UT3 Servicio de nombres de dominio (DNS)

Javier Rojas

1. DNS(Domain NameSystem)

- Es el principal servicio de resolución de nombres usado en redes TCP /IP, y por lo tanto en Internet.
- Los sistemas de nombres, no solo los usados en redes, se pueden clasificar en:
  - Sistemas de nombres planos:
    - Uso de nombres sin ningún tipo de agrupamiento.
    - No existe una jerarquía que permita clasificar dichos nombres.
    - Ejemplos: DNIs, nombres de ciudades, nombres de calles, nombres NETBIOS de Windows, etc.
  - Sistemas de nombres jerárquicos:
    - Uso de nombres agrupados y clasificados según algún criterio (por ejemplo, distribución geográfica, funcionalidad, tamaño, etc.)
    - Facilitan la administración y gestión distribuida.
    - Ejemplos: número de teléfono (0034918889999, 0034 ➔ identifica a España, 91 ➔ identifica a Madrid), nombres usados en los sistemas de ficheros de los sistemas operativos (C:\datos\apuntes.txt, C:\examen\apuntes.txt, /media/Datosjapuntes.txt), etc.

2. Historia

- En los comienzos de Internet se usaba un sistema de nombres planos. La relación entre nombres de equipos (hosts) y direcciones IP se almacenaba en un archivo (host.txt) localizado en un servidor central. Los equipos de la red obtenían periódicamente por FTP el archivo y así podían usar los nombres que contenía.
- Inicialmente, este esquema funcionaba bien (hasta mediados de los años 80) porque había pocos nombres y el fichero se actualizaba pocas veces a la semana. A medida que el número de equipos de la red aumentaba, el tamaño del archivo crecía y esto desencadenó una serie de problemas.
- En 1983, Ante los problemas de funcionamiento se pensó en un nuevo sistema que ofreciera características tales como escalabilidad, administración descentralizada y velocidad

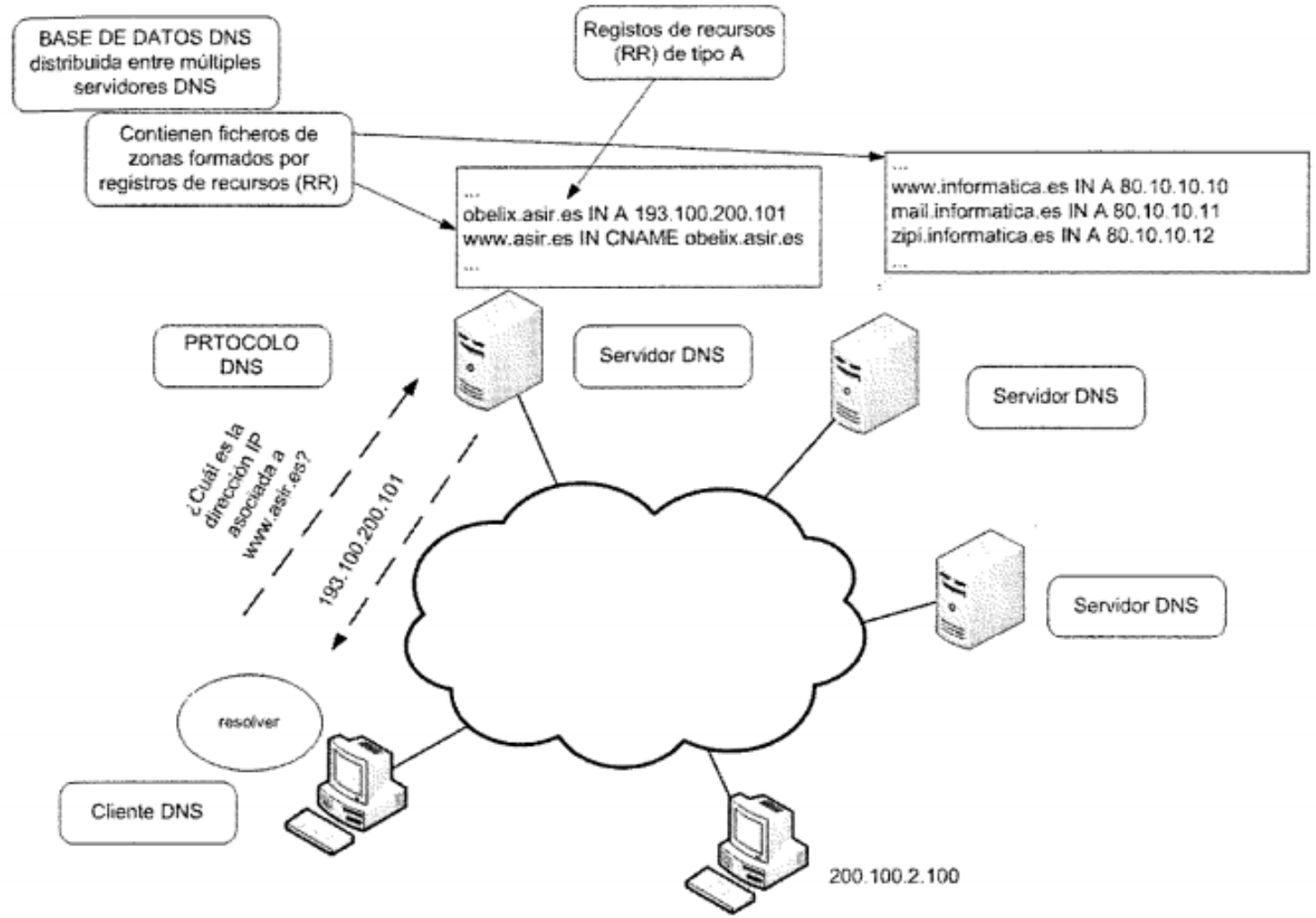
3. Características

- DNS puede almacenar varios tipos de información sobre cada nombre de dominio y por ello se puede utilizar para diferentes propósitos. Lo habitual es asociar direcciones IP con nombres de dominio y por eso se utiliza comúnmente para:
  - Resolución de nombres (búsqueda directa)
  - Resolución inversa de direcciones (búsqueda inversa)
  - Resolución de servidores de correo
- También se puede utilizar DNS para otros propósitos: balanceo de carga, obtención de claves públicas, ubicación de servidores para un servicio determinado, listas negras de spam, etc.

4. Componentes

- **Espacio de nombres de dominio (domain name space).** Conjunto de nombres que se pueden utilizar para identificar máquinas o servicios de una red.
- **Base de datos DNS.** Base de datos distribuida y redundante que almacena información, por ejemplo direcciones IP, sobre los nombres de dominio. Esta base de datos se organiza en zonas que almacenan la información en lo que se conoce como registros de recursos (RR, Resource Records).
- **Servidores de nombres (o servidores DNS) (name servers).** Programas que guardan parte de la base de datos DNS (zonas) y que responden a preguntas sobre la información almacenada. Por ejemplo, ¿cuál es la dirección IP asociada al nombre "www. asir. es" ?
- **Clientes DNS (resolvers).** Programas que realizan preguntas a los servidores de nombres y procesan las respuestas para ofrecerle la información a los usuarios y/ o a las aplicaciones que los invocan.
- **Protocolo DNS.** Conjunto de normas y reglas en base a las cuales "dialogan" los clientes y los servidores DNS.

Componentes



5. Funcionamiento

- El funcionamiento del servicio DNS se basa en el modelo cliente/servidor:
  - Los clientes DNS (resolvers) preguntan a los servidores de nombres.
  - Los servidores de nombres también se comunican entre sí.
    - Pueden realizar preguntas a otros servidores de nombres cuando no tienen la información por la que le han preguntado.
    - Pueden intercambiar información sobre sus zonas (transferencias de zona).

Actividad

- Inicia sesión a alguna de las máquinas de la red virtual (wxp) y abre un terminal. Ejecuta el comando nslookup www.google.es y observa los resultados.
- El comando nslookup realiza una pregunta al servidor DNS que esté configurado en las propiedades TCP /IP del equipo y muestra por pantalla información sobre la respuesta obtenida. En dicha respuesta se puede observar cual es el servidor DNS que responde, qué direcciones IP se asocian con el nombre de dominio www. google. es y por último otros nombres de dominio que son equivalentes a este (que se denominan alias).

Actividad

- ¿En qué capa opera DNS?
- Dibuja la pila de protocolos que opera cuando lo usas.
- ¿Qué se WINS?¿Qué protocolo usa?
- Dibuja las pilas de protocolos de ambos protocolos enfrentadas.

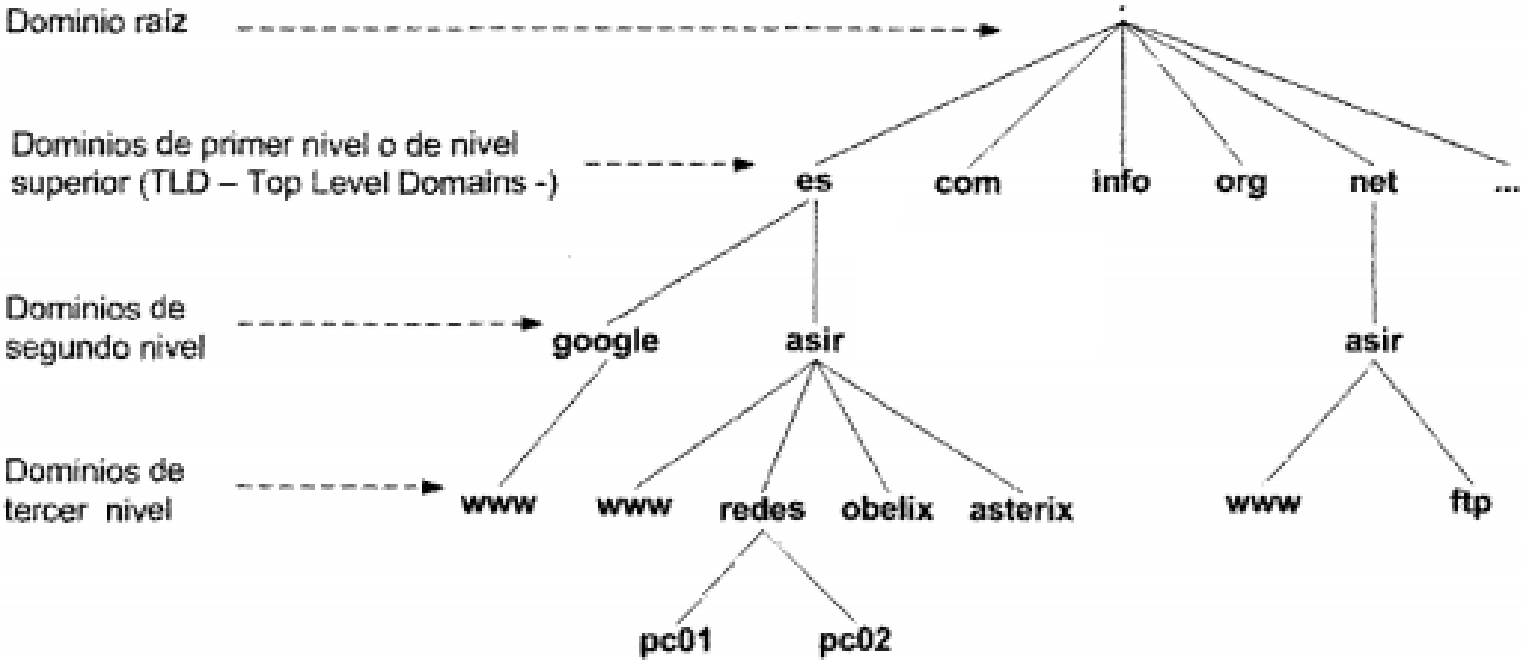
6 Espacio de nombres de dominio

- El espacio de nombres de dominio es el conjunto de nombres que se pueden utilizar para identificar máquinas o servicios de una red.
- Definiciones:
  - Nombres de dominio.
  - Dominio raíz. Dominios y subdominios.
  - Nombres relativos y absolutos (FQDN).
  - Uso de dominios.
  - Administración de nombres de dominio en Internet. Delegación.

6.1 Nombres de dominio

- Cada nombre de dominio puede estar formado por una o varias cadenas de caracteres separadas por puntos. **No se distingue entre mayúsculas y minúsculas**, por ejemplo, "ASIR. ES." es equivalente a “asir. es.”.
- El conjunto de nombres forman el denominado espacio de nombres de dominio que se puede representar mediante una estructura jerárquica organizada en forma de árbol, es decir, todos los nombres forman un árbol donde cada nodo se separa de los otros nodos por un punto

6.1 Nombres de dominio

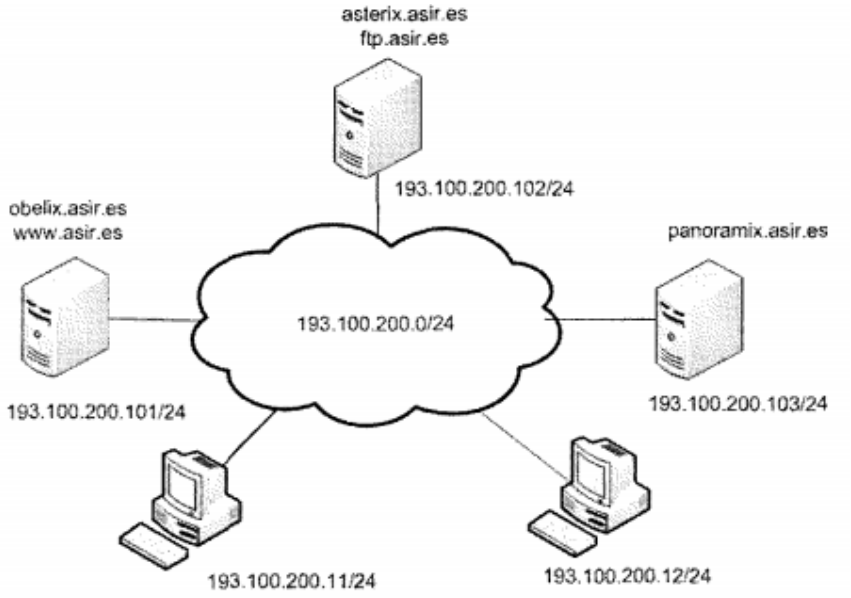


6.1 Nombres de dominio

- Como consecuencia de la organización jerárquica de los nombres de dominio es posible utilizar los términos dominio y subdominio, al igual que en un sistema de ficheros de un disco duro es posible referirse a directorios y subdirectorios. Por ejemplo, "asir. es." es un subdominio del dominio "es.", "redes. asir. es." es un subdominio del dominio "asir. es.".
- Los dominios o subdominios (usa el término que prefieras) que "cuelgan" del dominio raíz se conocen como 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 y así sucesivamente.

6.2 Nombres relativos y absolutos. FQDN

- Supongamos que hemos decido usar dominio "asir. es." para nombrar a todos los equipos de la red de área local de un instituto. En la red hay varios equipos y a cada uno se le identifica con **uno o varios nombres** que formen parte del dominio "asir. es."



6.2 Nombres relativos y absolutos. FQDN

- Si hacemos referencia a "www. asir. es." sabemos que se trata del equipo con IP 193. 100.100. 101, y si hacemos referencia a "www. google. es." sabemos que es otro equipo diferente. Si tan solo usamos www podríamos interpretar que es el equipo "www. asir. es." porque en nuestra red usamos el nombre de dominio "asir.es. ", pero ¿por qué tiene que ser este y no otro? ¿no podría ser "www. google. es”?

6.2 Nombres relativos y absolutos. FQDN

- Cuando se hace referencia a un dominio usando un nombre se puede emplear su nombre relativo o su nombre absoluto.
  - Nombres relativos: es necesario saber el contexto del dominio superior para determinar a qué nombre se hace referencia exactamente. Por ejemplo "obelix", "www", "panoramix.asir".
  - Nombres absolutos: nombre formado por todas las partes separadas por puntos desde el nodo correspondiente hasta el dominio raíz. Por ejemplo "asir. es.", "obelix.asir. es.", "www. asir. es.". Los nombres indicados de esta forma se llaman nombres de dominio completos (**FQDN, Fully Qualified Domain Names**). El "." final del dominio raíz permite distinguir si el nombre usado es FQDN o no.
- Normalmente, los usuarios no utilizamos el "." final de los nombres FQDN en las aplicaciones (navegadores web, clientes de ftp, clientes de correo, ...) pero internamente sí se utiliza.

6.3 Uso de dominios

- Lo habitual es usar un dominio, por ejemplo "asir. es", para nombrar a un conjunto de hosts y/o subdominios que se agrupan según algún criterio (hosts de la misma red, hosts de la misma empresa- este en la misma o en diferentes redes, hosts de una misma localización, ...) aunque no tiene por qué ser así.
- Se podría usar el dominio "asir. es" como en ejemplo anterior (equipos de una red de área local), pero también se podría emplear para referirse a hosts que no tienen por qué formar parte de la misma red ("www.asir.es" ➔ 90.100.10.10, "obelix.asir.es"➔ 200.10.20.1, "ftp.asir. es"➔ 100.100.100.2, ...).

6.4 Administración de nombres de dominio en Internet. Delegación

- La administración y organización del espacio de nombres de dominio de Internet se distribuye entre múltiples empresas y organizaciones, estando coordinada por la ICANN (Internet Corporation for Assigned Names and Numbers).

6.4.1 Dominio raíz y la ICANN

- La ICANN es una organización sin ánimo de lucro que tiene el objetivo de garantizar que Internet sea estable, operativa y segura. Se encarga, entre otras funciones, de administrar el dominio raíz y de mantener un registro de los **dominios de nivel superior (TLD)** existentes. InterNIC es la organización asociada a la ICANN que permite registrar dominios TLD.

6.4.2 Dominios TLD y los operadores de registro (registry)

- Los dominios de nivel superior (TLD, Top Level Domain) son clasificados por la ICANN desde un punto administrativo en:
  - Genéricos (gTLD, generic TLD)
    - Nombre significativo en función del propósito o el tipo de organización que lo utiliza.
    - Se clasifican a su vez en:
      - Dominios patrocinados (sTLD, sponsored TLD). Operan según las reglas de una entidad que soporta su patrocinio (Ejemplos: "aero", "asia", "cat", "coop", "edu", "gov", "travel" , ...).
      - Dominios no patrocinados (uTLD, unsponsored TLD). Operan según las reglas del ICANN con unas políticas de uso establecidas globalmente (Ejemplos: "com", "info", "org", "net" , ..

6.4.2 Dominios TLD y los operadores de registro (registry)

- Geográficos (ccTLDs, country code TLDs)
  - Nombres de dos letras establecidos en función países o regiones.
  - Las tareas de gestión y políticas de uso se delegan en una entidad del país o territorio (el gobierno de cada país determina la entidad que gestiona el dominio) para favorecer las políticas locales que permitan satisfacer mejor las circunstancias económicas, culturales, lingüísticas y legales del país o territorio en cuestión.
  - Ejemplos: "es" (España), "fr" (Francia), "np" (Nepal), etc.

6.4.2 Dominios TLD y los operadores de registro (registry)

- Dominios reservados
  - Existen una serie de nombres de dominio de primer nivel que están reservados para que puedan usarse en pruebas privadas, ejemplos de documentación, etc. sin temor a entrar en conflicto con nombres TLD actuales o futuros.
  - Los nombre reservados son: "test", "example", "invalid" y "localhost".

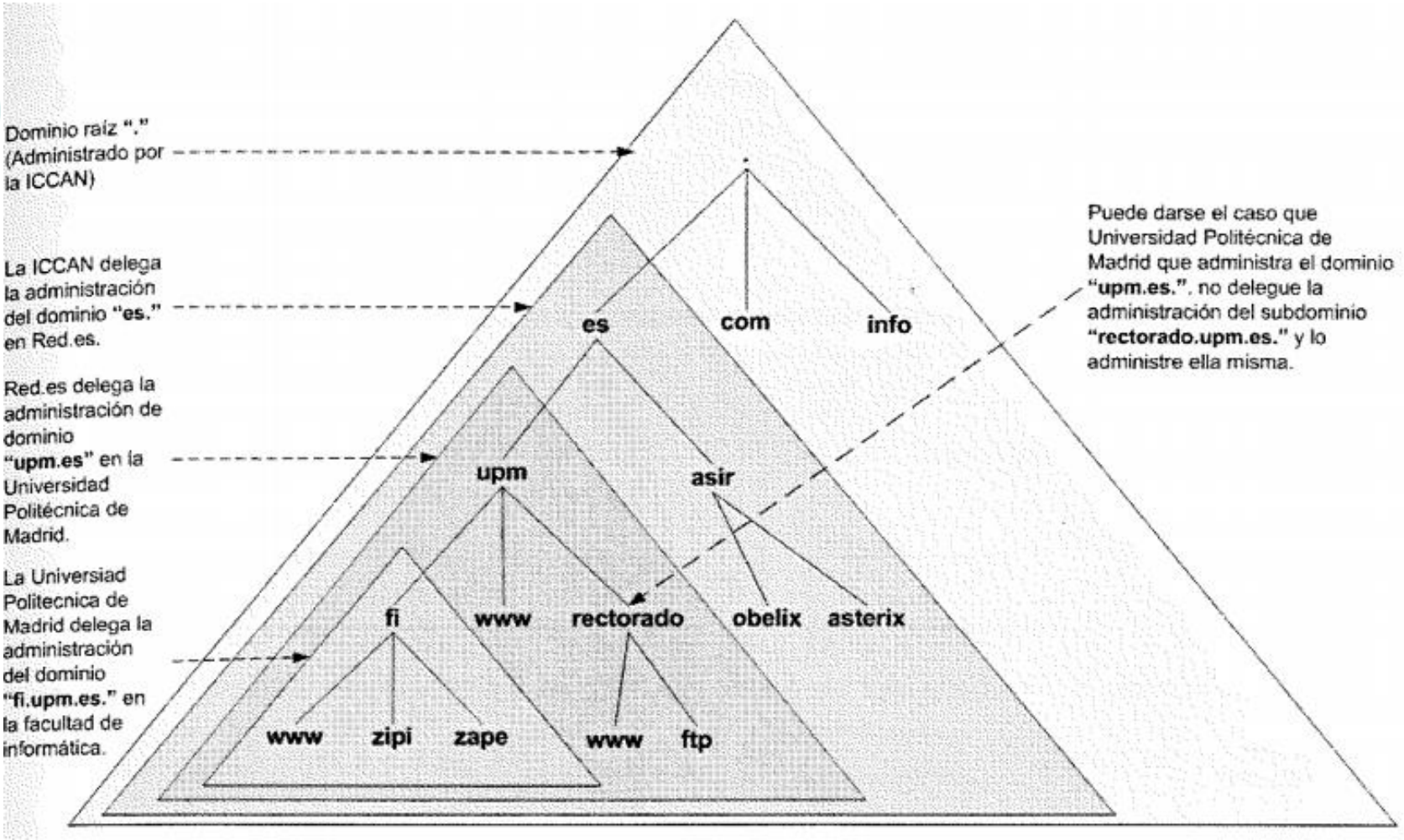
Actividad

- Lee la información sobre la función de la ICANN en https://www.icann.org/
- Consulta la web http://www.iana.org/domains/root/db/ y observa los dominios TLD existentes y como se clasifican según la ICANN.
- Consulta el documento http://www.rfc-es.org/rfc/rfc2606-es.txt donde se explica el uso recomendado de los dominios reservados.
- Consulta la web http://www.iana.org/domains/root/db para saber cuál es el operador de registro (registry) que se encarga de los dominios TLD "com", "net" y "es".
- Accede a la web http://www.red.es y consulta la información que ofrece sobre el dominio "es". Busca en la página oficial de dominios “es” si está disponible el dominio de tu nombre.

6.4.3 Delegación

- La delegación consiste en que la organización que administra un dominio cede la administración de uno, varios o todos sus subdominios a otras organizaciones. Como ya se ha explicado, la ICAAN administra el dominio raíz y delega la administración de los dominios TLD en otras organizaciones.
- Cada una de estas organizaciones (por ejemplo, Red.es para el dominio "es") puede delegar la administración de los dominios de segundo nivel en otras (por ejemplo, Red.es delega la administración del dominio "upm.es." en la Universidad Politécnica de Madrid)

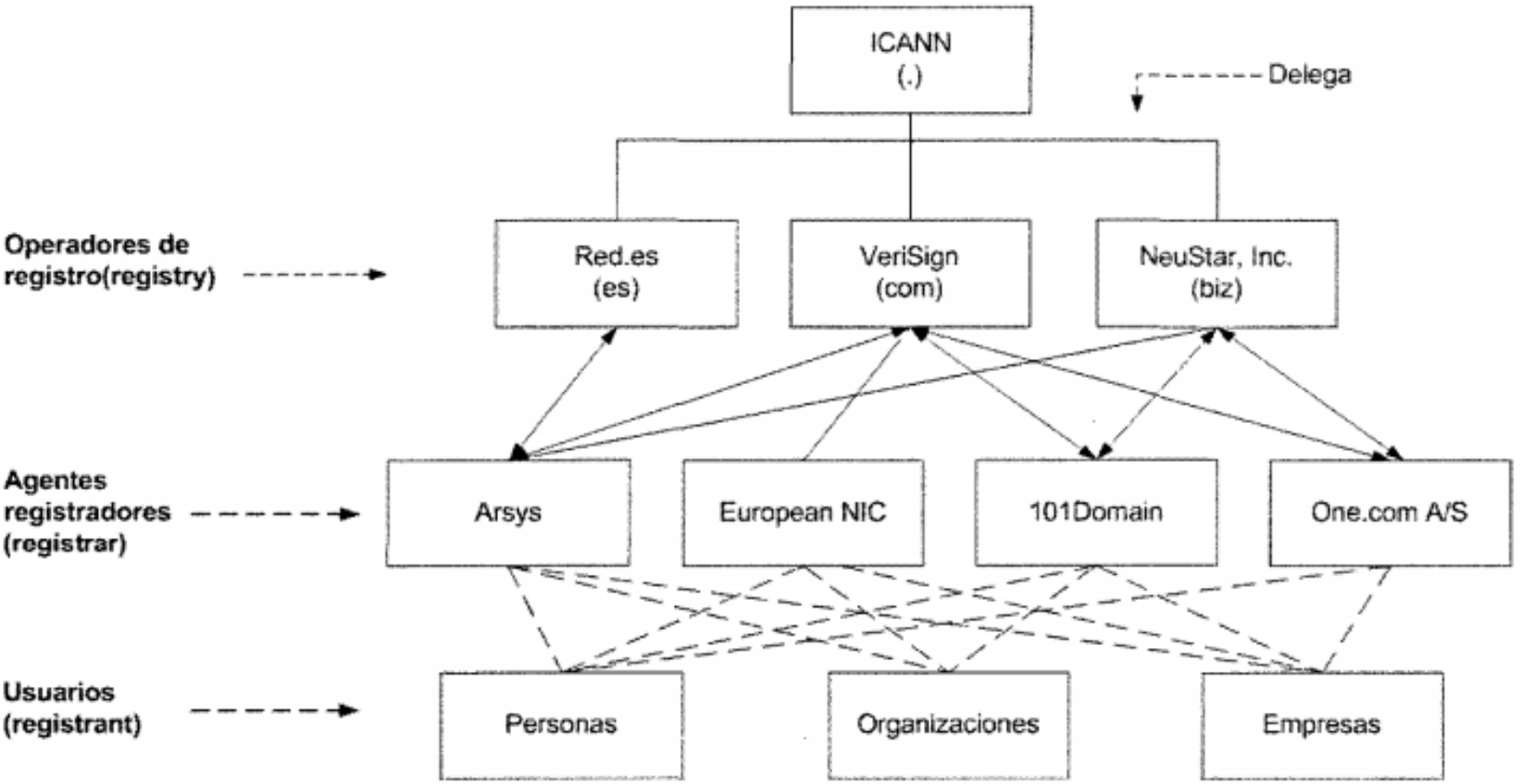
6.4.3 Delegación



6.4.4 Registro de dominios. Agentes registradores (registrar)

- Registrar un dominio consiste en "reservar" el nombre durante un tiempo (normalmente durante un año) para poder crear subdominios y asociar el nombre y/o los sub dominios con direcciones IP o con la información que se considere oportuna. Las personas, empresas u organizaciones, denominadas registradores (registrar), pueden registrar nombres de dominio de segundo nivel.
- Un nombre de dominio puede ser registrado a través de diferentes compañías, conocidas como agentes registradores(registrant), que asesoran a los registradores (registrar), y tramitan la solicitud haciendo de intermediario con los operadores de registro (registry) (estos también pueden actuar como agentes registradores). Los agentes registradores deben estar acreditados por los operadores de registro y tienen libertad para asignar una parte del precio que cuesta el registro

6.4.4 Registro de dominios. Agentes registradores (registrar)



Actividades

- Consulta las preguntas frecuentes (FAQs) de la web de la ICANN (https://www.icann.org/resources/pages/faqs-2014-01-22-es).
  - ¿Cuáles son las normas de registro de los dominios gTLD?
  - ¿Cuáles son las normas de registro de los dominios ccTLD?
  - Si hay problemas con un agente registrador ¿Hay que informar la ICANN?.
- Consulta las web de la ICANN (http://www.icann.org/) y de InterNIC (https://www.internic.net/) para conocer una lista de agentes registradores acreditados. Busca los españoles.
- Consulta la web de Red. es (http://www.red.es) para consultar la lista de agentes registradores acreditados para el dominio "es".

Actividades

- Elige un nombre de dominio (por ejemplo, "minombre.com"), accede a la web de tres agentes registradores acreditados por Red.es y:
  - Comprueba que no está registrado.
  - Realiza una comparativa de precios entre los 3 agentes registradores.
  - Elige un agente registrador y completa el proceso de registro hasta el punto donde se pide que realices el pago.

- Lee los siguientes enlaces
  - http://soytecno.com/2015/10/02/googlecom/
  - https://es.wikipedia.org/wiki/Arsys

Curiosidad

- La ciberocupación es la acción y efecto de registrar un nombre de dominio, sabiendo que existen otras organizaciones, empresas o particulares más adecuados para usarlo, con el propósito de extorsionarlo para que lo compre o bien simplemente para desviar el tráfico web hacia un sitio competidor o de cualquier otra índole.
- La ciberocupación y otros problemas relacionados con el registro de nombres de dominio llevaron a la creación de una política uniforme de resolución de controversias de nombres de dominio (URDP). La Organización Mundial de la Propiedad Intelectual (OMPI) es un organismo que se encarga de arbitrar y mediar.
- Actividad: Investiga cuál ha sido el mayor pago por un dominio

7 Servidores de nombres

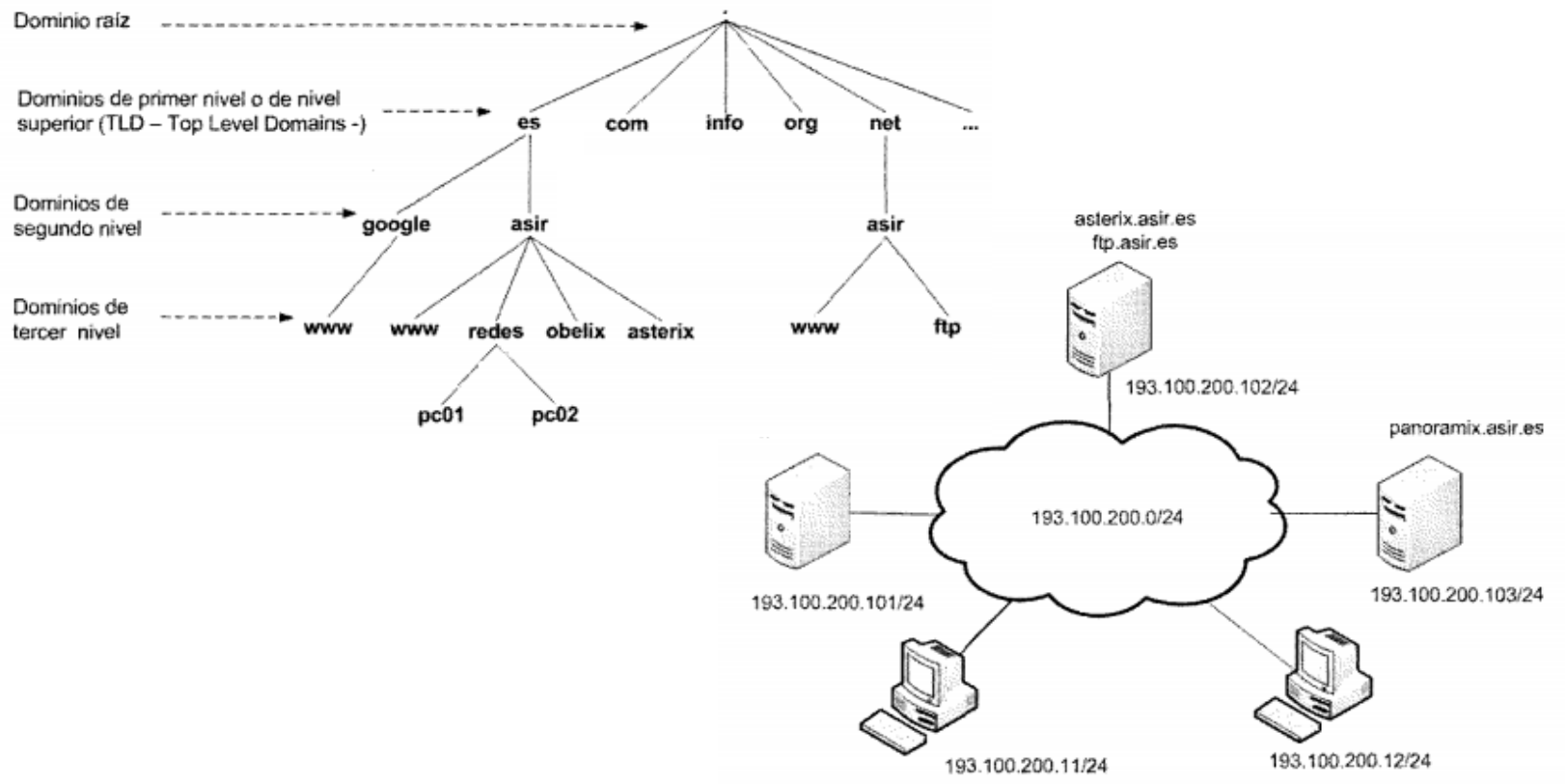
- Los servidores de nombres, también llamados servidores DNS, son programas que guardan información sobre nombres de dominio y responden a las preguntas que les realizan los clientes DNS y otros servidores de nombres. Almacenan por lo tanto, una parte de la base de datos DNS.
- Por defecto escuchan peticiones en los puertos 53/TCP y 53/UDP.

7.1 Zonas

- Los servidores de nombres mantienen información de una parte del espacio de nombres de dominio que se conoce como zona (por ejemplo, el servidor DNS del Instituto ASIR almacena la información de la zona "asir. es.").
- 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.

7.1 Zonas

- Recordamos el ejemplo:



7.1 Zonas

Fichero de zona de resolución directa del dominio **asir.es.** que se almacena en un servidor DNS que esta 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.
...
```

7.1 Zonas

Fichero de zona de resolución directa del dominio **asir.es.** que se almacena en un servidor DNS que esta 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
...
```

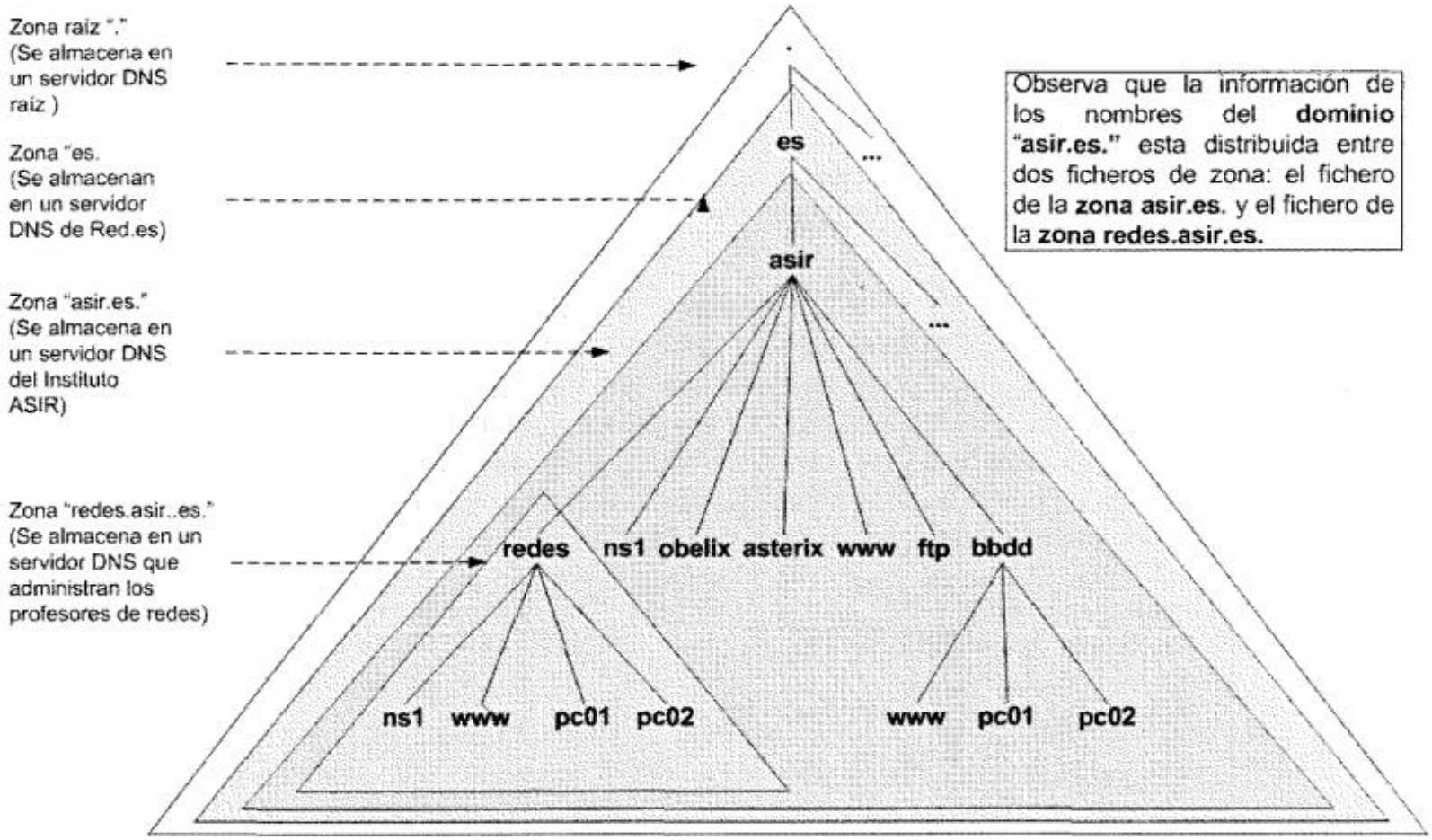
Actividad

- Busca en el RFC 1035 lo que significan las siglas anteriores
- Recuerda: http://www.rfc-es.org/

7.1 Zonas

- 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 subdominio "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.

7.1 Zonas


Zona raiz "."
(Se almacena en un servidor DNS raiz)
Zona "es.
(Se almacenan en un servidor DNS de Red.es)
Zona "asir.es."
(Se almacena en un servidor DNS del Instituto ASIR)
Zona "redes.asir..es."
(Se almacena en un servidor DNS que administran los profesores de redes)
.
es
asir
redes
ns1
obelix
asterix
www
ftp
bbdd
ns1
www
pc01
pc02
www
pc01
pc02
Observa que la información de los nombres del dominio "asir.es." esta distribuida entre dos ficheros de zona: el fichero de la zona asir.es. y el fichero de la zona redes.asir.es.

7.1 Zonas

- Para evitar problemas de sobrecarga 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 (lo vemos más adelante)

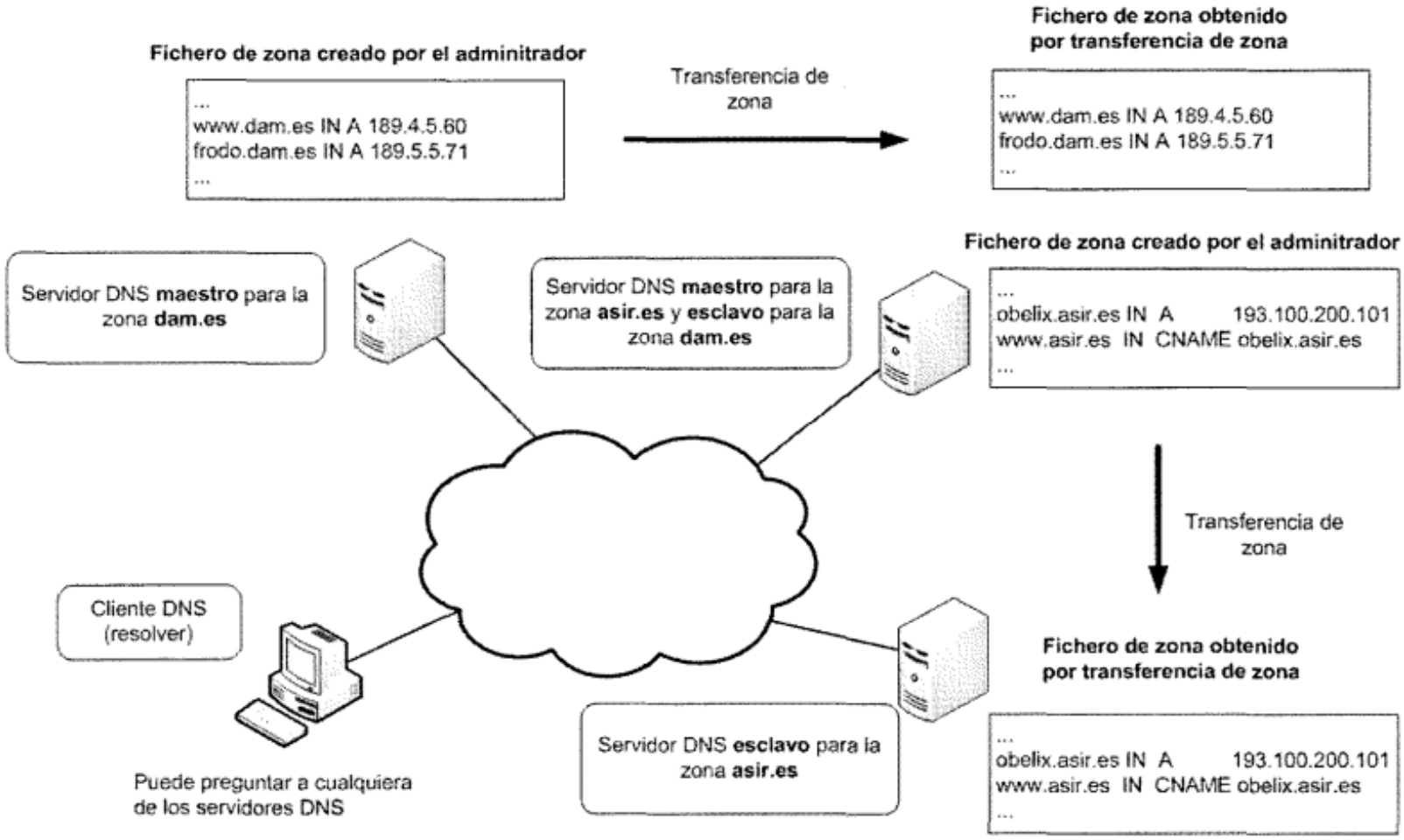
7.2 Tipos de servidores de nombres

- 7.2.1. Servidor maestro (o primario)
  - Un servidor DNS maestro (también denominado primario o principal) define una o varías 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.

7.2 Tipos de servidores de nombres

- 7.2.2. Servidor esclavo (o secundario)
  - Un servidor esclavo (también denominado secundario) define una o varías 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.

7.2 Tipos de servidores de nombres



7.2 Tipos de servidores de nombres

7.2.3. Servidor cache

- 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 cache 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.

Actividad

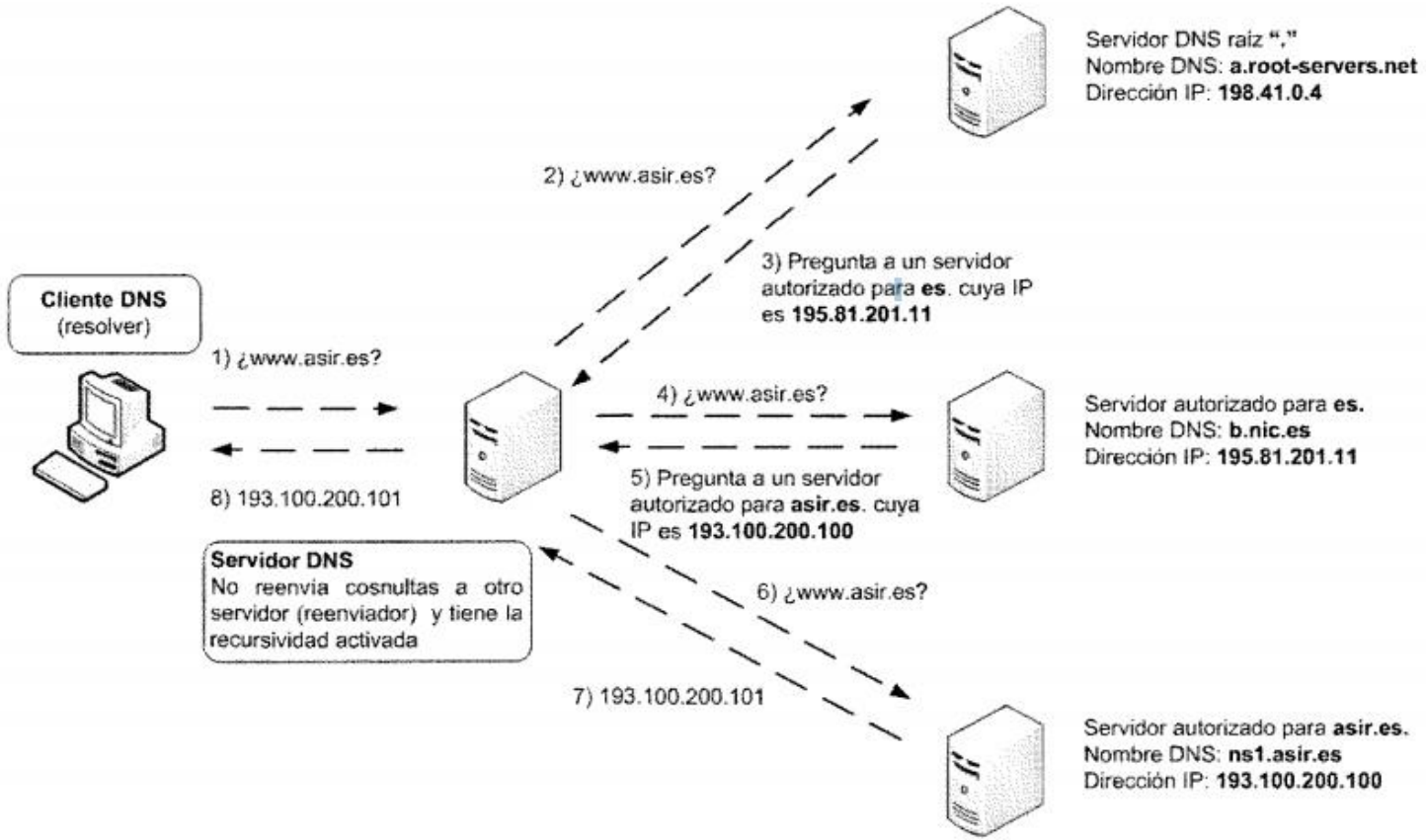
- Busca en Internet un listado que muestre los servidores DNS cache que ofrecen las empresas de comunicación que operan en España.
- Buscar cuáles son los servidores DNS cache que pone Google a disposición de todos los usuarios de Internet.

7.2 Tipos de servidores de nombres

- 7.2.4. 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.
    - Se encarga de procesar la consulta preguntando a diversos servidores DNS y empezando por los servidores DNS raíz.
    - 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 cache DNS del reenviador minimizando los tiempos de respuesta.

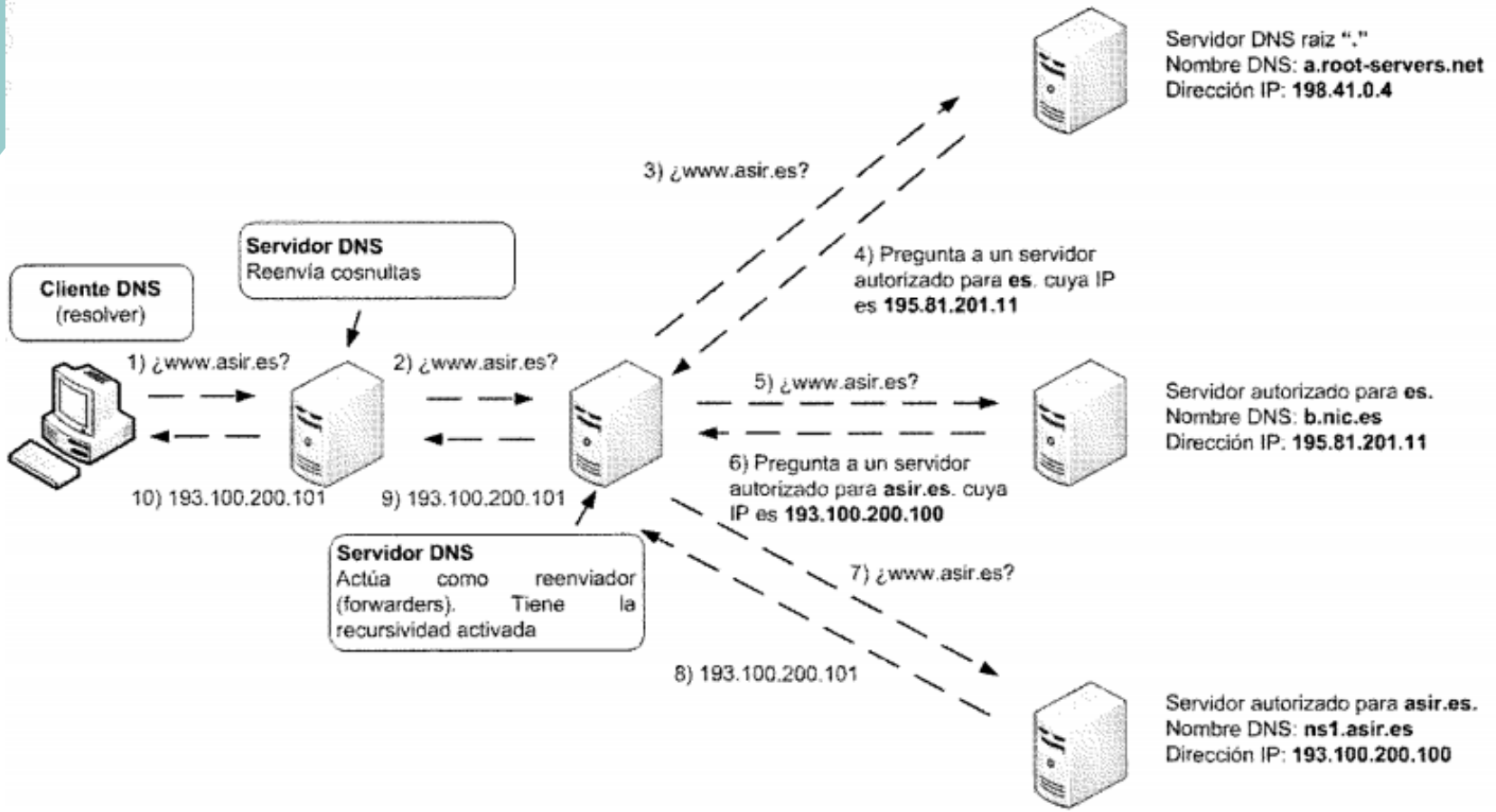
7.2 Tipos de servidores de nombres

- Servidor DNS que no reenvía consultas: procesa la consulta preguntando a diversos servidores DNS



7.2 Tipos de servidores de nombres

- Servidor DNS que actúa como reenviador



7.2 Tipos de servidores de nombres

7.2.5. Servidor solo autorizado

- 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 cache.

Actividad

- En tu equipo:
  - Ejecuta el comando nslookup www.google.es 8.8.8.8 para preguntar al servidor DNS de 8. 8. 8. 8 por el nombre de dominio www. google. es. Observa que la respuesta es no autorizada. Significa que el servidor DNS no es autorizado para la zona google.es.
  - Ejecuta el comando nslookup www.google.es ns1.google.com para preguntar al servidor DNS de ns1. google.com por el nombre de dominio www.google. es. Observa que la respuesta es autorizada. Significa que el servidor DNS si es autorizado para google. es.
  - Ejecuta el comando nslookup www.iescomercio.es 8.8.8.8 para preguntar al servidor DNS de 8.8.8.8 por el nombre de dominio www.garceta.es ¿Qué significa?
  - Ejecuta el comando nslookup www.iescomercio.es nsl.google.com para preguntar al servidor DNS de 8. 8. 8. 8 por el nombre de dominio www. garceta. es ¿Qué significa? ¿Qué diferencia hay entre el servidor DNS de 8. 8. 8. 8 y el servidor DNS de ns1. google.com?
  - Nota: en el momento de probar esta actividad la dirección IP de nsl.google.com era 216.239. 32. 10, por lo que era posible ejecutar por ejemplo nslookup www.garceta. es 216.239.32. 10

7.3 Servidores raíz

- Existen en Internet un conjunto de servidores DNS autorizados para el dominio raíz ".", conocidos como servidores raíz (root servers). Contienen por lo tanto el fichero de la zona "." que almacena cuales 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 13 servidores raíz" y cada uno de ellos tiene múltiples copias distribuidas por todo el mundo (es decir, que realmente no existen solo 13). Cada grupo, cada conjunto de copias de uno de los 13, 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.

Actividad

- descarga el archivo de la IANA root.zone y ábrelo con un editor de textos. Este archivo es una copia del fichero de la zona "." que contienen los servidores DNS raíz. Aunque no entiendas la mayor parte del contenido del fichero observa que hay varios registros de recursos de tipo NS para cada dominio TLD. Cada uno de ellos indica los servidores de nombres autorizados para el dominio TLD correspondiente. Así es como los servidores raíz delegan la autoridad de los dominios TLD en los servidores DNS de los operadores de registro (registry). Compara los servidores autorizados para el dominio “es“ que ya consultaste en la actividad anterior.

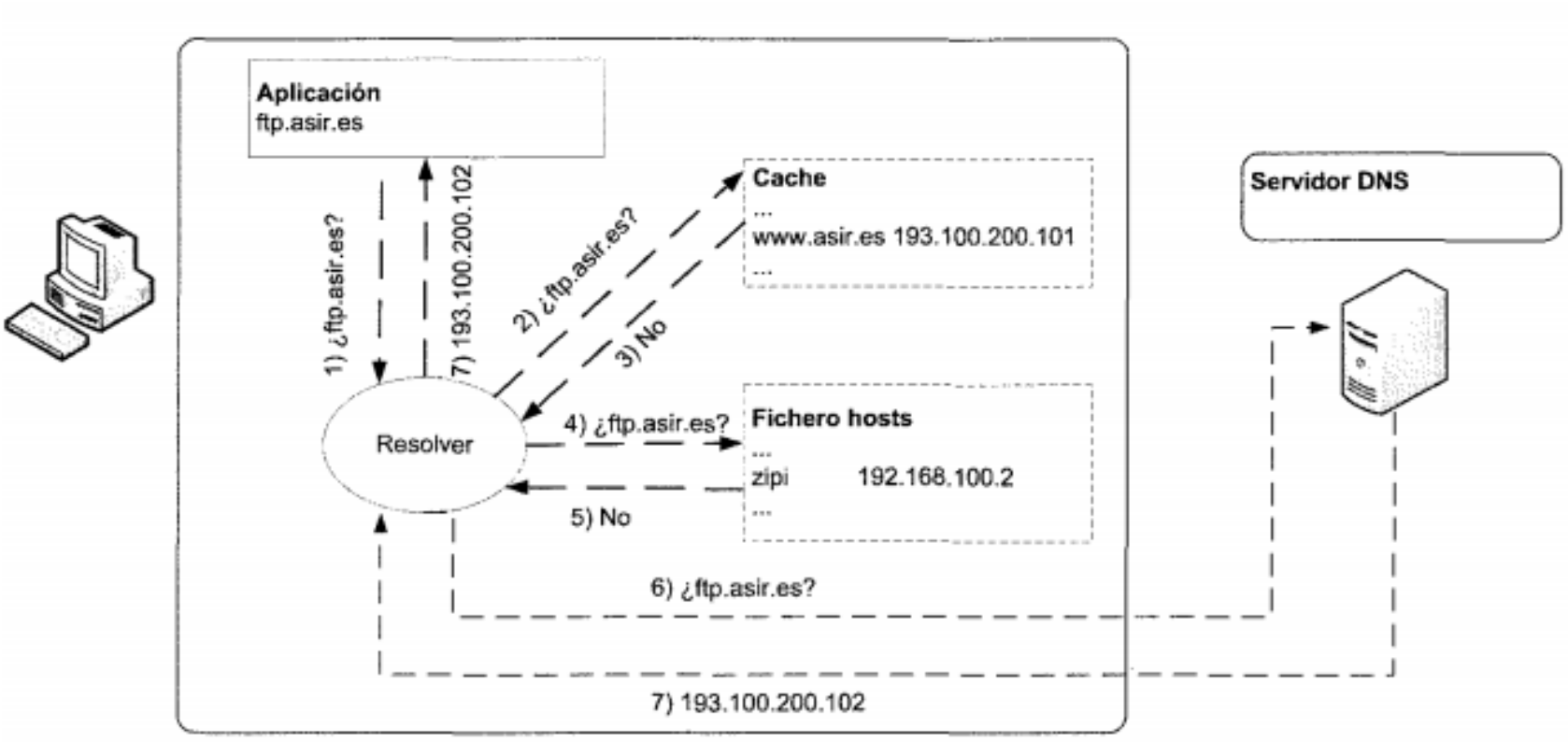
8. Clientes DNS (resolvers)

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

8. Clientes DNS (resolvers)

- El resolver consulta la cache de resolución de nombres del hosts (si está configurada) (almacenada en memoria). Si obtiene una respuesta positiva se la entrega a la aplicación.
- Si el nombre buscado no está en la cache, el resolver buscará en el archivo hosts local del equipo.
  - En sistemas Windows el archivo es
  - %SYSTEMROOT% \system32\drivers\etc\hosts
  - En sistemas Linux/Unix el archivo es
  - /etc/hosts.
- 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.

8. Clientes DNS (resolvers)



9. Proceso de resolución

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

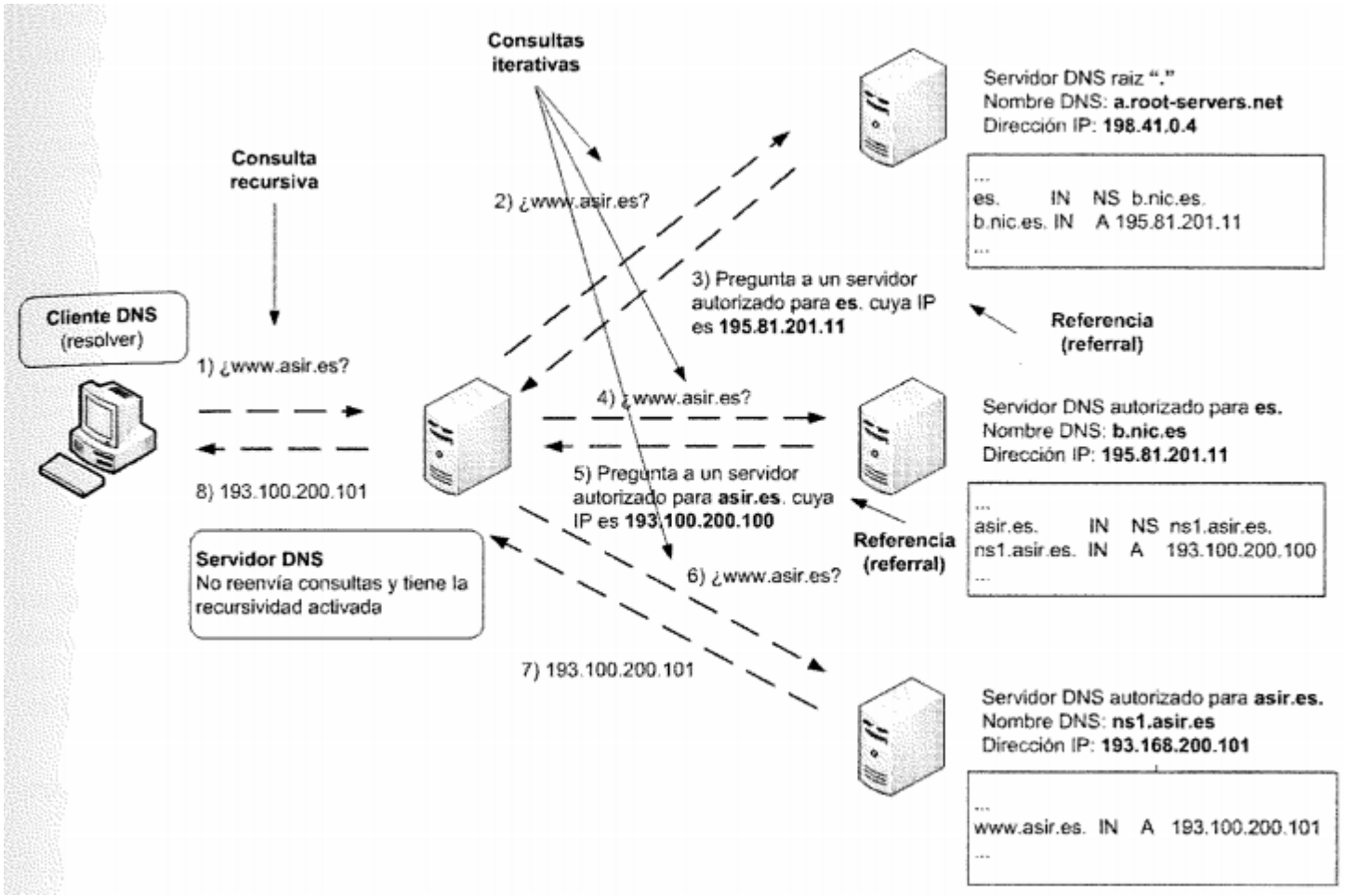
9.1 Consultas recursivas

- Una consulta recursiva es aquella en la que el servidor tiene que dar una respuesta completa o exacta
  - 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).

9.1 Consultas recursivas

- Cuando un servidor recibe una consulta recursiva:
  - 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.
  - Si no encuentra la respuesta o no es autorizado y actúa como cache, consulta su cache de respuestas anteriores. Si encuentra la respuesta responde indicando que la respuesta no es autoritativa.
  - En otro caso:
    - 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.
    - Si no tiene configurados reenviadores inicia una serie de consultas iterativas a otros servidores DNS.

9.1 Consultas recursivas



Actividad

- Accede a una máquina virtual ubuntu. Ejecuta el comando

  dig @8.8.8.8 www.iescomercio.com +trace.

- Con este comando se le envía una consulta recursiva al servidor DNS 8. 8. 8. 8 preguntando por el nombre www.iescomercio.com, y se le indica con la opción +trace que muestre el rastro de todo el proceso de resolución. Observa que se pregunta en primer lugar a un servidor raíz, posteriormente a un servidor autorizado para el dominio .com y por último al servidor autorizado para iescomercio.com. Adjunta la captura de pantalla en los apuntes.

9.2. Consultas iterativas

- Una consulta iterativa (o no recursiva) es aquella en la que el servidor DNS puede proporcionar una respuesta parcial.
  - 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.

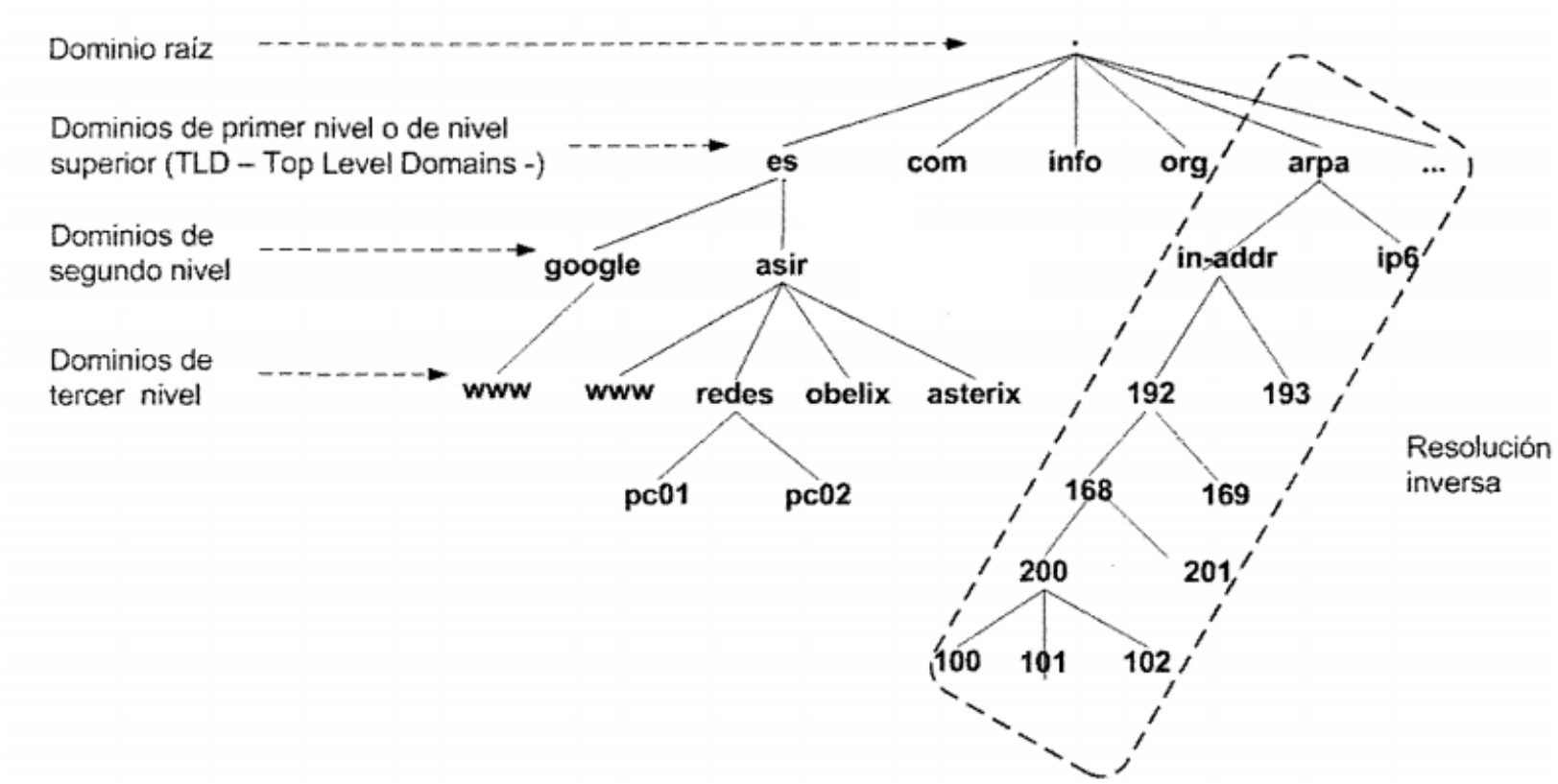
10. Resolución inversa

- 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 ¿cuál es o cuáles son los nombres de dominio asociados a la dirección IP 200.100.89.10?
- 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.

3.10.1. 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.

10.1. Mapeo de direcciones IP y dominio arpa



10.1. Mapeo de direcciones IP y dominio arpa

- 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 ultimo "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".

10.2. 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 las zonas inversas

10.2. 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.
...
```

10.2. Zonas de resolución inversa

- 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.

11. Registros de recursos DNS

- 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.

11.1. 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.

11.2. Registro NS

- El registro de recursos NS (Name Server) permite establecer:
- El/los servidores de nombres autorizados una zona

```
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
```

- Cada zona debe contener, como mínimo, un registro NS.

11.3. Registro A, AAAA

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

11.4. Registro CNAME

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

11.5. Registro MX

- El registro de recursos MX (Mail Exchange) permite definir equipos encargados de la entrega de correo en el dominio.

11.6. 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.

Actividad

- Crea en nuestro servidor una nueva zona “actividad” y (si no se han creado solos) crea un registro de cada tipo. Haz una captura de pantalla e indica sus principales características.
- Para el PTR te hará falta crear una zona inversa:

  6.2.10.in-addr. arpa

12. 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.

12. Transferencias de zona

- Las transferencias de zona son necesarias para el funcionamiento adecuado del servicio DNS pero también son una fuente de amenazas de seguridad. Un servidor DNS esclavo puede recibir registros de recursos de una fuente maliciosa envenenado así sus ficheros de zona. Cuando le pregunten por un nombre de dominio responderá con la dirección que haya puesto el atacante, por lo tanto, hay que configurar adecuadamente los servidores DNS que actúen como esclavos para que solo acepten transferencias de zonas de fuente conocidas.

12. Transferencias de zona completas (AXFR) e incrementales (IXFR)

- 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 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.

13. DNS Dinámico (DDNS, Dynamic DNS)

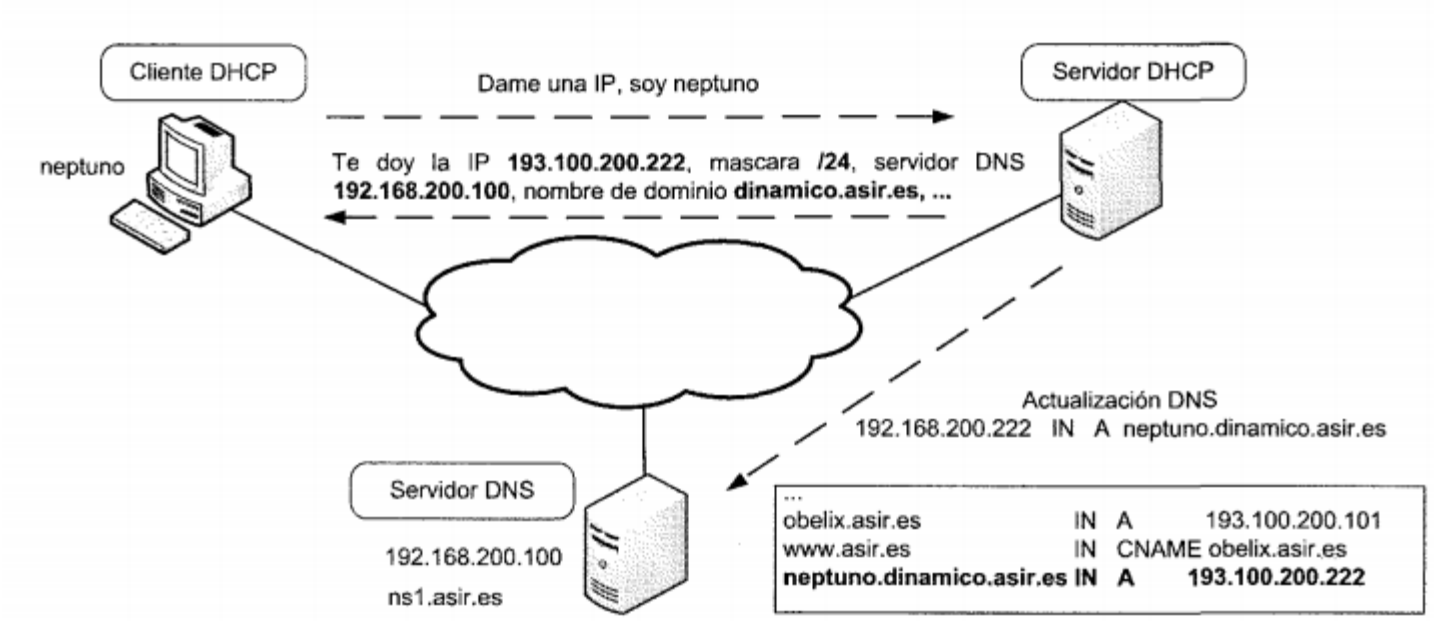
- Para que los usuarios tengan acceso a los recursos DNS correctamente, es fundamental que los servidores de nombres estén actualizados. La actualización de los registros de recursos de un archivo de zona se puede realizar manualmente o dinámicamente.

13.1. Actualizaciones manuales

- En las actualizaciones manuales el administrador crea, elimina o modifica registros de recursos editando los ficheros de zona. Cuando el volumen de actualizaciones de los archivos de zona es elevado y hay varias zonas (imagina una red en la que se asignan direcciones usando un servidor DHCP y se quieren registrar los nombres DNS de los clientes DHCP) el trabajo del administrador y las probabilidades de equivocarse y no mantener los archivos de zona actualizados crece considerablemente.

13.2. Actualizaciones dinámicas

- Las actualizaciones dinámicas pueden ser realizadas:
- Directamente por los equipos: configurando cliente y servidor para que se actualicen automáticamente.
- Por servidores DHCP:



13.3. DNS dinámico en Internet

- Los proveedores de acceso a Internet (ISP, Internet Services Provider) asignan una dirección IP por DHCP al router que nos conecta a su red (a no ser que contratemos una dirección IP fija). La dirección IP puede cambiar cada cierto tiempo o cada vez que se apaga o enciende el router, por lo tanto, no tenemos control sobre ella.
- ¿Qué ocurre si queremos asignar un nombre de dominio asociado a la IP del router para ofrecer servicios, por ejemplo, un servidor web en nuestra red?
- ¿Qué IP le asociamos a nuestro nombre de dominio?, la que tengamos en el momento actual ¿Y si cambia?

13.3. DNS dinámico en Internet

- Lo habitual es configurar un programa en el muter de conexión a Internet o en un equipo de la red para que actualice el servidor DNS cuando la IP asignada por DHCP cambie. Los routers que se comercializan actualmente suelen integrar estos programas

14. Seguridad DNS

- 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.

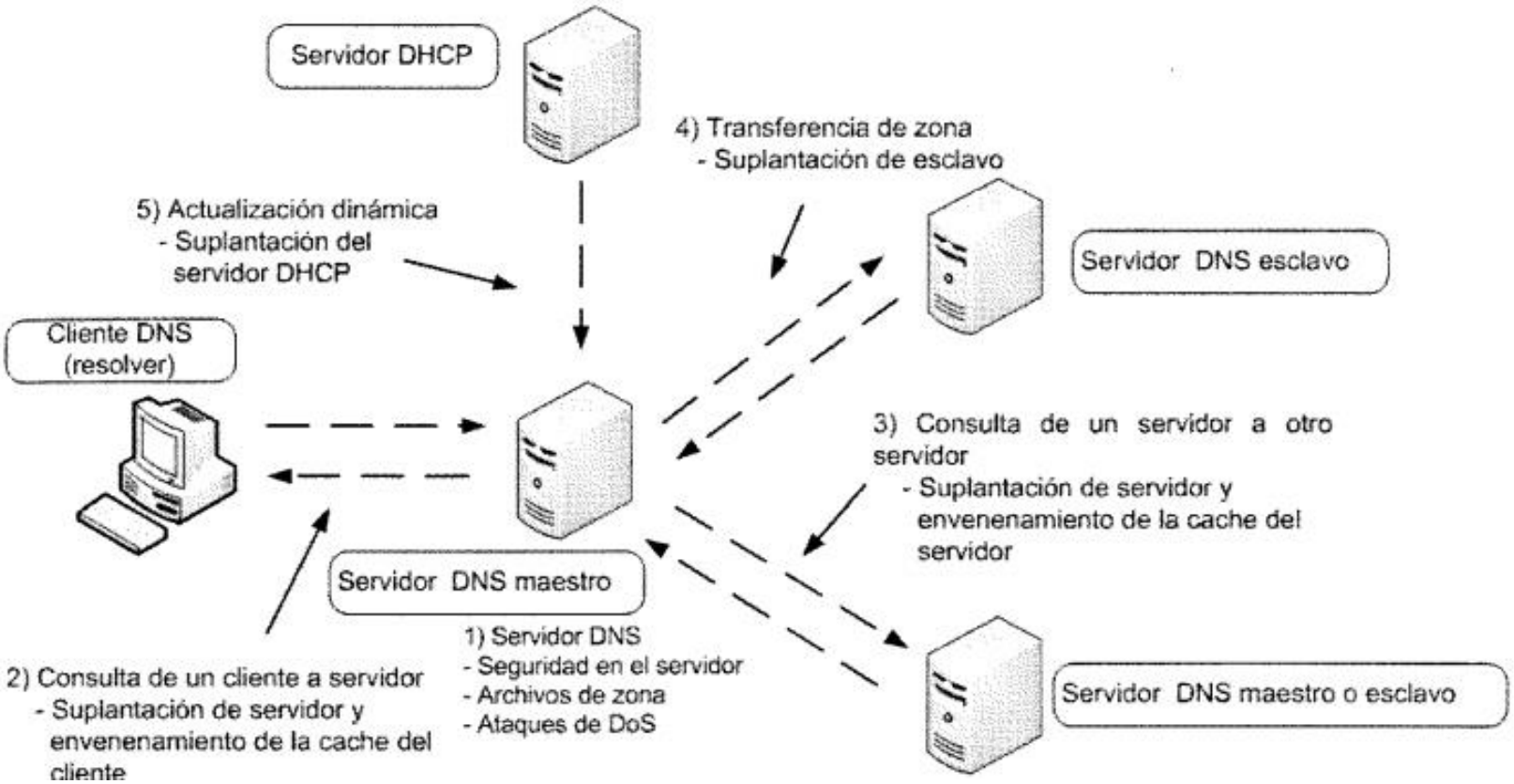
14.1 Vulnerabilidades, amenazas y ataques

- Cuando 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.

14.2. Puntos de amenaza

- Servidores DNS
  - Ataques contra el propio servidor aprovechando vulnerabilidades (uso de exploits).
  - Modificación de los archivos de zona por una mala configuración de seguridad en el sistema donde está instalado el servidor.
  - Ataques de denegación de servicio (DoS).
- Consultas de clientes DNS a otros a servidores DNS
  - Envenenamiento de la cache del cliente DNS suplantado al servidor DNS remoto y enviado registros de recursos incorrectos.
- Consultas de servidores DNS a otros a servidores DNS
  - Envenenamiento de la cache del servidor suplantado al servidor DNS remoto y enviado registros de recursos incorrectos. servidores DNS a otros a servidores DNS

14.2. Puntos de amenaza



14.3 Mecanismos de seguridad

- Las vulnerabilidades y las amenazas a DNS están relativamente controladas. Además, se han creado mecanismos para poder configurar el servicio de forma segura.
- Seguridad local en los servidores DNS
  - Actualizar a las últimas versiones y parches de seguridad.
  - En sistemas Linux/Unix ejecutar el servidor en un entorno chroot.
  - Configurar adecuadamente los privilegios de acceso a los ficheros de zonas.
  - Realizar copias de seguridad de los archivos de zona.
  - Evitar puntos de fallo y prevenir ataques de denegación de servicIO (DoS) creando al menos un servidor secundario por cada zona, distribuyendo los servidores DNS en diferentes redes y ubicaciones, etc.

14.3 Mecanismos de seguridad

- Seguridad en las transferencias de zona y en las actualizaciones dinámicas
  - Establecer a nivel de direcciones IP y/o nombres de dominio (usando listas de control de acceso) los servidores desde los que se permiten transferencias de zona y/o actualizaciones dinámicas.
  - Utilizar cortafuegos para controlar las solicitudes de transferencias de zona y 1 o actualizaciones dinámicas.
  - Mecanismos de autenticación de Active Directory en dominios Microsoft para garantizar transferencias de zona y actualizaciones dinámicas seguras.

15 Whois

- Whois es un protocolo que permite realizar consultas a bases de datos que contienen información sobre el usuario, empresa u organización que registra un nombre de dominio y lo una dirección IP en Internet. El protocol
- whois se encapsula en TCP y solo específica el intercambio de peticiones y respuestas, no el formato de datos a intercambiar. Por eso, los resultados de las consultas whois pueden ser diferentes dependiendo de la base de datos whois a la que se pregunte.
- Las consultas a bases de datos Whois se puede realizar:
  - Usando webs
  - Usando clientes instalados en un equipo.

Actividad

- Noticias sobre ataques a servidores DNS.
- Información sobre el ataque Pharming.
- Información sobre técnicas de Footprinting basadas en DNS.

Actividad

- Accede a la web http://whois.domaintools.com y consulta información sobre el nombre "google. com.".
- Inicia sesión en ubuntu abre un terminal y ejecuta whois google.com.
- Inicia sesión en ubuntuXy accede a Sistema, Administración, Herramientas de red y a la pestaña Whois. Busca información sobre el nombre de dominio que quieras.