

# DNS

Servicios de resolución de nombres

# INTRODUCCIÓN

- ▶ Cada equipo tiene asignado un nombre y una dirección
- ▶ Para el ser humano para acceder a un recurso es más sencillo recordar un nombre que una dirección.
- ▶ Ya sea en Internet o en una red privada local, los servicios de resolución de nombres juegan un papel crucial a la hora de acceder a los recursos.
- ▶ A lo largo de este tema se describirán los diferentes servicios encargados de llevar a cabo las traducciones de nombres a direcciones IP y viceversa.

# SISTEMAS DE NOMBRES PLANOS

- ▶ Identificar y acceder a equipos de una misma red, no se conoce la estructura lógica de la misma (cae en desuso)
- ▶ Arquitecturas cliente/servidor o sistemas distribuidos
- ▶ Ejemplo Sistema Distribuido:
  - ▶ NetBios (Network Basic Input-Output System)
  - ▶ Permite conocer la dirección lógica (IP) asignada a un dispositivo dentro de una red a partir de un nombre plano y sin necesidad de un servidor que centralice el servicio.
- ▶ Ejemplo Sistema Centralizado (cliente/servidor):
  - ▶ WINS ( Windows Internet Naming Service)
  - ▶ Controla las solicitudes de registro, renovación y liberación que recibe por parte de los clientes, además de responder a las consultas con la dirección IP (siempre y cuando el nombre se encuentre registrado en su base de datos).

# SISTEMAS DE NOMBRES JERÁRQUICOS

- ▶ Traducción de nombres a direcciones lógicas y viceversa
- ▶ Permite conocer la ubicación y forma de acceso a determinados servicios dentro de un dominio (conjunto de recursos que comparten parte de su identificador y que son controlados por la misma entidad)
- ▶ Ejemplo: DNS

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Qué es

- ▶ DNS es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio tanto en redes locales como en Internet.
- ▶ Como base de datos es capaz de asociar distintos tipos de información a cada nombre, pero lo más común es:
  - ▶ La asignación de nombres de dominio a direcciones IP
  - ▶ La localización de los servidores de correo electrónico de cada dominio.
- ▶ Los motivos para descentralizar a BBDD, principalmente, son:
  - ▶ Evitar tener un único punto de fallo.
  - ▶ Balancear la carga, ya que el volumen de tráfico es importante.
  - ▶ Evitar retardos derivados de la distancia que puede existir a una única BBDD centralizada.
  - ▶ Favorecer la escalabilidad del sistema

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Características y funcionamiento

- ▶ Un servidor DNS permanece en continua escucha ante posibles peticiones de los clientes que deba atender.
- ▶ Los clientes, implementarán en sus sistemas operativos el *DNS resolver*, que es el servicio encargado de realizar las consultas a los servidores DNS correspondientes, interpretar las respuestas recibidas y devolver el resultado al programa que desencadenó la consulta.
- ▶ Debido al elevado número de nombres para traducir → Varios servidores DNS para trabajar de forma jerárquica y distribuida
- ▶ Cada servidor es responsable de pequeñas parcelas de nombres conocidas como **zonas**.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Características y funcionamiento

- ▶ El protocolo DNS emplea nombres articulados jerárquicos que permiten:
  - ▶ Realizar la traducción de los mismos a direcciones IP y viceversa
  - ▶ Conocer servicios de red asociados a cada nombre
  - ▶ Conocer la estructura jerárquica del dominio en el cual se encuentra ubicado el dispositivo.
- ▶ El servicio DNS se implanta en redes locales de ámbito corporativo con la finalidad de servir de elemento traductor a los clientes que necesitan acceder a un determinado dispositivo.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Espacio de nombres y administración

- ▶ DNS se organiza conforme a un sistema jerárquico en forma de árbol invertido
- ▶ La raíz del árbol se corresponde con el dominio raíz (todo nombre de dominio finaliza con el carácter punto "." que representa dicho dominio raíz).
  - ▶ El dominio raíz es gestionado por el ICANN y está disponible en trece servidores
  - ▶ Existen centenares de réplicas de los mismos ubicadas en todo el mundo. Esta redundancia ofrece una alta disponibilidad.
  - ▶ Los servidores raíz se identifican por letras de la A a la M y sus nombres son a.root-servers.net., b.root-servers.net., . . . m.root-servers.net.
- ▶ No todos los nombres de dominio pueden alojarse bajo el dominio raíz directamente → Se distribuyen en dominios de nivel inferior llamados dominios TLD (Top Level Domain), o "dominios de primer nivel".
  - ▶ Estos dominios son delegados de la ICANN a otras organizaciones



# SISTEMAS DE NOMBRES JERÁRQUICOS

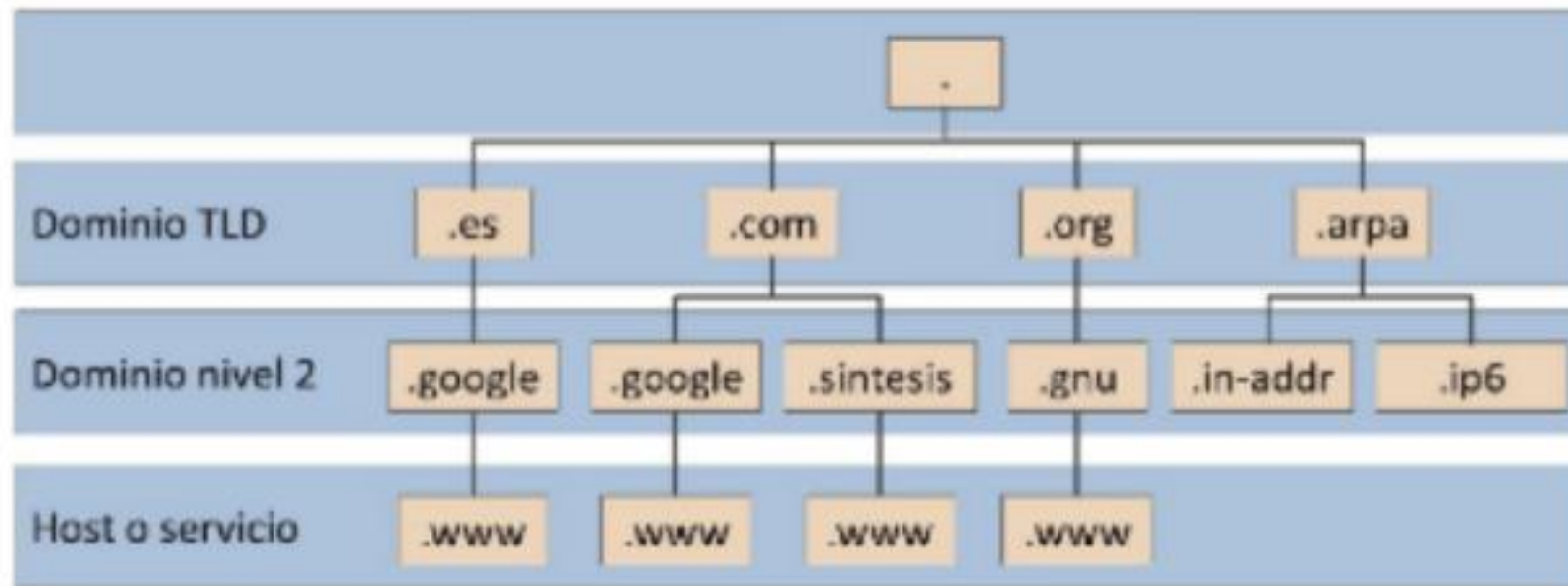
## DNS - Espacio de nombres y administración

### ► TIPOS DE TLD:

- **De infraestructura:** dominios empleados para obtener el nombre completo de una dirección IP (dominio .arpa)
- **Genéricos (gTLD):** Son dominios utilizados por un tipo concreto de organización que no pertenece a ningún país y están compuestos, como mínimo, de tres caracteres:
  - **Restringidos:** Para poder utilizarlos se debe cumplir una serie de requisitos. Ejemplos: .pro, (profesionales acreditados), o .name (utilizado para dominios personales).
  - **No restringidos:** Utilizados para cualquier finalidad. Ejemplos: .com (uso comercial), .info (uso informativo) .net (previsto inicialmente para organizaciones relacionadas con tecnologías de redes; hoy es de propósito general), .org (uso para organizaciones) ...
  - **Patrocinados:** Empleados para un fin concreto. Ejemplos: .edu (educación), .gov (Gobierno de Estados Unidos), .mil (ejército de Estados Unidos)...
  - **Comerciales:** Son de uso libre y no existen restricciones para su uso. Ejemplos: .eus (Euskadi), .gal (Galicia), .madrid (Comunidad de Madrid) ...
- **Geográficos (ccTLD):** Son dominios utilizados por países o territorios. Se componen de dos caracteres. Ejemplos: .es (España), .pt (Portugal), .ad (Andorra) ...

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Espacio de nombres y administración



Un FQDN (Full Qualified Domain Name) corresponde con un host o servicio completo.

Ejemplo: `www.google.es`

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Espacio de nombres y administración

- ▶ Cada nombre de dominio cumple que:
  - ▶ Lo forman un conjunto de hasta 127 etiquetas separadas por el carácter punto ".", donde cada etiqueta representa un nodo (dominio) y tiene una longitud máxima de 63 caracteres.
  - ▶ Su longitud total es de 255 caracteres.
  - ▶ No se hace distinción entre mayúsculas y minúsculas.
  - ▶ El proceso mediante el que un cliente (particular o empresa) alquila un dominio para su uso se denomina registro de dominio. El registro de dominio no puede realizarse sobre los servidores raíz, sino que debe hacerse contra un servidor TLD o de niveles inferiores.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ▶ Consulta el listado completo de dominios de TLD en la norma 1503166 e indica los países o los que pertenecen los dominios:

- ▶ .cu
- ▶ .de
- ▶ .fr
- ▶ .pe
- ▶ .ru

# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ▶ Accede a la web <https://root-servers.org> donde puedes ver los servidores raíz e investiga:
  - ▶ ¿Cuántos hay en España?
  - ▶ ¿Y en todo el mundo?
  - ▶ Curiosear los propietarios de dichos servidores

# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ▶ Uno de los dominios de nivel superior geográfico (ccTLD) es el dominio .tk
- ▶ Busca información acerca de este dominio y su relación con el cibercrimen.
- ▶ Investigar las características y propietarios de los dominios oficialmente registrados, que pueden encontrarse en la web <http://www.iana.org/domains/root/db/>
  - ▶ ¿Qué empresa o persona es responsable de administrar el dominio ".es"?

# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ▶ Elige un posible nombre de dominio para una nueva empresa.
- ▶ Accede a la web de algún registrador de nombres de dominio y haz la simulación de la contratación del dominio.
- ▶ ¿Qué precios y características tienen los servicios investigados?
- ▶ Realiza una tabla comparativa de los precios que ofrecen diferentes empresas registradoras de dominios.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ▶ Con whois podemos saber a quien pertenece un dominio, esto puedes realizarlo directamente desde la web [www.nic.es](http://www.nic.es) o desde whois.sc
- ▶ Obtén los datos del titular, fecha de alta y renovación del dominio, y servidores DNS de los dominios:
  - ▶ google.com
  - ▶ google.es
  - ▶ terra.es
  - ▶ yahoo.com



# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ▶ Busca en la web de la IANA las entidades que hacen de registros para
  - ▶ .gal
  - ▶ .es
  - ▶ .eu
  - ▶ .com
  - ▶ .org
  - ▶ otros tres más que sean de tu interés.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ▶ Buscar en internet el contenido de la zona raíz.
- ▶ Muestra los servidores de cuatro de los dominios de la actividad anterior

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Consultas y respuestas

- ▶ Las consultas formuladas por los DNS resolver (cliente) y las respuestas emitidas por los servicios DNS se realizan sobre el protocolo de transporte UDP.
- ▶ Las consultas pueden preguntar por una dirección correspondiente a un equipo con un nombre determinado, por un nombre asociado a una dirección concreta, por servicios para un determinado nombre del dominio ...
- ▶ Las consultas pueden ser:
  - ▶ Recursivas
  - ▶ Iterativas

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Consultas y respuestas

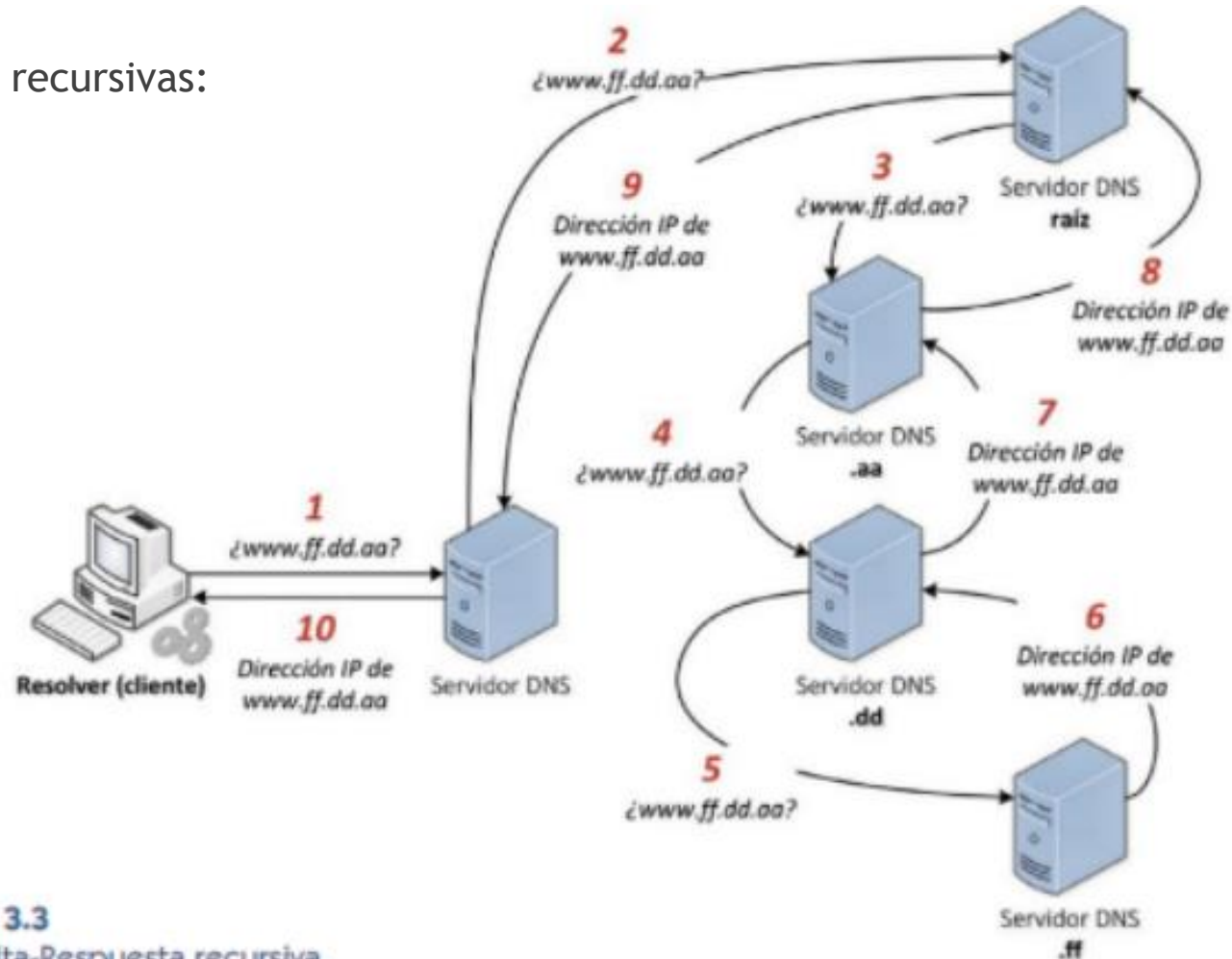
### ► Consultas recursivas:

- Se solicita al servidor DNS que conteste directamente con el resultado o con un error (en caso de no existir respuesta).
- Si la respuesta del servidor se construye con base en la información contenida dentro de las zonas que él mismo gestiona → ***Respuesta autoritativa***.
- En caso contrario, (suponiendo que el servidor no se haya configurado para rechazar consultas recursivas), el servidor actúa como intermediario, consultando al servidor que tiene la información correspondiente y almacena dicha información en su caché para posteriormente dar como respuesta → ***Respuesta no autoritativa***.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Consultas y respuestas

### ► Consultas recursivas:



**Figura 3.3**  
Consulta-Respuesta recursiva.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Consultas y respuestas

- ▶ Consultas iterativas:
  - ▶ Se solicita al servidor que conteste:
    - ▶ Con el resultado si lo conoce
    - ▶ Con un error en caso de que el recurso solicitado no exista en las zonas que gestiona directamente
    - ▶ Con un **referral**: indica una respuesta que está vacía pero que contiene uno o más servidores de nombres autorizados que contienen dicha respuesta.
- ▶ Este modo deben soportarlo todos los servidores DNS.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Consultas y respuestas

### ► Consultas iterativas:

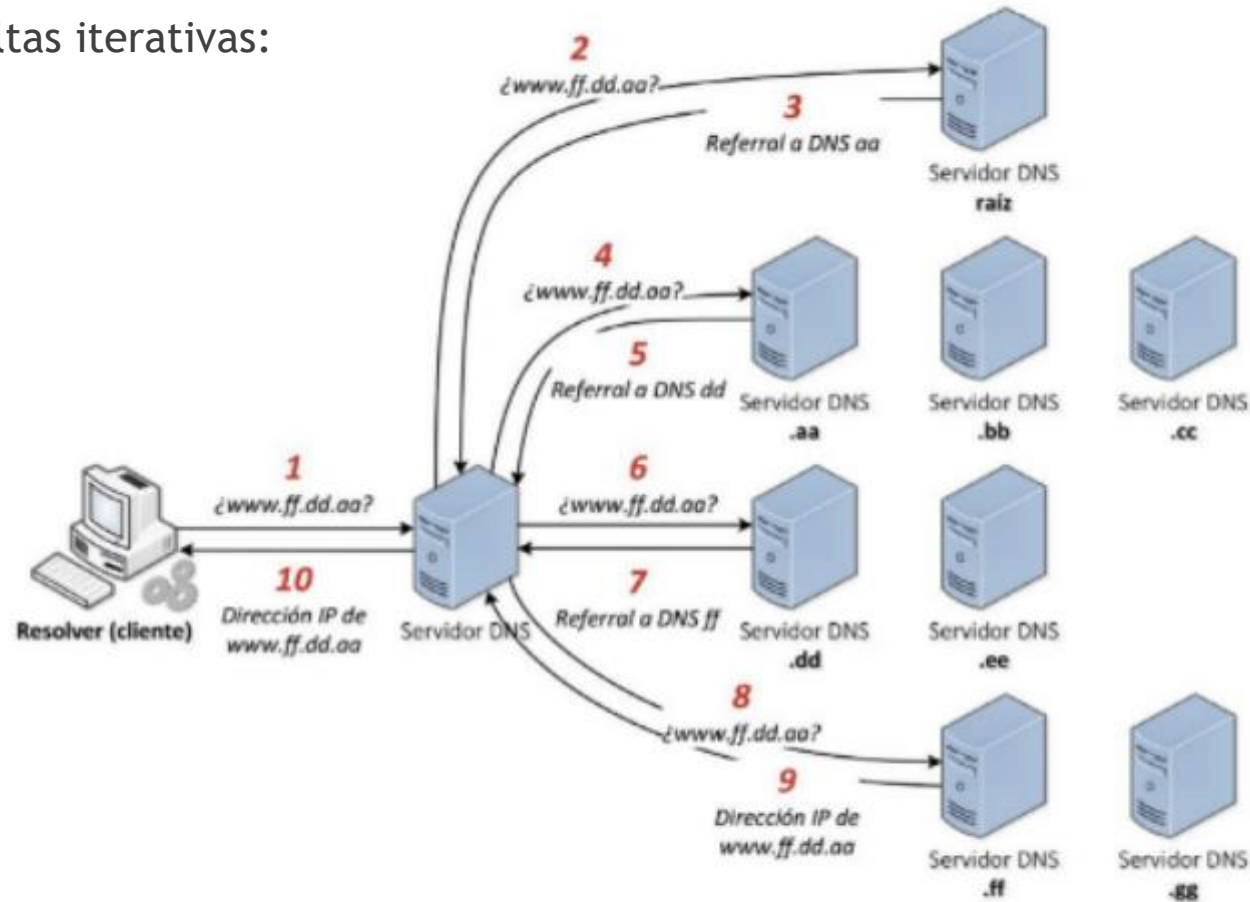


Figura 3.4  
Consulta-Respuesta iterativa.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Tipos de servidor

- ▶ Como un servidor DNS pueda estar inoperativo durante un periodo determinado →, exista más de un servidor DNS que contenga una réplica de la información de las zonas. → Tolerancia ante posibles caídas de alguno de los servidores, así como balanceo de carga entre ellos en condiciones de funcionamiento normales.
- ▶ **Servidor primario o maestro:** Los registros contenidos en la zona que maneja se gestionan directamente en él.
- ▶ **Servidor secundario o esclavo:** Los registros contenidos en la zona que maneja se obtienen a través de una sincronización con el servidor primario para dicha zona.
- ▶ **Servidor caché:** Si la información que este conoce, lo es por haber tenido que preguntar previamente a otro servidor para resolver una consulta que desconocía y tras ese paso la almacenó en su caché durante un tiempo determinado.



# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ▶ ¿Puede un servidor ser primario y secundario al mismo tiempo?
- ▶ ¿Puede un servidor ser primario y caché al mismo tiempo?

# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ▶ Prueba en un equipo con Windows, a consultar la caché DNS local mediante o comando
  - ▶ `ipconfig /displayDNS`
- ▶ Vacíala mediante el comando
  - ▶ `ipconfig /flushDNS`
- ▶ Accede a la web [www.edu.xunta.gal](http://www.edu.xunta.gal) y comprueba la caché DNS generada

# SISTEMAS DE NOMBRES JERÁRQUICOS

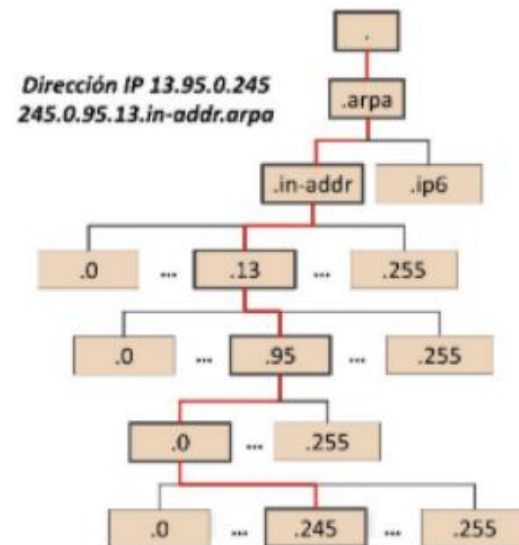
## DNS - Transferencia de zona

- ▶ Existen varios servidores con la misma información → Necesitamos un proceso de sincronización.
- ▶ La transferencia de zona, es el proceso mediante el cual los servidores de una zona, sincronizan la información que contienen → Conexión TCP desde servidor secundario (cliente) y el primario
- ▶ Las transferencias de zona se realizarán con la periodicidad declarada en el campo **Intervalo de actualización** del registro SOA, aunque se puede configurar el servicio para que el servidor primario notifique cada cambio producido en la zona haciendo uso de los mensajes **NOTIFY**.
- ▶ Las transferencias de zona pueden ser **completas** (consultas AXFR) o **incrementales** (consultas IXFR ), siendo estas más seguras y ligeras al transferirse únicamente los cambios producidos desde la última versión de la zona cargada.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Zonas de resolución directa e inversa

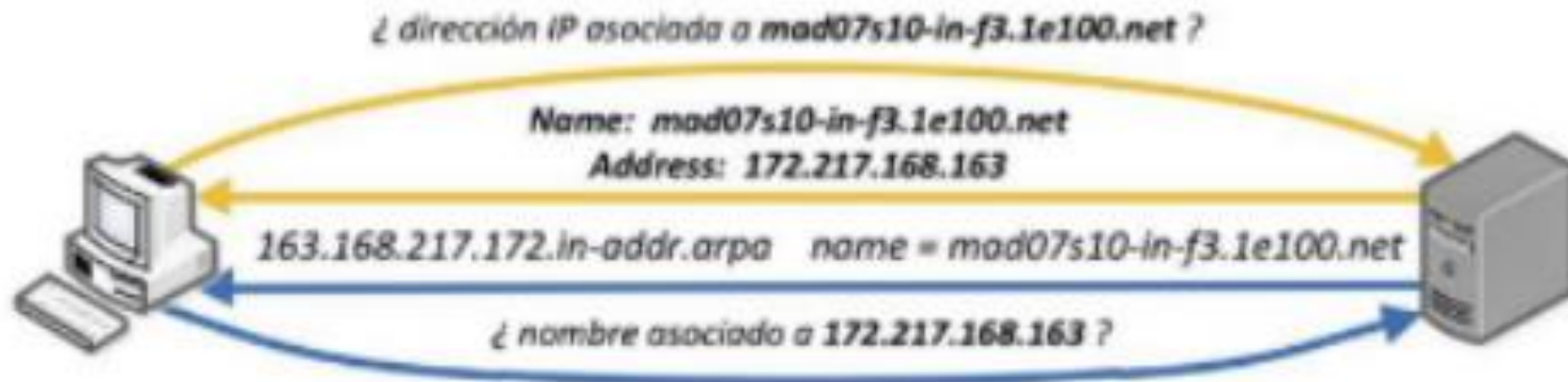
- Una **zona de resolución directa** permite la traducción de nombres DNS en direcciones IP, así como obtener información sobre los servicios de red disponibles.
- Una **zona de resolución inversa** permite la traducción de direcciones IP a nombres.
- Para IPv4 se utiliza el dominio in-addr.arpa y para IPv6 se utiliza el dominio ip6.arpa.
- Ejemplo:



**Figura 3.5**  
Jerarquía para zonas de resolución inversa.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Zonas de resolución directa e inversa



**Figura 3.6**

Intercambio de mensajes en resolución directa e inversa.

En naranja la resolución directa y en azul la inversa

# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ***nslookup*** es una herramienta de línea de comandos muy práctica y fácil de usar, cuya función básica es encontrar la dirección IP de un equipo determinado o realizar una búsqueda DNS inversa

# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ▶ Ejecutar el comando "nslookup <URL>", donde <URL> es alguna dirección web conocida.
  - ▶ Observar la salida del comando.
  - ▶ ¿Qué servidor DNS está respondiendo?
  - ▶ ¿Qué direcciones IP se asocian con la URL?

# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ▶ Ejecutar las siguientes consultas DNS y explicar los resultados:
  - ▶ `nslookup www.google.es 8.8.8.8`
  - ▶ `nslookup www.google.es ns1.google.com`



# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ▶ Obtén la dirección IP de los siguientes dominios:
  - ▶ [www.edu.xunta.gal](http://www.edu.xunta.gal)
  - ▶ [www.eltiempo.es](http://www.eltiempo.es)
  - ▶ [www.google.es](http://www.google.es)
  - ▶ [es.wikipedia.org](http://es.wikipedia.org)
  - ▶ [www.ubuntu.com](http://www.ubuntu.com)

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Delegaciones, reenvíos y sugerencias

- ▶ Cuando un servidor DNS recibe una consulta, intenta resolverla utilizando la información existente sus zonas primarias, sus zonas secundarias y su caché (siempre en este orden)
- ▶ Si la respuesta puede darse basándose en la información contenida en sus zonas (primarias o secundarias), esta será una respuesta autoritativa
- ▶ Si la información reside en su caché, será no autoritativa
- ▶ Cuando la consulta sea sobre un recurso desconocido que no se encuentra en sus zonas ni en su caché:
  - ▶ En el caso de que el recurso esté contenido en alguna zona de nivel inferior a la zona gestionada directamente por el servidor, se deberá delegar la responsabilidad de responder sobre el servidor DNS autorizado para dicha zona (estas delegaciones se irán produciendo en orden descendente).
  - ▶ Ejemplo: Un servidor DNS encargado de resolver el dominio ejemplo.local recibe una consulta para resolver pc1.subdominio.ejemplo.local; en este caso, se delega la responsabilidad de resolver la consulta sobre el servidor autorizado del dominio subdomnio.ejemplo.local.

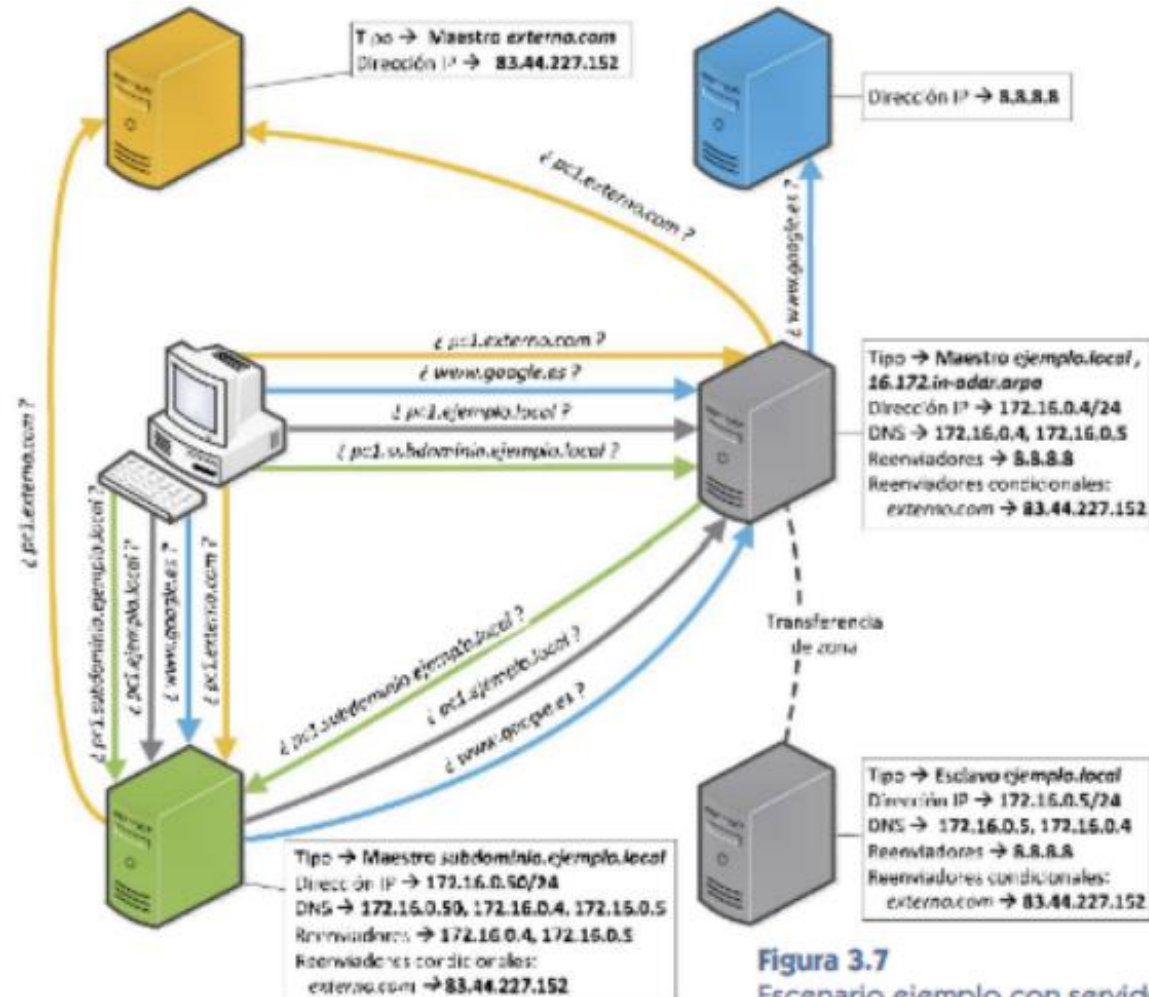
# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Delegaciones, reenvíos y sugerencias

- ▶ Cuando la consulta sea sobre un recurso desconocido que no se encuentra en sus zonas ni en su caché:
  - ▶ Cuando el recurso esté fuera de la zona gestionada de forma directa, y también de cualquier zona de nivel inferior, deberá ser otro servidor el encargado de hacer la resolución.
    - ▶ Si se han declarado reenviadores. será a estos a quienes se les envíe una consulta recursiva quedando a la espera de respuesta. Estos pueden ser:
      - ▶ **Absolutos:** Si las consultas se reenvían directamente.
      - ▶ **Condicionales:** Si las consulta se reenvían a un servidor concreto basándose en el sufijo DNS del nombre de dominio buscado.
    - ▶ Si no se han declarado reenviadores o si no se ha podido contactar con ellos en un periodo de tiempo determinado, se enviará una consulta iterativa a uno de los servidores DNS especificados en las sugerencias de raíz DNS.
    - ▶ En el ejemplo se puede ver reenviadores absolutos y condicionales configurados sobre los servidores de dominio de ejemplo.local y subdominio.ejemplo.local, de manera que las consultas recibidas sobre recursos por ellos desconocidos se reenvían al servidor 8.8.8.8 a excepción de aquellas que estén contenidas dentro del dominio externo.com, que se reenvían al servidor autorizado de dicho dominio

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Delegaciones, reenvíos y sugerencias



**Figura 3.7**  
Escenario ejemplo con servidores secundarios, delegados y reenviadores.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Tipos de registros

- ▶ Dentro de las zonas de resolución directa o inversa se pueden encontrar diferentes registros destinados a contener la información que el servidor deberá resolver.
- ▶ Cada registro tiene una serie de campos en los que se almacena su información.
  - ▶ **Nombre del dominio:** Contiene el nombre del dispositivo en el cual se encuentra el recurso que se está describiendo.
  - ▶ **TTL (Time to live):** Indica el tiempo que puede permanecer dicho registro almacenado en la caché de un servidor DNS. Puede indicarse en segundos, minutos, horas, días o semanas, o no indicarse, en cuyo caso se tomará el valor general de la zona.
  - ▶ **Clase:** Hace referencia a la familia de protocolos que se empleará.
    - ▶ IN: Para registros DNS comunes que involucren nombres de host, servidores o direcciones IP
    - ▶ HS: Empleado para compartir información sobre diversas bases de datos de sistemas, como usuarios, grupos, impresoras, etc.
    - ▶ CH: desuso
  - ▶ **Tipo:** Es el tipo de registro (lo veremos a continuación)
  - ▶ **Datos:** Contiene la información que registrar y depende del tipo de registro. Puede ser una dirección IP, un nombre ...

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Tipos de registros

- ▶ **Registro A (Address):** Contiene la correspondencia entre un nombre y su dirección IPv4
- ▶ **Registro AAAA:** Contiene la dirección correspondiente al nombre es una dirección Pv6.
- ▶ **Registro CNAME (Canonical Name):** Conocido como "alias", contiene la correspondencia de un nombre alternativo a un registro ya existente. Por ejemplo cuando tenemos dos servicios en el servidor (ftp y web) pero usan una misma IP.
- ▶ **Registro NS (Name Server):** Define la asociación que existe entre un nombre de dominio y los servidores con autoridad para ese dominio.
- ▶ **Registro MX (Mail Exchanger):** Registro empleado para indicar los servidores de correo electrónico de la zona
- ▶ **Registro PTR (Pointer):** Traduce direcciones IP a nombres de dominio.
- ▶ **Registro TXT (Text):** Permite al administrador insertar texto en un registro DNS.
- ▶ **Registro SRV (Service):** Ofrece información acerca de otros servicios diferentes al de correo electrónico o de resolución de nombres disponibles en la zona.
- ▶ **Registro SOA (Start of Authority):** Proporciona información sobre el servidor DNS primario de la zona.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## Tarea

- ▶ ¿Qué diferencia el campo “intervalo de actualización” del campo “intervalo de reintento”?
- ▶ ¿Qué tipo de registro se encuentra únicamente en las zonas de resolución inverso?
- ▶ Si un registro MX dispone de un valor en Preference de 10 y otro registro similar dispone de un valor en Preference de 20, ¿cuál de los dos registros MX tendrá menor prioridad?
- ▶ ¿Qué campo se utiliza para diferenciar la versión de la zona?
- ▶ Indica el nombre de tres tipos de registros que requieran de la existencia de registros A o AAAA.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Tipos de registros

- ▶ **dig** es un comando que permite realizar consultas a servidores DNS para obtener información relacionada con este servicio
- ▶ Instalación en Linux Debian y Ubuntu:
  - ▶ `apt-get install dnsutils`
- ▶ Comprobación:
  - ▶ `dig -v`
- ▶ Sintaxis
  - ▶ `dig [servidor] [nombre] [tipo]`
    - ▶ [servidor] - la dirección IP o el hostname del nombre del servidor a consultar. Esto es opcional y si no proporcionas un argumento de servidor, dig utiliza los nombres de servidores que figuran en `/etc/resolv.conf`.
    - ▶ [nombre] - el nombre del registro de recursos que se debe buscar.
    - ▶ [tipo] - el tipo de consulta solicitada por dig. Por ejemplo, puede ser un registro A, un registro MX, un registro SOA o cualquier otro tipo. De forma predeterminada, dig realiza una búsqueda de un registro A si no se especifica ningún argumento de tipo



# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Tipos de registros

### ► Uso de dig:

- Consultar un nombre de dominio

```
dig xunta.gal
```

- Respuestas cortas:

```
dig xunta.gal +short
```

- Respuestas detalladas:

```
dig xunta.gal +noall +answer
```

- Especificar servidores de nombres

```
dig @8.8.8.8 xunta.gal
```

- Consultar todos los registros DNS

```
dig xunta.gal ANY
```

- Buscar por tipo de registro

```
dig xunta.gal MX / dig xunta.gal NS...
```

- Trazar la ruta DNS

```
dig xunta.gal +trace
```

- Búsqueda inversa DNS

```
dig +answer -x <IP> / dig +answer -x 10.180.188.36
```

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Tipos de registros

- ▶ Usando el comando dig (Investiga que parámetros puede llevar) y realiza los siguientes ejercicios:
- ▶ Preguntas a registros tipo NS:
  - ▶ Obtén la dirección y los servidores DNS que corresponden a los siguientes dominios: dominio raíz, com, org, es, uvigo.es, wikipedia.org, ubuntu.com
- ▶ Preguntas a registros MX:
  - ▶ Obtén el nombre y la dirección del ordenador al que se mandan los correos que se envían a los siguientes dominios: uvigo.es, us.es, wikipedia.org, ubuntu.com
- ▶ ¿Qué tipo de registro es el que resuelve las siguientes direcciones: es.wikipedia.org, uvigo.es. Indica el nombre canónico de las máquinas a las que corresponden.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Tipos de registros

- ▶ Ejecutar el siguiente comando y observar la salida:
  - ▶ `dig google.es +trace`
- ▶ Ejecutar los siguientes comandos para obtener los registros DNS de una web conocida:
  - ▶ `dig @8.8.8.8 xunta.gal SOA / dig xunta.gal SOA`
  - ▶ `dig @8.8.8.8 xunta.gal NS / dig xunta.gal NS`
  - ▶ `dig @8.8.8.8 xunta.gal A / dig xunta.gal A`
- ▶ ¿Qué diferencia hay entre usar el servidor de Google y no usarlo?

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Tipos de registros

- ▶ Realiza un dig sobre el registro NS de uvigo.es
  - ▶ ¿Sabemos cual es el servidor primario?
  - ▶ Si no es así, con qué registro podemos saberlo y cual es?
- ▶ Determinar el nombre de dominio para 147.96.85.71 partiendo del servidor raíz a.root-servers.net. ¿Qué comando se usa y con que opciones?

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Tipos de registros

- ▶ **host (Linux)**: El comando host es una utilidad simple para realizar búsquedas de DNS.
- ▶ Normalmente se utiliza para convertir nombres a direcciones IP y viceversa.
- ▶ Cuando no se le dan argumentos ni opciones, host imprime un breve resumen de sus argumentos y opciones de línea de comandos.
- ▶ Le debemos pasar el nombre que dominio que queremos buscar. También puede ser una dirección IPv4 decimal con puntos o bien una dirección IPv6 delimitada por puntos, en cuyo caso el host realizará por defecto una búsqueda inversa para esa dirección.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Tipos de registros

- ▶ Uso:
  - ▶ `host nombre_dominio`
    - ▶ `host google.es` → Devuelve la IP del dominio
  - ▶ `host ip`
    - ▶ `host 46.50.10.6` → Devuelve el dominio de la IP
- ▶ Para que se nos muestre más información debemos habilitar el modo «verbose», que se encuentra en la mayoría de los comandos en GNU/Linux. Para ello debemos utilizar los parámetros “-v” o bien “-a”
- ▶ Para especificar el tipo de consulta que queremos hacer debemos utilizar el parámetro “-t”, por ejemplo, la consulta de resolución de nombres con “ns”
  - ▶ `host -t ns nombre_dominio`
  - ▶ `host -t SOA nombre_dominio`
- ▶ También podemos consultar directamente los registros SOA en servidores de nombre autorizados, con el parámetro “-C”
- ▶ Para enumerar todos los hosts de un dominio se usa la opción -l

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - Actualizaciones dinámicas

- ▶ Todo esto ocurre porque las IP de nuestros servidores son estáticas y se encuentra vinculada a un nombre de dominio.
- ▶ Puede ocurrir que por algún motivo las IP del servidor sea dinámica
  - ▶ Existe una variable llamada DDNS es posible actualizar automáticamente la información relativa a un nombre de dominio en un DNS, de manera que siempre será posible obtener la dirección IP asociada a dicho nombre independientemente de que esta varíe
- ▶ Ejemplo: Clientes que obtienen su IP y dominio por DHCP. La información DNS puede actualizarse equipo a equipo de forma manual, pero es más práctico realizarlo directamente desde el servidor
- ▶ Ejemplo: Se pretende instalar un servidor en un entorno doméstico para ofrecer servicio a Internet. En estos entornos, los servidores se encuentran tras un router cuya dirección IP pública es dinámica, salvo que se contrate lo contrario con el ISP. Esta situación dificulta el acceso al servicio, el cual debe realizarse a través de la IP que irá variando o a través de un nombre que deberá estar actualizado en todo momento.

# SISTEMAS DE NOMBRES JERÁRQUICOS

## DNS - DNS Seguro

- ▶ El servicio DNSSEC añade una capa extra de seguridad a los servidores DNS de un dominio con la finalidad de evitar que un atacante pueda falsificar datos DNS mediante un envenenamiento de caché DNS.
- ▶ Los datos que obtendrá un cliente mediante este servicio serán auténticos e íntegros. Se utiliza un mecanismo de cifrado asimétrico de clave pública.
- ▶ Para poder hacer uso de este servicio, es preciso que los servidores DNS autoritativos dispongan de la versión firmada del dominio.
- ▶ No todos los servidores DNS soportan DNSSEC.



# RESUMEN DNS

- ▶ Existen varios mecanismos que permiten llevar a cabo la traducción de nombres a direcciones IP y viceversa.
  - ▶ sistemas basados en nombres planos como NetBIOS y WINS
  - ▶ sistemas basados en nombres jerárquicos como DNS
- ▶ DNS se organiza conforme a un sistema jerárquico en forma de árbol invertido, en el que el elemento raíz del árbol se corresponde con el dominio raíz. Este lo gestiona el ICANN y está disponible en trece servidores con centenares de réplicas por todo el mundo. El siguiente nivel está formado por dominios TLD.
- ▶ Las consultas DNS pueden ser recursivas o iterativas y todos los servidores deben atender como mínimo a las iterativas.

# RESUMEN DNS

- ▶ Para que un servidor resuelva consultas de nombre a IP, debe crearse una zona de resolución directa; para las resoluciones opuestas, debe crearse una zona de resolución inversa.
- ▶ Un servidor DNS puede trabajar como servidor maestro (la información la maneja de primera mano), esclavo (la información la obtiene desde un maestro mediante una "Transferencia de zona"), caché (la información la obtiene al preguntar a otros servidores) o como una combinación de los anteriores.
- ▶ Cuando la información no se encuentra contenida en la zona que un servidor gestiona:
  - ▶ Reenvía la consulta a otro servidor si es sobre recursos que están en otra zona ajena. Si este proceso falla, se hace la consulta pertinente a un servidor raíz.
  - ▶ Delega la consulta en otro servidor si es sobre recursos que están en una subzona.
- ▶ Existen diferentes tipos de registros para identificar cada tipo de información.
- ▶ Los servidores DNS pueden admitir actualizaciones dinámicas por parte de clientes o servidores DHCP.
- ▶ El *resolver* es el componente cliente encargado de consultar al DNS para conseguir la dirección IP. Existen varios tipos de herramientas que permiten interrogar a servidores DNS (nslookup, dig o host son algunas de ellas).

# SISTEMAS DE NOMBRES JERÁRQUICOS

## TAREA

- ▶ Captura y análisis del tráfico DNS con Wireshark
  - ▶ Esta tarea consiste en utilizar un sniffer de red para analizar los mensajes intercambiados entre un cliente e un servidor DNS.
  - ▶ El primer paso consistirá en interceptar el tráfico DNS entre un equipo cliente e un servidor DNS al intentar visitar el dominio `www.edu.xunta.gal`.
  - ▶ A continuación habrá que configurar en el equipo cliente un servidor DNS inexistente para comprobar como los navegadores web almacenan las resoluciones DNS en su caché y como esta se vacía por defecto al reiniciarse la aplicación.
  - ▶ Por último, se configurará el fichero hosts con una dupla IP-dominio con el fin de enseñar que es el DNS spoofing y cómo funciona.