa.

Ejemplo de archivo de zona de resolución directa

```
$ttl 38400 ;
aula.izv.  IN  SOA  ubup.aula.izv. carlos.aula.izv. (
                2012041401          ; nº de versión del archivo de zona
                604800              ; tiempo de refresco
                86400               ; tiempo de reintento
                2419200             ; tiempo de expiración
                38400 )             ; TTL negativo
aula.izv.       IN      NS      ubup.aula.izv.      ; servidor maestro autorizado
ubup.aula.izv.  IN      A       192.168.110.211     ; correspondencia FDQN a IP
winp.aula.izv.  IN      A       192.168.110.212
profe.aula.izv. IN      A       192.168.110.110
smtp.aula.izv.  IN      CNAME   profe.aula.izv.      ; alias para nombres de dominio
www.aula.izv.   IN      CNAME   profe.aula.izv.
aula.izv.       IN      MX  10  profe.aula.izv.      ; quien entrega el correo al dominio
```

Ejemplo de archivo de zona de resolución inversa

```
$ttl 38400 ;
110.168.192.in-addr.arpa.  IN      SOA     ubup.aula.izv. carlos.aula.izv. (
                                   1316802825
                                   10800
                                   3600
                                   604800
                                   38400 )
110.168.192.in-addr.arpa.          IN      NS      ubup.aula.izv.
211.110.168.192.in-addr.arpa.      IN      PTR     ubup.aula.izv.
212.110.168.192.in-addr.arpa.      IN      PTR     winp.aula.izv.
110.110.168.192.in-addr.arpa.      IN      PTR     profe.aula.izv.
```

En los archivos de zona puede usarse expresiones del tipo $TTL 86400. Esto permite especificar un valor de TTL por defecto para todos los registros. También se puede usar el carácter "@" como sustituto del nombre de la zona definida en named.conf.local para no tener que repetirla en el archivo.

Después de reiniciar el servicio y comprobar que no hay errores, deberíamos configurar los clientes para que usen como servidor DNS la máquina en donde hemos instalado y configurado el servidor.

- Servidor DNS como secundario para una zona de resolución directa y una zona de resolución inversa.

En el servidor que se configure como esclavo para una zona debe editarse su archivo /etc/named.conf.local e indicar el nombre de la zona (*zone*), el tipo de servidor (*type slave*), cual es el servidor maestro del que recibirá la transferencia (*masters*), y el archivo donde se almacenarán los registros de recursos que se reciban (*file*).

Por ejemplo, si el equipo donde se va a configurar un servidor esclavo para una zona de resolución directa fuera profe.aula.izv con IP 192.168.110.110, escribiríamos en /etc/named.conf.local de este servidor:

```
zone "aula.izv" {
        type slave;
        masters { 192.168.110.211; };
        file "/etc/bind/db.aula.izv";
        };
```

En el archivo /etc/named.conf.local del servidor maestro de la zona, deberemos indicar que se permitan transferencias de zona hacia el servidor esclavo (*allow-transfer*), y además se puede configurar para que notifique a los servidores esclavos los cambios que se produzcan en el maestro (*notify*).

```
zone "aula.izv" {
        type master;
        file "/etc/bind/db.aula.izv";
        allow-transfer { 192.168.110.110; };
        notify yes;
        };
```

Por último, en el archivo de zona del servidor maestro, se debe indicar la existencia de otro servidor DNS para la zona, añadiendo para ello un nuevo registro NS con el nombre de dominio del esclavo:

```
. . .
aula.izv.       IN      NS      profe.aula.izv.     ; servidor esclavo
. . .
```

13. Servidores DNS en Windows.

La instalación del servicio DNS se puede realizar desde el botón "Inicio" - > "Panel de Control" - > "Agregar o quitar programas" -> "Agregar o quitar componentes de Windows". Como resultado de la acción anterior, pasa a ser mostrada la ventana del "Asistente para componentes de Windows", en la que nos situaremos sobre el apartado "Servicios de red", y tras ello pulsaremos sobre el botón "Detalles".

En la nueva ventana mostrada, activaremos la casilla correspondiente al apartado "Sistema de nombres de dominio (DNS)", y tras ello pulsaremos sobre el botón "Aceptar", y de vuelta a la ventana anterior, sobre el botón "Siguiente". En ese instante comienza la instalación del servicio DNS de "Windows 2003 Server".

El proceso de instalación nos solicitará el CD de "Windows 2003 Server". Terminada la instalación, en las "Herramientas Administrativas" del "Panel de Control" dispondremos de una nueva entrada "DNS", correspondiente al servidor DNS recién instalado.

Otra posibilidad para realizar el proceso de instalación es desde "Herramientas Administrativas", y seleccionar “Administre su servidor”. En la parte superior de la ventana que aparece deberíamos activar el enlace “Agregar o quitar función”. Esto lanzará un asistente donde podremos elegir de una lista de servicios el “Servidor DNS”.

Si en algún momento se lanza un asistente para crear una zona, cancelaremos esta opción ya que crearemos las zonas necesarias posteriormente.

Si ejecutamos desde “Herramientas administrativas” la consola de administración del servidor DNS, aparecerá una ventana de administración dividida en dos partes. En la parte izquierda aparecen los equipos con servicios DNS a administrar. En principio aparece nuestra máquina, pero podríamos administrar otros servidores (icono DNS, opción “Conectar con el servidor DNS” del menú contextual).

Para cada servidor se puede gestionar las zonas de resolución directa e inversa expandiendo el icono que representa el servidor. En nuestro caso no existe ninguna zona, pero las crearemos luego.

- Servidor DNS como solo caché.

Por defecto el servidor DNS está configurado como sólo caché (no está autorizado para ninguna zona) y responde a consultas recursivas. Podemos comprobarlo seleccionado las propiedades del servidor, y en la ventana que aparece, en la ficha “Sugerencias de raíz” se presenta una lista con los FQDN y direcciones IP de los 13 servidores DNS raíz.

Para ver las búsquedas que están en caché, se debe activar “Avanzadas” de la opción “Ver” de la barra de menú principal. Si acabamos de instalar el servicio DNS, la carpeta “Búsquedas en caché” estará vacía. Si configuramos un cliente indicándole como servidor DNS el que hemos instalado, y preguntamos por un nombre de dominio, por ejemplo, *nslookup* *www.google.es*, podremos comprobar como la información obtenida se queda almacenada en la caché del servidor.

- Servidor DNS para que reenvíe las consultas a reenviadores (*forwarding*).

En las propiedades del servidor, pestaña "Reenviadores" podemos configurar la IP del servidor DNS al que se le reenviará la consulta cuando se pregunte por un dominio concreto o por cualquier dominio (opción por defecto), en vez de consultar a los servidores raíz.

- Servidor DNS como maestro para una zona de resolución directa y una zona de resolución inversa.

Lo primero será configurar, si no lo está ya, el sufijo DNS del equipo. Se establece en propiedades de Mi PC, pestaña "Nombre de equipo", botón "Cambiar", botón "Más …", en "sufijo principal del equipo". (Por ejemplo *aula.izv*). Este sufijo se añadirá automáticamente al nombre del equipo cuando usemos el nombre del equipo sin indicar un dominio.

La manera más cómoda de configurar el servidor DNS como maestro para una zona de resolución directa y una zona de resolución inversa, es crear primero ambas zonas pero sin añadir registros a la zona directa hasta que no esté creada la zona inversa. Cuando añadamos los registros a la zona de resolución directa, indicaremos que se crean de forma automática los correspondientes *PTR* en la zona inversa.

A continuación vamos a definir una nueva zona de búsqueda directa gestionada por nuestro equipo, para lo cual pulsamos sobre el icono "+" mostrado junto al icono del equipo, y tras ello nos ubicamos sobre la carpeta "Zonas de búsqueda directa", pulsando en la misma con el botón derecho del ratón para elegir la opción "Zona nueva..." en el desplegable correspondiente.

Como resultado pasa a ejecutarse el asistente de creación de nueva zona, en cuya primera ventana debemos seleccionar "Zona principal". A continuación debemos indicar el nombre que vamos a asignar a la nueva zona definida y el nombre del archivo de disco donde se almacenará los datos de la zona.

Luego hemos de indicar como se realizarán las actualizaciones de nuestro servidor DNS; en nuestro caso dejaremos activada la opción "No admitir actualizaciones dinámicas". Esto obligará a actualizar manualmente los registros de recursos. Para concluir la definición de la nueva zona creada, pulsaremos sobre el botón "Finalizar".

Al pulsar en la zona, deberá aparecer una lista con los registros definidos en esta zona. En su creación se definen tres registros por defecto: *SOA* (registro de autoridad) *NS* (servidor DNS) y *A* (Address).

Para crear la zona de resolución inversa, deberemos seguir de forma análoga los pasos anteriores hasta llegar al punto en que el asistente nos preguntará por el "Id. de red" (parte de la dirección IP que corresponde a la red, pero sin utilizar el orden inverso). Seguidamente indicaremos el nombre del archivo de disco que almacenará los datos de la zona y la opción "No admitir actualizaciones dinámicas". Cuando pulsemos el botón finalizar, se creará la zona inversa.

Al pulsar en la zona, deberá aparecer una lista con los registros definidos en esta zona. En su creación se definen dos registros por defecto: *SOA* (registro de autoridad) y *NS* (servidor DNS).

Ahora ya podemos añadir registros a las zonas. Para ello hay que seleccionar la zona y pulsar en la opción del menú principal "Acción" y elegir de la lista el tipo de registro a añadir.

Para cualquier tipo de registro creado, podemos realizar modificaciones a través de la opción "Propiedades" de su menú contextual.

Siempre que se creen o se realicen modificaciones en el servidor, deberemos reiniciar el servicio. Para ello, en el menú contextual del icono que representa al servidor, se elige la opción "Todas la tareas" y luego "Reiniciar".

14. Configuración de clientes.

14.1. Clientes Linux.

***Importante**. En Ubuntu, la configuración de las interfaces de red debe siempre realizarse a través de la misma aplicación. Podemos usar la aplicación Network Manager, o los comandos ifconfig o ip. También es factible editar el archivo de configuración /etc/network/interfaces. No se deben mezclar dichos modos por que se producen configuraciones inconsistentes.*

Por ejemplo, datos típicos de la interfaces de red en un archivo /etc/network/interfaces serían:

```
# the loopback network interface
auto lo
iface lo inet loopback

# the primary network interface
auto eth0
iface eth0 inet static
        address 192.168.110.212
        netmask 255.255.255.0
        gateway 192.168.110.254
        broadcast 192.168.110.255
```

Si hacemos algún cambio, siempre deberemos reiniciar el servicio de red y posteriormente ejecutar el comando *ifconfig* para verificar la configuración.

```
$ /etc/init.d/networking restart
```

La configuración de los clientes DNS usando los archivos de configuración se realiza básicamente editando los archivos etc/nsswitch.conf y /etc/resolv.conf

- etc/nsswitch.conf. En este archivo se define el orden que usará el *resolver* a la hora de buscar información sobre nombres de dominio. El orden por defecto es: primero *files* (se consulta en el archivo */etc/hosts*) y luego *dns* (se consulta a los servidores DNS definidos en /etc/resolv.conf).
- etc/resolv.conf. Este archivo contiene una serie de atributos a los que se puede asociar valores. El atributo *nameserver* indica los servidores DNS que consultará el resolvedor. El atributo *domain* especifica el dominio por defecto al que pertenece la máquina y el que se añadirá a la búsqueda de nombres no cualificados. El atributo *search* permite ampliar la lista de dominios que se añadirán a los nombres de dominio en las búsquedas de nombres no cualificados, los llamados sufijos. Las opciones *domain* y *search* no pueden usarse simultáneamente. Por ejemplo:

  ```
  nameserver 192.168.110.211
  nameserver 8.8.8.8
  search aula.izv
  ```

Si usamos la aplicación *Network Manager*, desde ajustes de IPv4 de las propiedades TCP/IP del adaptador de red (Sistema -> Preferencias -> Conexiones de red) podremos editar en los correspondientes cuadros de texto tanto las IP de los servidores DNS (se escriben uno detrás de otro separados por comas), como el dominio de búsqueda al que pertenece la máquina. *Network Manager* guarda los datos de configuración en /etc/NetworkManager/system-connections/nombre-de-la-conexión.

Es conveniente editar el archivo /etc/hostname y comprobar que contiene el nombre que realmente queremos para el equipo.

14.2. Clientes Windows.

En los clientes Windows la configuración de red se establece a través de las propiedades del protocolo TCP/IP que se activa mediante las propiedades de la "Conexión de área local". En "Usar las siguientes direcciones de servidores DNS" es posible definir dos servidores DNS. El segundo servidor DNS que señalemos, será un servidor alternativo en el caso de que el primero de ellos no esté disponible.

En "Opciones avanzadas", en la pestaña "DNS" se pueden añadir más servidores DNS alternativos, y varios sufijos para los nombres DNS no cualificados. Por defecto el único prefijo que se añade a los nombres no cualificados es el llamado sufijo principal que se configura en las propiedades del nombre del equipo (Equipo o MiPc -> Propiedades -> Configuración avanzada del sistema - > Pestaña Nombre de equipo -> botón Cambiar -> Botón Más -> sufijo DNS principal del equipo). Si se desea añadir más

sufijos al nombre del equipo, habrá que habilitar el botón de opción "Anexar estos sufijos (en este orden)" e introducir la lista de sufijos.

El comando **ipconfig /displyadns** permite ver el contenido de la caché de resolución de un cliente DNS, incluyendo las entradas cargadas previamente desde el archivo hosts local, así como los registros de recursos obtenidos recientemente para las consultas de nombres que han sido resueltas.

El comando **ipconfig /flushdns** permite vaciar el contenido de la caché de resolución de un cliente DNS. Al restablecer la caché no se eliminan las entradas que se cargan previamente del archivo hosts local. Para eliminar estas entradas de la caché, habría que eliminarlas del archivo hosts.

15. Herramientas de consulta.

Los comandos *nslookup*, *dig* y *host* permiten comprobar el funcionamiento del servicio DNS y de los servidores DNS. El comando *nslookup* es más antiguo y ofrece menos información que *dig*, pero está disponible en equipos Linux y Windows.

- **nslookup**. De forma general obtiene registros de recursos tipo A o PTR, pero dispone de opciones para obtener otros tipos de informaciones. Puede funcionar en línea de comandos o de forma interactiva. El comando actúa de una forma predeterminada según se haya establecido mediante unos parámetros, los cuales podemos cambiarlos. Esta lista de parámetros se pueden obtener invocando el comando seguido del argumento *-all*.

  Ejemplos de uso en línea de comandos:

  ```
  # obtiene la dirección de un nombre de dominio (pregunta al servidor DNS configurado en el equipo)
  nslookup www.mec.es

  # obtiene la dirección de un nombre de dominio preguntando al servidor DNS especificado
   nslookup www.mec.es a.nic.es

  # obtiene el nombre de dominio correspondiente a la IP
  nslookup 150.214.20.1

  # obtiene todos los tipos de registros de un dominio
  nslookup -type=ANY mec.es

  # obtiene el registro SOA del dominio
  nslookup -type=SOA example.com
  ```

  Cuando se usa de forma interactiva (sin argumentos) aparece un indicador de órdenes (>) donde se puede ir escribiendo comandos. Se sale con "exit" o bien Ctrl+C (Windows) o Crtl+D (Linux). Las posibles órdenes que se pueden ejecutar dependen del sistema operativo, algunas son comunes a Windows y a Linux, y otras sólo funcionan en uno de ellos.

  Con unos ejemplos veremos las posibilidades:

  ```
  # indicamos el servidor a quien se le preguntará y luego se le pregunta por los servidores autorizados para ugr.es
  nslookup
  > server 8.8.8.8
  > set type=NS
  > ugr.es
  # indicamos el servidor a quien se le preguntará y preguntamos por el nombre de dominio correspondiente a la IP
  nslookup
  > server a.nic.es
  > set type=PTR
  > 150.214.20.1
  ```

- **dig**. Este commando ofrece más opciones y suministra más información en sus respuestas que *nslookup*. Organiza la información en secciones que se corresponden con los campos principales de los mensajes DNS. Los registros de recursos los muestra con un formato similar a como se escriben en los archivos de zona.

  El formato (simplificado) es el siguiente:

  ```
  dig [@dns] domain [question-type]
  ```

  donde *dns* especifica el servidor de dominio al que se le realizará la consulta; *domain* indica el nombre de dominio a preguntar, y *question-type* expresa el tipo de recurso consultado. Ejemplos:

```
#por defecto se obtiene la IP correspondiente al nombre del dominio (question-type: A)
dig www.mec.es

#obtiene el nombre de dominio correspondiente a la dirección IP
dig –x 8.8.4.4

# pregunta al servidor 8.8.8.8  por el nombre del dominio (question-type: A) mostrando la traza de la consulta
dig @8.8.8.8 www.google.es +trace

#pregunta al servidor 8.8.8.8 por los servidores autorizados para el dominio es. (question-type: NS)
dig @8.8.8.8 es NS

# pregunta al servidor 8.8.8.8 por todos los registros de recursos del dominio mec.es. (question-type: ANY)
dig @8.8.8.8 mec.es ANY
```

- **host**. Es un comando Linux cuyo formato simplificado es:

```
host [options] name [server]
```

donde *options* indica entre otras cosas el tipo de recurso a preguntar, *name* es el nombre de dominio por el que se consulta *y server* es el servidor de dominio consultado. Ejemplo:

```
#obtiene la IP correspondiente al nombre del dominio (registro tipo A)
host www.mec.es

#obtiene la dirección IP correspondiente al nombre de dominio (registro tipo PTR)
host 8.8.4.4

#pregunta al servidor 8.8.8.8 por los servidores autorizados (registro tipo NS) para el dominio  "es"
host  -t NS es 8.8.8.8

# pregunta al servidor 8.8.8.8 por todos los registros de recursos (registro tipo ANY) del dominio "mec.es" con
# información detallada en secciones (verbose)
host –v –t  ANY mec.es 8.8.8.8
```