DNS

Domain Name System

DNS

Servidores de nombres

Los servidores de nombres, también llamados servidores DNS, son programas que guardan información sobre nombres de dominio y responden a las preguntas que les realizan los clientes DNS y otros servidores de nombres. Almacenan, por lo tanto, una parte de la base de datos DNS.

Por defecto escuchan peticiones en los puertos 53/TCP y 53/UDP.

DNS

Zonas

Los servidores de nombres mantienen información de una parte del espacio de nombres de dominio que se conoce como **zona**. Cuando un servidor de nombres contiene una zona se dice que es autorizado (authoritative) para esa zona (el servidor de DNS del Instituto ASIR es autorizado para la zona "asir.es.").

Las zonas se almacenan en **ficheros de texto** o en bases de datos (en tablas relacionales, en un directorio LDAP, etc.), dependiendo del tipo de servidor usado y de cómo se configure. Su formato está definido en la **RFC 1035**.

En la imagen siguiente se puede observar una parte del fichero de zona del dominio "asir.es.". Cada una de las líneas del fichero es lo que se conoce como **registro de recursos (RR, Resource Records)**.

DNS

Según el tipo de información que se asocie con un nombre de dominio se utiliza un tipo de registro de recursos (por ejemplo, un registro de tipo **A** permite asociar una dirección IP con un nombre de dominio y un registro **NS** permite definir un servidor DNS autorizado para la zona).

Cuando un servidor DNS es autorizado para una zona es responsable de los nombres de dominio de la misma. El servidor DNS del Instituto ASIR que es autorizado para la zona "asir.es" , y por lo tanto en él se define los nombres que "cuelgan" de "asir.es" como por ejemplo "ftp.asir.es", "asterix.asir.es", etc.

Fichero de zona de resolución directa del dominio **asir.es.** que se almacena en un servidor DNS que está en el equipo con IP **193.100.200.100** y cuyo nombre es **ns1.asir.es.**

```
...
asir.es.              IN      NS      ns1.asir.es.
ns1.asir.es.          IN      A       193.100.200.100
obelix.asir.es.       IN      A       193.100.200.101
asterix.asir.es.      IN      A       193.100.200.102
www.asir.es.          IN      CNAME   obelix.asir.es.
ftp.asir.es.          IN      CNAME   asterix.asir.es.
...
```

DNS

La organización que administra el servidor de nombres y por lo tanto la zona puede decidir si delega o no alguno de sus subdominios.

En las Figuras 3.9 y 3.10 se puede observar como el instituto ha delegado el subdominio "redes. asir. es .", en los profesores de redes. Existirá otro servidor DNS que sea autorizado para el dominio "redes. asir. es . ", y que almacene el fichero de zona del dominio. Sin embargo, el sub dominio "bbdd. asir. es", no se ha delegado.

Una zona no es lo mismo que un dominio. Un dominio es un subárbol del espacio de nombres de dominio. Los datos asociados a los nombres de un dominio pueden estar almacenados en una o varias zonas distribuidas en uno o varios servidores DNS.

DNS

La organización que administra el servidor de nombres y por lo tanto la zona puede decidir si delega o no alguno de sus subdominios. En las imagenes se puede observar como el instituto ha delegado el subdominio "redes. asir. es .", en los profesores de redes. Existirá otro servidor DNS que sea autorizado para el dominio "redes. asir. es . ", y que almacene el fichero de zona del dominio. Sin embargo, el sub dominio "bbdd. asir. es", no se ha delegado.

Fichero de zona de resolución directa del dominio **asir.es.** que se almacena en un servidor DNS que está en el equipo con IP **193.100.200.100** y cuyo nombre es **ns1.asir.es.**

```
…
asir.es.              IN     NS     ns1.asir.es.
ns1.asir.es.          IN     A      193.100.200.100
obelix.asir.es.       IN     A      193.100.200.101
asterix.asir.es.      IN     A      193.100.200.102
www.asir.es.          IN     CNAME  obelix.asir.es.
ftp.asir.es.          IN     CNAME  asterix.asir.es.

;Subdominio redes.asir.es. delegado

redes.asir.es.        IN     NS     ns1.redes.asir.es.
ns1.redes.asir.es.    IN     A      193.100.40.100

;Subdominio bbdd.asir.es. NO delegado

www.bbdd.asir.es.     IN     A      193.100.110.200
pc01.bbdd.asir.es.    IN     A      193.100.110.101
pc02.bbdd.asir.es.    IN     A      193.100.110.102
...
```

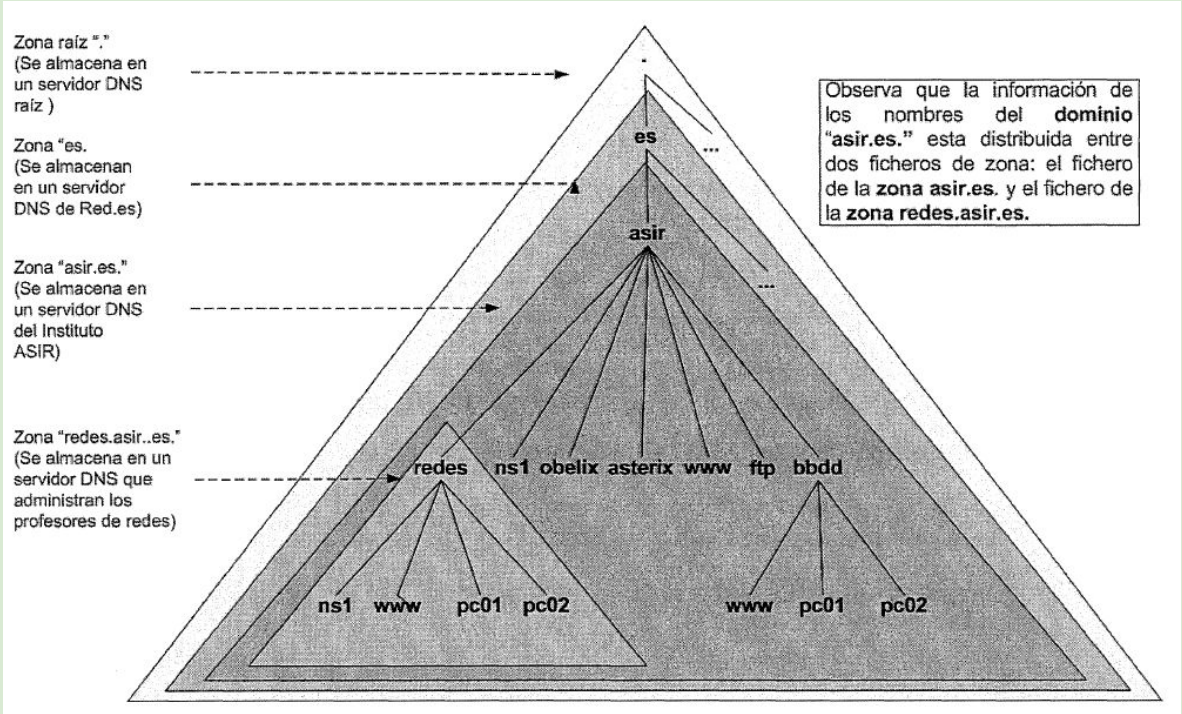
Fichero de zona de resolución directa del dominio **redes.asir.es.** que se almacena en un servidor DNS que está en el equipo con IP **193.100.40.100** y cuyo nombre es **ns1.redes.asir.es.**

```
…
redes.asir.es.        IN     NS     ns1.redes.asir.es.
ns1.redes.asir.es.    IN     A      193.100.40.100
www.redes.asir.es.    IN     A      193.100.40.200
pc01.redes.asir.es.   IN     A      193.100.40.101
pc02.redes.asir.es.   IN     A      193.100.40.102
...
```

DNS

Una zona no es lo mismo que un dominio. Un dominio es un subárbol del espacio de nombres de dominio.

Los datos asociados a los nombres de un dominio pueden estar almacenados en una o varias zonas distribuidas en uno o varios servidores DNS.



DNS

Un servidor de nombres puede tener autoridad sobre varias zonas (por ejemplo, el mismo servidor puede ser autorizado para la zona "asir.es" y para la zona "informatica.es").

Supongamos que el servidor autorizado para la zona "asir.es", tiene un problema y deja de estar activo, ¿qué pasaría cuándo los clientes DNS le preguntasen?, y si el servidor autorizado para "google.com" recibe tantas preguntas que responde lentamente, ¿qué ocurriría cuando un los usuarios de Internet pusiese en el navegador www. google. com y tuviesen que esperar varios segundos?

Para evitar este tipo de problemas y mejorar el funcionamiento del servicio, DNS permite almacenar una misma zona en varios servidores DNS, ofreciendo así balanceo de carga, rapidez y una mayor tolerancia a fallos. Teniendo en cuenta esto es posible distinguir entre zonas maestras o primarias y zonas esclavas o secundarias.

DNS

Tipos de servidores de nombres

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

- Servidor maestro o primario.
- Servidor esclavo o secundario.
- Servidor cache.
- Servidor reenviador (forwarding).
- Servidor solo autorizado.

Es muy importante tener en cuenta que un mismo servidor DNS puede combinar varias de estas funciones simultáneamente (por ejemplo, un servidor DNS puede ser simultáneamente maestro para una zona, secundario para otra zona y actuar como cache).

DNS

Servidor maestro (o primario)

Un servidor DNS maestro (también denominado primario o principal) define una o varias zonas para las que es autorizado. Sus archivos de zona locales son de lectura y escritura, y es en ellos donde el administrador añade, modifica o elimina nombres de dominio.

- Si un cliente DNS u otro servidor DNS le pregunta por un nombre de dominio para el que es autorizado, consulta con los ficheros de zona y responde a la pregunta.
- Si un cliente DNS u otro servidor DNS le pregunta por un nombre de dominio para el que el que no es autorizado, tendrá que buscar la información en otros servidores DNS o responder que no conoce la respuesta.

DNS

Servidor esclavo (o secundario)

Un servidor esclavo (también denominado secundario) define una o varias zonas para las que es autorizado.

La diferencia con un maestro es que **obtiene los ficheros de zona de otro servidor autorizado para la zona** (normalmente un servidor maestro) mediante un proceso que se denomina **transferencia de zona**.

Los ficheros de zona del servidor esclavo son solo de lectura, y por lo tanto, el administrador no tiene que editar estos ficheros. La modificación de los ficheros de zona debe realizarse en el servidor maestro.

El funcionamiento ante las respuestas de los clientes es similar al de un servidor maestro.

La definición de maestro o esclavo se determina a nivel de zona, así, un servidor DNS puede ser maestro para una o varias zonas y al mismo tiempo esclavo para otras.

DNS

Pueden existir varios servidores esclavos para una misma zona. Las principales razones para su implantación son:

- Reducir y repartir la carga entre varios servidores.
- Favorecer la tolerancia a fallos (al menos un servidor primario y un secundario para cada zona).
- Ofrecer respuestas más rápidas.

Lo ideal es que los servidores DNS de una zona estén ubicados en redes y localizaciones diferentes para evitar que un problema (por ejemplo, un fallo eléctrico o un ataque de denegación de servicio) les afecte simultáneamente y deje sin servicio de resolución a los nombres de dicha zona.

DNS

Servidor caché

El proceso de resolución de nombres es costoso ya que utiliza los recursos de la red y los recursos de los equipos que ejecutan los servidores y los clientes. Para mejorar los tiempos de respuesta de las consultas, reducir la carga de los equipos y disminuir el tráfico de red, los servidores de nombres pueden actuar como servidores caché.

Cuando un servidor DNS recibe una pregunta sobre un nombre de dominio de una zona para la que no es autorizado, es decir, de un nombre del que no tiene información, puede preguntar (si así se ha configurado) a otros servidores para que le den la respuesta.

Si el servidor actúa como caché guarda durante un tiempo (**TTL, Time To Live**) las respuestas a las últimas preguntas que ha realizado a otros servidores de nombres. Cada vez que un cliente DNS u otro servidor DNS le formula una pregunta, consulta en primer lugar en su memoria caché, ahorrándose la pregunta a otros servidores si ya la había hecho anteriormente.

Un servidor de nombres es solo caché (caching only server) cuando:

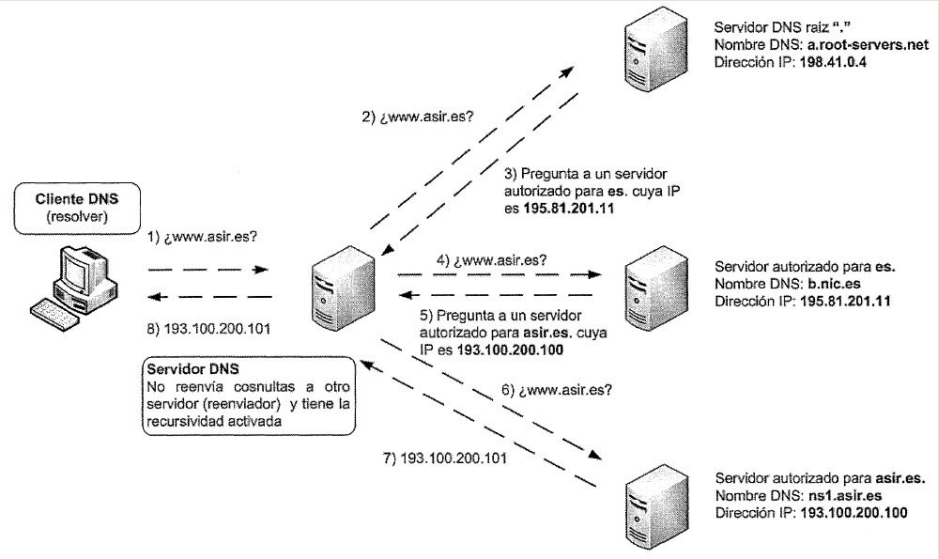
- No tiene autoridad sobre ningún dominio.
- Pregunta a otros servidores para resolver las peticiones de los clientes DNS y guarda las respuestas en caché.

DNS

Servidor reenviador (forwarder)

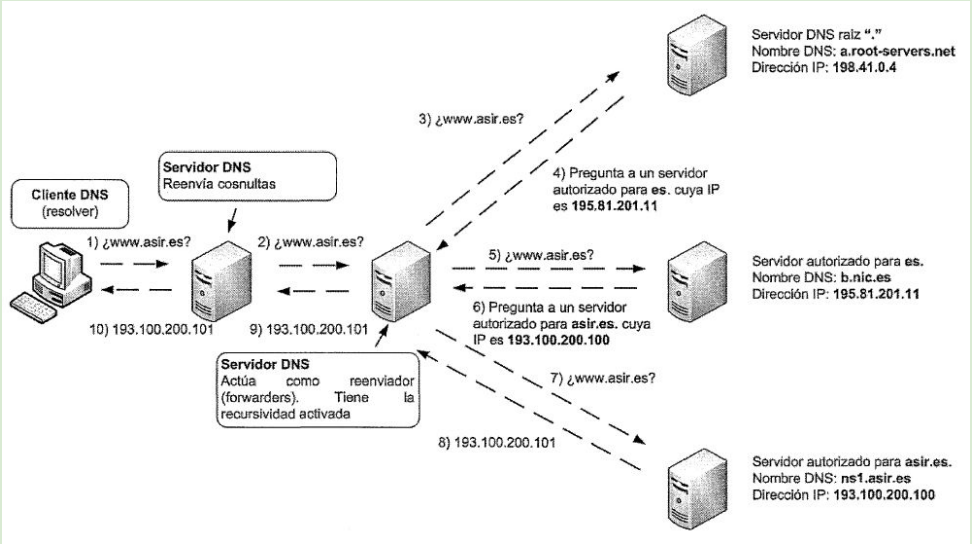
Cuando un servidor DNS recibe una pregunta sobre un nombre de dominio del que no dispone información puede preguntar a otros servidores DNS. Por ahora vamos a distinguir entre dos posibilidades:

- Se encarga de procesar la consulta preguntando a diversos servidores DNS y empezando por los servidores DNS raíz.



DNS

- Reenvía la consulta a otro servidor DNS, que se denomina reenviador (forwarder), para que se encargue de resolverla



Por lo tanto, un reenviador es un servidor DNS que otros servidores DNS designan para reenviarle consultas. Se utilizan para minimizar las consultas y el tráfico de peticiones DNS desde una red hacía Internet. Además permite a los equipos locales compartir la caché DNS del reenviador minimizando los tiempos de respuesta.

DNS

Servidor solo autorizado

El término solo autorizado (authoritative only) se usa para describir un servidor que:

- Es autorizado para una o varias zonas como maestro y/o esclavo.
- No responde a preguntas que no sean relativas a sus zonas, es decir, no pregunta a otros servidores DNS. Esto implica que no tiene activada la **recursividad**, no es **reenviador** y no actúa como **caché**.

DNS

Ejemplos de servidores de nombres

Existen múltiples servidores DNS tanto para sistemas libres como para sistemas propietarios.

Algunos de los más utilizados son:

- BIND
- Servidor DNS de Microsoft
- PowerDNS
- NSD
- Knot DNS
- Cisco Network Registrar
- dnsmasq

DNS

Servidores raíz (root servers)

Existen en Internet un conjunto de servidores DNS autorizados para el dominio raíz ".", conocidos como servidores raíz (mot servers). Contienen, por lo tanto, el fichero de la zona "." que almacena cuáles son los servidores DNS autorizados para cada uno de los dominios TLD.

Los servidores raíz están bajo la responsabilidad de la ICANN, pero son operados por un consorcio de organizaciones. El RSSAC (Root Servers Systems Advisory Committee) proporciona asesoramiento en su administración. "Existen 12 servidores raíz" y cada uno de ellos tiene múltiples copias distribuidas por todo el mundo (es decir, que realmente no existen solo 12).

Cada grupo, cada conjunto de copias de uno de los 12, se identifica por una misma IP. Cuando un cliente realiza una pregunta a una IP de un servidor raíz, ten en cuenta que esa IP se corresponde realmente con tantos equipos como copias de ese servidor existan, los routers de Internet encaminan la pregunta hacia la copia más cercana mediante un procedimiento denominado anycasting.

https://root-servers.org/

DNS

Clientes DNS (resolvers)

Se puede considerar que un **resolver** es cualquier software capaz de preguntar a un servidor DNS e interpretar sus respuestas.

Los sistemas operativos incluyen o permiten instalar un conjunto de librerías, denominadas **stub resolver**, que realizan estas funciones. Son invocadas por las aplicaciones (navegador web, cliente ftp, ...) cuando se utiliza un nombre de dominio. Si se configuran para ello pueden mantener una caché de respuestas, al igual que los servidores de nombres, para minimizar los accesos a la red e incrementar el rendimiento.

La forma en la que se resuelven nombres de dominio en un sistema operativo es configurable.

En la mayoría de los sistemas hay archivos de texto en donde se pueden asociar direcciones IP con nombres y es posible definir si el resolver mirará en primer lugar en estos archivos para hacer la resolución. También es posible habilitar o no la caché de respuestas.

DNS

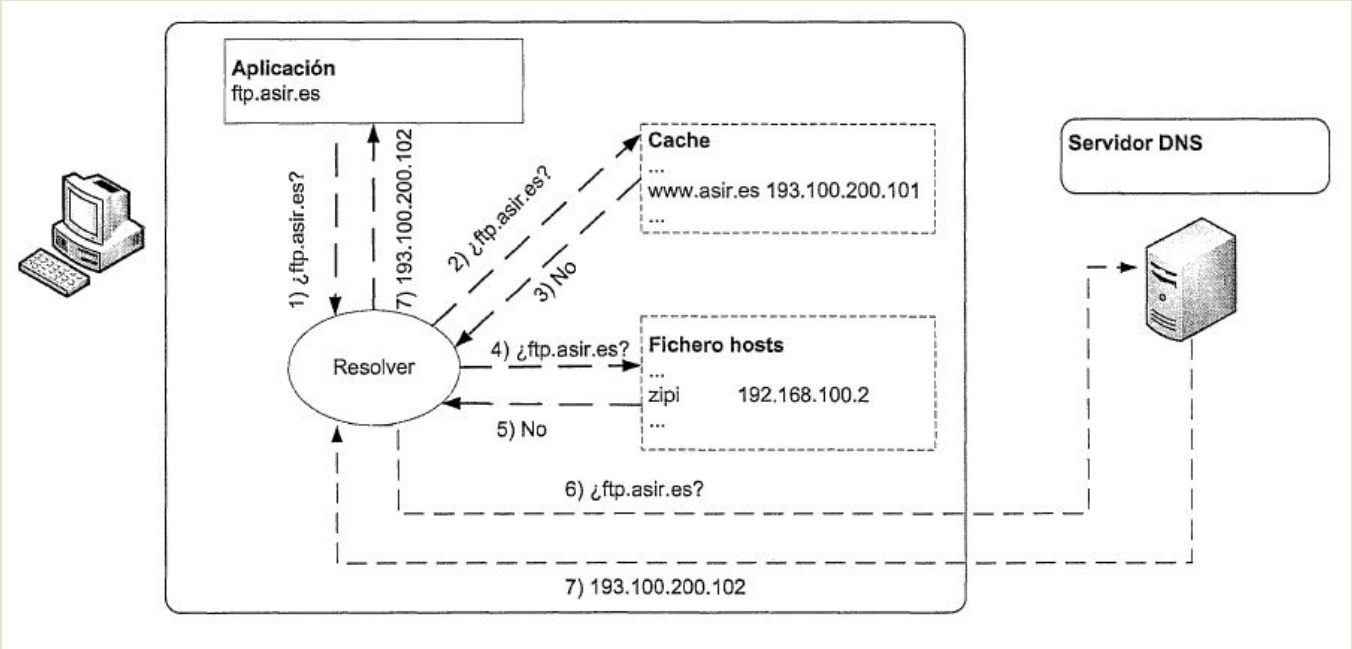
Clientes DNS (resolvers)

Cuando una aplicación quiere resolver un nombre invoca al resolver. A continuación se describe la configuración más habitual, véase:

1. El resolver consulta la caché de resolución de nombres del hosts (si está configurada) (almacenada en memoria). Si obtiene una respuesta positiva se la entrega a la aplicación.
2. Si el nombre buscado no está en la caché, el resolver buscará en el archivo hosts local del equipo. En sistemas Windows el archivo es **%SYSTEMROOT%\system32\drivers\etc\hosts** y en sistemas Linux/Unix el archivo es **/etc/hosts**.
3. Si el nombre buscado no está en el archivo hosts, el resolver efectuará una **consulta recursiva** al servidor de nombres que esté configurado y le entregará la respuesta a la aplicación.

DNS

Clientes DNS (resolvers)



DNS

Proceso de resolución

Las consultas a un servidor DNS pueden ser de dos tipos: recursivas o iterativas.

Consultas recursivas

Una consulta recursiva es aquella en la que el servidor tiene que dar una respuesta completa o exacta. Hay tres posibles respuestas:

- **Respuesta positiva**, es decir, da la información del nombre por el que se ha preguntado. En ella se indica si es autorizada o no. No es posible saber si el servidor que responde con autoridad es maestro o esclavo para el dominio preguntado.
- **Respuesta negativa**, indica que el nombre no se pudo resolver (NXDOMAIN).
- Una **indicación de error** (por ejemplo, que no se puede preguntar a otros servidores por un fallo en la red).

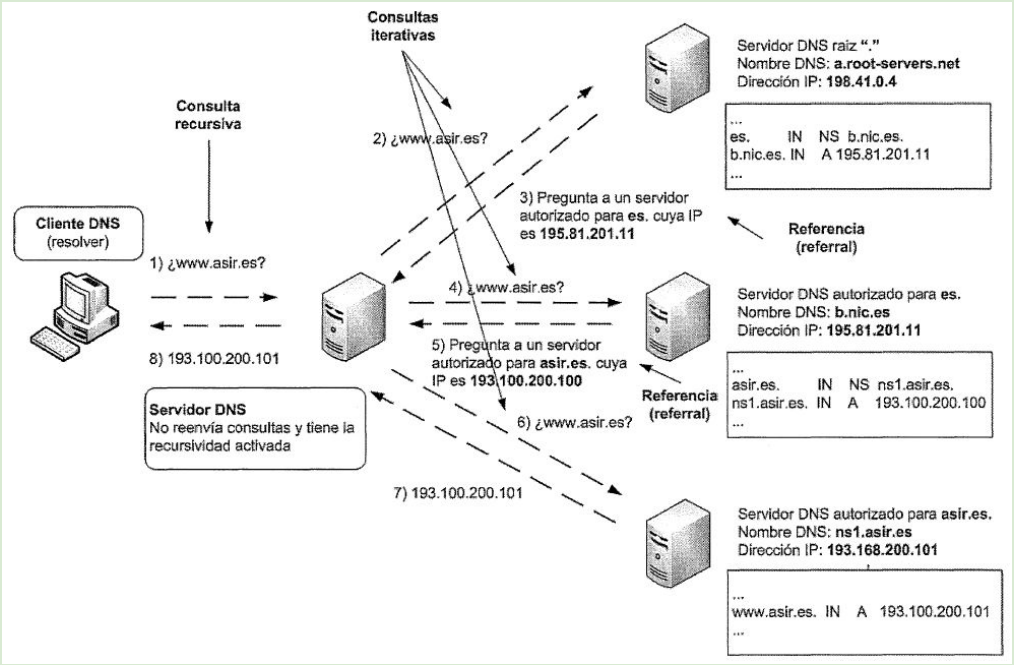
DNS

Cuando un servidor recibe una consulta recursiva:

1. Si es **autorizado** para alguna zona (maestro o esclavo) comprueba sus **archivos de zona.** 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 respuestas anteriores. Si encuentra la respuesta responde indicando que la respuesta no es autoritativa.
3. En otro caso:
    a. Si tiene configurados **reenviadores** entonces reenvía la consulta recursiva a otro servidor DNS. La respuesta que obtenga se la traslada al cliente o al servidor que le preguntó.
    b. Si no tiene configurados reenviadores:
        i. Inicia una serie de **consultas iterativas** a otros servidores DNS.
        ii. Los servidores DNS consultados devuelven referencias (**referrals**) a otros servidores DNS que se usan para realizar otra pregunta.
        iii. La recursividad finaliza siempre cuando un servidor autorizado del espacio de nombres proporcione una respuesta positiva o negativa.

DNS

Ejemplo de resolución DNS



DNS

Ejemplo de resolución DNS

1. El resolver del equipo envía una **consulta recursiva** al servidor DNS. El servidor DNS recibe la pregunta. Como no es autorizado para la zona "asir.es" no tiene en sus archivos de zona el nombre de dominio por el que le han preguntado. No está configurado para reenviar consultas y además actúa como caché, es decir, tiene activada la recursividad, por lo que es capaz de tratar una consulta recursiva. Para resolver la pregunta inicia una serie de consultas iterativas.

2. La primera consulta iterativa se la envía a uno de los servidores raíz. El servidor sabe quiénes son los servidores raíz, porque almacena el fichero **hits file**.

3. El servidor raíz que recibe la consulta iterativa responde con una referencia al servidor autorizado para el dominio "es". El servidor raíz ha delegado la autoridad del dominio "es" en otros servidores DNS. Realmente le envía la referencia de todos los que existan, pero en la imagen se ha simplificado mostrando solo uno. Observa que en el fichero de la zona raíz se indica cuál es el servidor autorizado del dominio "es", en el que se delega, con un RR de tipo NS.

4. A continuación el servidor DNS envía una consulta iterativa al servidor autorizado del dominio "es" .

DNS

5. El servidor autorizado para el dominio "es" que recibe la consulta iterativa responde con una referencia al servidor autorizado para el dominio "asir.es". El servidor autorizado para el dominio "es" ha delegado la autoridad del dominio "asir.es", en otros servidores DNS. Realmente le envía la referencia de todos los que existan, pero en la figura se ha simplificado mostrando solo uno. Observa que en el fichero de la zona "es" se indica cuál es el servidor autorizado del dominio "asir.es", en el que se delega, con un RR de tipo NS.

6. Posteriormente, el servidor DNS envía una consulta iterativa al servidor autorizado del dominio "asir.es".

7. El servidor autorizado para el dominio "asir. es", consulta sus ficheros de zona y como existe el nombre de dominio .. www.asir.es .. , responde con la información asociada a él. Si no existiese el nombre en los archivos de zona, respondería de forma negativa indicando que no sabe resolver el nombre.

8. El servidor que recibió la consulta recursiva responde al resolver con la información por la que se le preguntó.

Las consultas recursivas son iniciadas por un cliente DNS (resolver) o por un servidor DNS que reenvía la consulta recursiva a otro servidor (reenviador).

Las consultas recursivas son costosas para los servidores DNS, y por eso es habitual que si un servidor DNS es autorizado para una zona no responda a consultas recursivas. Los servidores DNS raíz y los servidores DNS autorizados para los dominios TLD no responden a consultas recursivas.

DNS

Consultas iterativas

Una consulta iterativa (o no recursiva) es aquella en la que el servidor DNS puede proporcionar una respuesta parcial. Hay cuatro posibles respuestas:

- **Respuesta positiva**, es decir, da la información del nombre por el que se ha preguntado. En ella se indica si es autorizada o no.
- **Respuesta negativa**, indica que el nombre no se pudo resolver (NXDOMAIN).
- Respuesta **indicando una referencia a otros servidores**, autorizados o no, a los que se puede preguntar para resolver la pregunta (una referencia no se es válida como respuesta a una consulta recursiva).
- Una indicación de **error**.

DNS

Cuando un servidor recibe una consulta iterativa:

1. Si es autorizado para alguna zona (maestro o esclavo) comprueba sus archivos de zona. 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 respuestas anteriores. Si encuentra la respuesta responde indicando que la respuesta no es autoritativa.

3. Si no se encuentra respuesta exacta con el nombre, devuelve una referencia que apunta a un servidor DNS que está autorizado para un nivel inferior del espacio de nombres de dominio. Como ya se ha explicado, esta información es usada por el servidor que realizó la consulta iterativa para continuar su proceso de resolución (proceso recursivo).

Las consultas iterativas son realizadas por servidores a otros servidores DNS después de haber recibido una consulta recursiva (y no encontrar respuesta en sus archivos de zona o cache').

DNS

Caché y TTL

Ya se ha explicado que los clientes y los servidores DNS mantienen en memoria caché, si están configurados para ello, las respuestas a las preguntas que realizan a otros servidores. El tiempo que guardan las respuestas en caché se denomina TTL (Time To Live) y se define en los archivos de zona de los servidores DNS preguntados.

Los clientes y servidores DNS almacenan en caché:

- Respuestas positivas. Registros de recursos de nombres resueltos.
- Respuestas negativas. Información de que no existen registros de recursos para un nombre consultado. Impiden la repetición de solicitudes adicionales para nombres que no existen.

En los ficheros de zona se define el tiempo que se guardarán en caché las respuestas positivas y el tiempo que se guardan en caché las respuestas negativas. Por lo tanto, se diferencia entre TTL de respuestas positivas y TTL de respuestas negativas.

La RFC 1912 recomienda que el valor TTL positivo sea de 1 día o mayor, y para los registros de recursos que cambien poco se usen valores de 2 o 3 semanas. La RFC 2308 indica que el máximo valor del TTL negativo sea de 3 horas.

DNS

Resolución inversa

Ahora que ya se ha explicado el funcionamiento del servicio DNS basándose en la resolución directa, vamos a tratar la resolución inversa. Recuerda que una consulta inversa a un servidor DNS consiste en preguntar por una dirección IP en lugar de preguntar por un nombre de dominio. Por ejemplo, la dirección actual de www.microsoft.com es 65.55.206.154. ¿cuáles son los nombres de dominio asociados a esa dirección?

Existen muchos motivos para preguntar por los nombres de dominio asociados a una IP, por ejemplo, resolver problemas de red, detectar spam en los servidores de correo, seguir la traza de un ataque, conocer qué nombres aloja un servidor de hosting, etc.

DNS

Mapeo de direcciones IP y dominio arpa

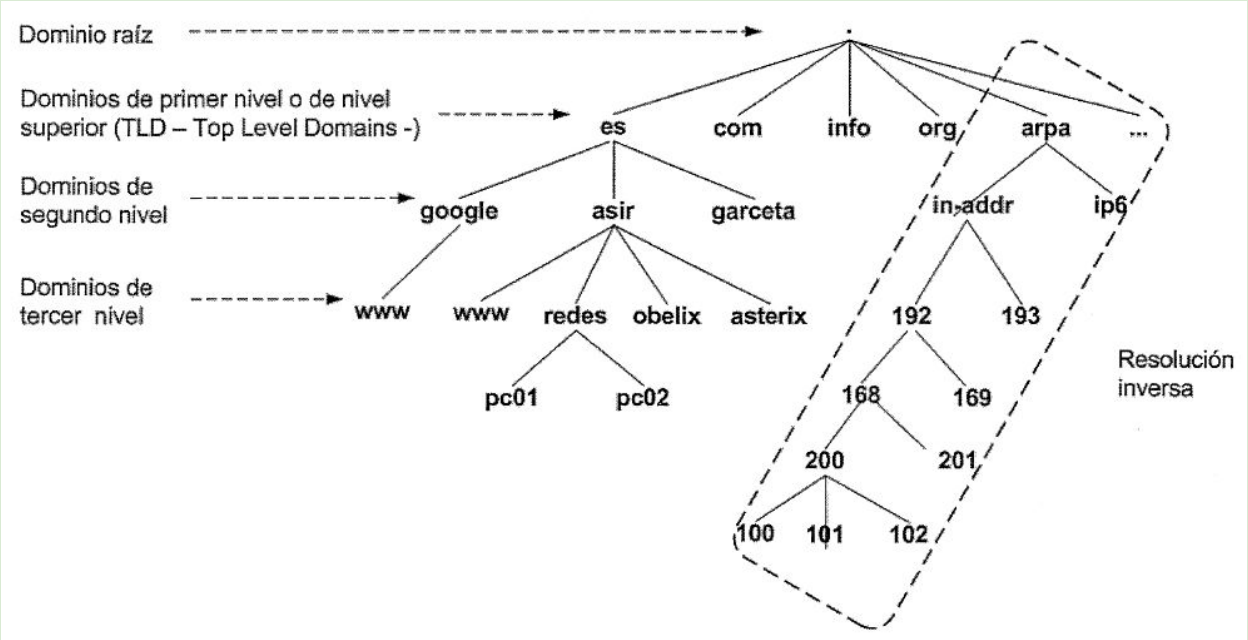
La resolución de direcciones IP funciona igual que la resolución de nombres de dominio. Las direcciones IP se tratan como nombres donde cada byte es un dominio que cuelga de los dominios "in-addr. arpa" para direcciones IPv4 , e "ip6. arpa" para las direcciones IPv6.

• Cuando usamos un nombre de dominio, por ejemplo “www.asir.es.” lo leemos y lo escribimos de izquierda a derecha, pero su estructura jerárquica es de derecha a izquierda, el dominio más alto de la jerarquía es el raíz ".", después "es.", después "asir" y por último "www" .

• Cuando usamos una dirección IP para realizar una pregunta DNS inversa, por ejemplo 192.168.200.100, realmente estamos preguntando por el nombre de dominio "100.200.168.192.in-addr.arpa". La estructura jerárquica de la dirección IP tratada como nombre de dominio es de izquierda a derecha y comenzado por el dominio "in-addr.arpa".

DNS

Mapeo de direcciones IP y dominio arpa



DNS

Zonas de resolución inversa

Los servidores de nombres tienen que almacenar zonas de resolución inversa con registros de recursos que asocien nombres de dominio con direcciones IP. Pueden existir zonas de resolución inversa maestras o primarias, y zonas de resolución inversa esclavas o secundarias.

Las zonas directas e inversas son independientes, y es responsabilidad de los administradores que contengan información coherente y que no existan discrepancias. Además, no es obligatorio que un organismo o empresa que administra la zona directa de un dominio tenga que administrar la o las zonas inversas que se corresponden con las direcciones IPs asociadas a los nombres del dominio.

Por ejemplo, si administramos un dominio y asociamos un nombre con una IP pública contratada a un ISP, tendremos que ponernos en contacto con él para que modifique su zona inversa e incluya nuestro nombre de dominio, si queremos que las consultas inversas a esa IP se resuelvan con el nombre correcto que nosotros queremos.

DNS

Zonas de resolución inversa

Fichero de la zona de resolución directa **asir.es.** que permite resolver las consultas directas de los nombres del dominio asir.es.

```
...
asir.es.              IN     NS     ns1.asir.es.
ns1.asir.es.          IN     A      193.100.200.100
obelix.asir.es.       IN     A      193.100.200.101
asterix.asir.es.      IN     A      193.100.200.102
panoramix.asir.es.    IN     A      193.100.200.103
...
```

Fichero de la zona de resolución inversa **200.100.193.in-addr.arpa.**, que permite resolver las consultas inversas sobre direcciones IP de la red **193.100.200.0/24**

```
...
200.100.193.in-addr.arpa.          IN     NS     ns1.asir.es.
100.200.100.193.in-addr.arpa.      IN     PTR    ns1.asir.es.
101.200.100.193.in-addr.arpa.      IN     PTR    obelix.asir.es.
102.200.100.193.in-addr.arpa.      IN     PTR    asterix.asir.es.
133.200.100.193.in-addr.arpa.      IN     PTR    panoramix.asir.es.
...
```

Si un cliente DNS pregunta por el nombre de dominio "obelix.asir.es" el servidor DNS consultará el fichero de resolución directa y devolverá la ip 193.100.200.101.

• Si un cliente DNS pregunta la dirección IP 193.100.200.101 el servidor DNS consultará el fichero de resolución inversa y devolverá el nombre "obelix.asir.es" .

• Si un cliente DNS pregunta por el nombre de dominio "panoramix.asir.es" el servidor DNS consultará el fichero de resolución directa y devolverá la ip 193.100.200.103.

• Si un cliente DNS pregunta la dirección IP 193.100.200.103 el servidor DNS consultará el fichero de resolución inversa y devolverá que no ha encontrado nada. En este caso, la zona de resolución directa e inversa no son coherentes.

• Si un cliente DNS pregunta la dirección IP 193.100.200.133 el servidor DNS consultará el fichero de resolución inversa y devolverá el nombre "panoramix. asir. es". En este caso, la zona de resolución directa e inversa no son coherentes.

DNS

Registros de recursos DNS

Ya sabemos que el servicio DNS gestiona una base de datos distribuida entre múltiples servidores DNS que almacenan ficheros de zona con información sobre nombres de dominio. Cada fichero de zona organiza esta información en **registros de recurso (RR, Resource Records)** los cuales se envían en las preguntas y respuestas entre cliente y servidores DNS.

Formato general

Los RR tienen dos representaciones. La representación textual utilizada en los archivos de zona y la representación en binario, que es la que se emplea en los mensajes del protocolo DNS (definida en la RFC 1035). A continuación se explica la representación textual.

Formato: NombreDeDominio [TTL] Clase Tipo Tipo-Dato

DNS

Formato: NombreDeDominio [TTL] Clase Tipo Tipo-Dato

Ejemplo: obelix.asir.es. 7200 IN A 193.100.200.101

- Nombre de dominio
  - Nombre de dominio con el que se asocia el recurso
  - Ejemplos: obelix.asir.es, 101.200.100.193.in-addr.arpa
- TTL (Time To Live)
  - Número de segundos que puede estar el registro en caché antes de ser descartado.
  - Es opcional a nivel de recurso.
  - Se puede definir un tiempo global que se aplica a todos los registros de una zona.
  - Un TTL de 0 indica que el registro no tiene que ser almacenado en caché.
- Clase
  - Define la arquitectura de protocolos usada.
  - IN para la TCP /IP.
- Tipo
  - Tipo de registro.
  - Son diferentes en función del campo clase.
  - Para el campo IN existen muchos tipos (A, CNAME, NS, MX ...)
- Tipo-Dato
  - Información asociada al nombre de dominio.
  - Varía en función del tipo de registro.
  - Ejemplo: dirección IP para el tipo A.

DNS

Tipos de registros

Registro SOA

El registro SOA (Start Of Authority) es el primer registro de una zona y define una serie de opciones generales de la misma. Los datos asociados con un registro SOA son los siguientes (consulta el apartado relativo a transferencias de zona para relacionarlo con los valores que se definen en este registro):

- MNAME
  - Nombre FQDN del servidor de nombres maestro del dominio.
  - Ejemplo: nsi.asir.es.
- Contacto (contact)
  - Correo de la persona responsable del dominio.
  - Es parecido a una dirección de correo electrónico normal, a excepción que la arroba se remplaza con un punto.
  - Ejemplo: admi.asir.es

DNS

Registro SOA (cont.)

- Numero de serie (serial)
  - Indica la versión del archivo de zona, y debe ser incrementado cada vez que el archivo se modifique.
  - Los servidores secundarios consultan el registro SOA para realizar transferencias de zona. Si ha cambiado, entonces se realiza la transferencia de zona.
  - Una práctica muy común es utilizar la fecha en el formato aaaammdd y agregarle dos dígitos más para los cambios que se hacen al archivo en el mismo día.
  - Ejemplo: 2001032201.
- Actualización (refresh)
  - Tiempo que esperan los servidores esclavos para preguntar al servidor maestro si hay cambios en la zona.
  - La RFC 1912 recomienda valores entre 1200 y 43200 segundos (12 horas) dependiendo de la frecuencia de cambios en los archivos de zona.
  - Si se usan notificaciones (NOTIFY) se puede usar un valor muy alto (1 o más días).

DNS

Registro SOA (cont.)

- Reintentos (retry)
  - Si la transferencia de zona ha fallado, indica el tiempo que espera el servidor secundario
  - antes de volver a intentarlo.
  - Valores inferiores al tiempo de actualización.
- Caducidad (expire)
  - Determina el tiempo que el servidor esclavo puede estar intentando contactar con el maestro para ver si hay cambios de zona.
  - Si el tiempo expira, el servidor esclavo considera que algo ha pasado y se declara como no autorizado para la zona, y por lo tanto, no responde a preguntas sobre esa zona.
  - La RFC 1912 recomienda valores entre 2 y 4 semanas.
- TTL negativo (Time To Live)
  - Tiempo mínimo que se almacenan las respuestas negativas sobre esa zona.
  - Diferente al TTL de los RR.

DNS

Registro SOA (cont.)

```
asir.es.    IN    SOA   ns1.asir.es. admin.asir.es.(
                        1           ; Número de serie
                        604800      ; Tiempo de refresco
                        86400       ; Tiempo de reintento
                        2419200     ; Tiempo de expiración
                        604800 )    ; TTL negativo
```

DNS

Registro NS

El registro de recursos NS (Name Server) permite establecer:

- El/los servidores de nombres autorizados una zona.
  - Cada zona debe contener, como mínimo, un registro NS.
  - Los servidores DNS, pueden tener un nombre de la misma zona o de otras.

```
asir.es.     IN   NS    ns1.asir.es.   ; Servidor DNS maestro
asir.es.     IN   NS    ns2.asir.es.   ; Servidor DNS esclavo
asir.es.     IN   NS    dns.asir.org.  ; Servidor DNS esclavo

ns1.asir.es. IN    A    193.100.200.100
ns2.asir.es. IN    A    193.100.200.200
```

DNS

Registro NS

El registro de recursos NS (Name Server) permite establecer (cont.):

- Quiénes son los servidores de nombres con autoridad en los sub dominios delegados
  - Cada zona debe contener, al menos, un registro NS por cada sub dominio que haya delegado.

```
asir.es.     IN    NS    ns1.asir.es. ; Servidor DNS maestro
asir.es.     IN    NS    ns2.asir.es. ; Servidor DNS maestro
asir.es.     IN    NS    dns.asir.org. ; Servidor DNS esclavo

ns1.asir.es. IN    A     193.100.200.100
ns2.asir.es. IN    A     193.100.200.200

;Delegación
redes.asir.es.     IN    NS    ns1.redes.asir.es. ;Delegación
sistemas.asir.es. IN    NS    dns.asir.org. ;Delegación

ns1.redes.asir.es. IN   A 193.100.40.100 ; GLUE RECORD
```

La parte de derecha de un registro NS no debe ser un nombre de tipo CNAME

DNS

Registro A

El registro de recursos A (Address) establece una correspondencia entre un nombre de dominio completamente cualificado (FQDN) y una dirección IP versión 4.

```
ns1.asir.es.     IN   A     193.100.200.100
ns2.asir.es.     IN   A     193.100.200.200
obelix.asir.es.  IN   A     193.100.200.101
marmita.asir.es.IN   A     193.100.200.101
asterix.asir.es.IN   A     193.100.200.102
```

Registro AAAA

El registro de recursos AAAA (Address Address Address Address) establece una correspondencia entre un nombre de dominio completamente cualificado (FQDN) y una dirección IP versión 6.

```
ns1.asir.es.     IN   A     193.100.200.100
ns2.asir.es.     IN   A     193.100.200.200
obelix.asir.es.  IN   A     193.100.200.101
marmita.asir.es.IN   A     193.100.200.101
asterix.asir.es.IN   A     193.100.200.102
obelix.asir.es.  IN   AAAA  2001:db8::63
asterix.asir.es.IN   AAAA  2001:db8::64
```

DNS

Registro CNAME

El registro de recursos CNAME (Canonical Name) permite crear alias para nombres de dominio especificados en registros A y AAAA.

```
obelix.asir.es.  IN   A     193.100.200.101
www.asir.es.     IN   CNAME obelix.asir.es.
bd.asir.es.      IN   CNAME obelix.asir.es.
```

Un registro CNAME puede apuntar a un nombre de otro dominio.

```
www.asir.es.     IN   CNAME  www.garceta.es.
```

No se deben usar registros CNAME en la parte derecha de registros MX y NS. La parte derecha de estos recursos tiene que ser un nombre que aparezca en un registro de tipo A.

Hay que tener en cuenta que el uso de muchos CNAME perjudica el rendimiento de los servidores DNS. Cuando se pregunta por un registro CNAME hay que buscar dos veces en el fichero de zona para encontrarlo.

DNS

Registro MX

El registro de recursos MX (Mail Exchange) permite definir equipos encargados de la entrega de correo en el dominio. Son consultados por los agentes de transporte de correo SMTP (MTA, Mal Transport Agent).

```
asir.es.    IN    MX    10    mail1.asir.es.
asir.es.    IN    MX    20    mail2.asir.es.

mail1.asir.es.  IN    A       193.100.200.221
mail2.asir.es.  IN    A       193.100.200.222
```

Un registro MX puede apuntar a un nombre de otro dominio.

Es posible definir varios registros MX para un mismo dominio, es decir, varios servidores de correo para ese dominio. En cada registro MX se especifica un número positivo (entre 0 y 65535) que determina la preferencia en el caso de que existan varios registros MX. Un número más pequeño indica mayor preferencia.

La parte de derecha de un registro MX no debe ser un nombre de tipo CNAME.

DNS

Registro SRV

El registro de recursos SRV (Servíces Record) permite definir equipos que soportan un servicio en particular.

```
_http._tcp.asir.es.     IN      SRV     0 5 80   www.asir.es.
_ldap._tcp.asir.es.     IN      SRV     0 0 389  ldap.asir.es.
```

No se explican en detalle los campos de este tipo de registro. Puedes consultar una descripción en la RFC 2782.

DNS

Registro PTR

El registro de recursos PTR (Pointer Record) establece una correspondencia entre nombres de direcciones IPv4 e IPv6 y nombres de dominio. Se utilizan por lo tanto en las zonas de resolución inversa.

En una misma zona no puede haber registros PTR IPv4 y registros PTR IPv6. Existen por lo tanto zonas de resolución inversa IPv4 y zonas IPv6.

```
100.200.100.193.in-addr.arpa.   IN   PTR ns1.asir.es.
200.200.100.193.in-addr.arpa.   IN   PTR ns2.asir.es.
101.200.100.193.in-addr.arpa.   IN   PTR obelix.asir.es.
```

```
$ORIGIN 0.0.0.0.0.0.0.0.0.0.0.1.0.0.0 .0.0.0.0.8.b.d.0.1.0.0.2.IP6.ARPA.

3.6.0.0        IN      PTR     obelix.asir.es.
4.6.0.0        IN      PTR     asterix.asir.es.
```

DNS

Delegación y registros pegamento (Glue Record)

La organización que administra un servidor de nombres, y por lo tanto, sus zonas, puede decidir si delega o no alguno de sus subdominios en otros servidores de nombres. Se puede diferenciar dos casos:

- Si el nombre del servidor DNS autorizado del sub dominio (en el que se delega) se encuentra a su vez dentro del propio subdominio.
    - Hay que añadir un registro NS en la zona del padre que define el servidor de nombres autorizado para la zona delegada.
    - Hay que añadir un registro de tipo A para indicar la dirección IP del servidor de nombres autorizado para la zona delegada.
        - A este tipo de registros se les denomina "**glue record**" porque unen o pegan la zona hija con la zona padre (realmente no pertenecen a la zona padre).
        - Observa que si no se define este registro, el cliente que realiza una pregunta iterativa (por ejemplo pe1.redes.asir.es) y obtiene una referencia al siguiente servidor DNS al que preguntar (ns1.redes.asir.es) no podría obtener la IP del nuevo servidor DNS hasta que no acceda a él (ns1 es un nombre del dominio redes.asir.es). Observa que no puede preguntarle si no sabe su IP (" .. .la pescadilla que se muerde la cola ... ").
    - Si se omiten o se colocan registros de pegamento incorrectos, se dejará parte del espacio de nombres inaccesible.
    - Por lo tanto, los servidores de un dominio padre deben conocer la dirección IP de los servidores de nombres de todos sus subdominios .

DNS

```
asir.es.     IN    NS    ns1.asir.es. ; Servidor DNS maestro
asir.es.     IN    NS    ns2.asir.es. ; Servidor DNS maestro
asir.es.     IN    NS    dns.asir.org. ; Servidor DNS esclavo

ns1.asir.es. IN    A     193.100.200.100
ns2.asir.es. IN    A     193.100.200.200

;Delegación
redes.asir.es.      IN    NS    ns1.redes.asir.es. ;Delegación
ns1.redes.asir.es.  IN    A 193.100.40.100 ; GLUE RECORD
```

DNS

La organización que administra un servidor de nombres, y por lo tanto, sus zonas, puede decidir si delega o no alguno de sus subdominios en otros servidores de nombres. Se puede diferenciar dos casos (cont.):

- Si el nombre del servidor DNS del subdominio (en el que se delega) no se encuentra en el subdominio.
    - Hay que añadir un registro NS en la zona del padre que define el servidor de nombres autorizado para la zona delegada.
    - No hace falta ni hay que añadir un registro de tipo A para indicar la dirección IP del servidor de nombres autorizado para la zona delegada.
        - En este caso, el cliente que realiza una pregunta iterativa (por ejemplo pe1.sistemas.asir.es) y obtiene una referencia al siguiente servidor DNS al que preguntar (dns.asir.org) podrá resolver el nombre dns.asir.org normalmente.
        - Es un error incluir registros de pegamento para nombres de host que no los necesitan. La regla general es que se deben incluir registros A únicamente para los hosts que están dentro del dominio o cualquiera de sus sub dominios.

DNS

```
asir.es.      IN    NS    ns1.asir.es. ; Servidor DNS maestro
asir.es.      IN    NS    ns2.asir.es. ; Servidor DNS maestro
asir.es.      IN    NS    dns.asir.org. ; Servidor DNS esclavo

ns1.asir.es.  IN    A     193.100.200.100
ns2.asir.es.  IN    A     193.100.200.200

;Delegación
sistemas.asir.es.  IN   NS    dns.asir.org. ;Delegación
```

DNS

Transferencias de zona

Los servidores DNS que declaran zonas esclavas o secundarias obtienen los archivos de zona (los registros de recursos) de otros servidores DNS autorizados para esas zonas.

A este proceso se le denomina transferencia de zona. Existen diferentes formas de llevarlo a cabo y es posible configurarlo en los servidores de nombres.

El objetivo es que todos los servidores autorizados para una zona tengan la misma información. Los servidores maestros usan el puerto 53/TCP para el intercambio de datos en las transferencias de zona.

Existen dos tipos de transferencias de zona entres servidores maestros y esclavos.

DNS

Transferencias de zona completas (AXFR)

En una transferencia de zona completa el servidor maestro le envía al servidor esclavo todos los datos de la zona. Una petición AXFR de un servidor esclavo a uno maestro es una solicitud para una transferencia de zona completa. Las especificaciones originales del servicio DNS (RFC 1034 y RFC 1035) solo contemplaban este tipo de transferencias.

Transferencias de zona incrementales (IXFR)

Las transferencias completas de zonas con muchos registros de recursos consumen ancho de banda, y puede llegar a tardar "mucho tiempo" dependiendo de las condiciones de la red y del tamaño de la zona. Para evitar estos inconvenientes, en la RFC 1995 se introdujeron las transferencias de zona incrementales.

En una transferencia de zona incremental el servidor maestro le envía al servidor esclavo solo los datos que han cambiado desde la última transferencia de zona. Una petición IXFR de un servidor esclavo a uno maestro es una solicitud para una transferencia de zona incremental.

DNS

Proceso de transferencia de zona

El proceso de transferencia de zona se puede iniciar de dos maneras:

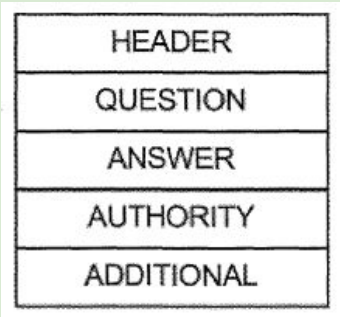
- El servidor esclavo pregunta al servidor maestro para comprobar si hay cambios en los archivos de zona. Lo hace cuando se inicia por primera vez y posteriormente, cada cierto tiempo de forma periódica .

- El servido maestro notifica (NOTIFY) al servidor o servidores esclavos que se han producido cambios en sus archivos de zona.

DNS

Protocolo DNS

El protocolo DNS determina el conjunto de normas y reglas en base a las cuales "dialogan" los clientes y los servidores DNS. El formato de un mensaje DNS es el que se muestra en la imagen. Como ya sabemos usa TCP como protocolo de transporte.



- **Header:** específica cuales son las secciones presentes, el tipo de mensaje y otros campos.
- **Question:** campos que definen una consulta a un servidor de nombres.
- **Answer:** RRs que responden a la consulta.
- **Authority:** RRs que apuntan a los servidores de nombre autoritativos.
- **Additional:** RRs que contienen información adicional.

DNS

Seguridad DNS

El servicio DNS es un servicio vital para el funcionamiento de Internet y de cualquier red TCP/IP. Los usuarios y el resto de servicios de la red que dependen de él se verían afectados si no funcionase correctamente. Por ello, está en el punto de mira de potenciales atacantes.

Se diseñó como un sistema abierto y en sus especificaciones originales no se contemplaban aspectos de seguridad. Además, su seguridad es difícil de gestionar y administrar al ser un servicio distribuido formado por varios componentes que se comunican entre sí.

Vulnerabilidades, amenazas y ataques

Cuándo se pregunta a un servidor DNS ¿Podemos fiarnos de que es quien dice ser o ha sido suplantado? ¿Las respuestas son reales o están falsificadas? ¿Si un servidor secundario recibe una transferencia de zona, la ha obtenido del maestro o ha sido suplantado? ...

Desde su puesta en marcha en Internet DNS ha sufrido muchos tipos de ataques y se han publicado múltiples vulnerabilidades. Además, la información que se puede obtener de los servidores DNS de una organización se puede utilizar como punto de partida para otros tipos de ataques.

DNS

Teniendo en cuenta los componentes del servicio DNS y el flujo de información entre ellos es posible definir diferentes puntos de amenazas.

1. Servidores DNS
    a. Ataques contra el propio servidor aprovechando vulnerabilidades (uso de exploits).
    b. Modificación de los archivos de zona por una mala configuración de seguridad en el sistema donde está instalado el servidor.
    c. Ataques de denegación de servicio (DoS).
2. Consultas de clientes DNS a servidores DNS
    a. Envenenamiento de la caché del cliente DNS, suplantado al servidor DNS remoto y enviando registros de recursos incorrectos.
3. Consultas de servidores DNS a otros a servidores DNS
    a. Envenenamiento de la caché del servidor suplantado al servidor DNS remoto y enviando registros de recursos incorrectos.
4. Transferencias de zona
    a. Suplantación del servidor maestro que envía registros de recursos a los secundarios.
5. Actualizaciones dinámicas a servidores DNS
    a. Suplantación de la fuente externa que envía las actualizaciones al servidor DNS.