

# Índice hora 4

## *Hora 1*

- 1 Aplicaciones de red
- 2 World Wide Web/HTTP

## *Hora 2*

### *HTTP*

## *Hora 3*

- 2.4 Autenticación básica de usuarios HTTP
- 2.5 Seguimiento de estado
- 2.6 Caché
- 2.7 CGIs
- 2.8 Proxy web
- 2.9 HTTP seguro

## **Hora 4**

- 3 Resolución de nombres DNS**
  - 3.1 Tipos de servidores de nombres
  - 3.2 Top-level domains
  - 3.3 Proceso de consulta DNS
  - [...]
- 4 Transferencia de archivos/FTP**
  - 4.1 Comandos y códigos FTP
  - 4.2 TFTP

## *Hora 5*

- 5 Correo electrónico/SMTP,POP3,IMAP

## *Hora 6*

- 6 Multimedia

## *Hora 7*

- 7 Multimedia /VoIP

## Objetivos

- Entender la necesidad de un sistema de mapeo de direcciones IP a nombres de máquinas
- Describir el funcionamiento del protocolo DNS
- Comprender la escalabilidad del servicio DNS
- Revisar el funcionamiento del protocolo FTP
- Entender FTP como un protocolo con señalización fuera de banda
- Presentar una simplificación del protocolo FTP: TFTP

## 3 Resolución de nombres DNS

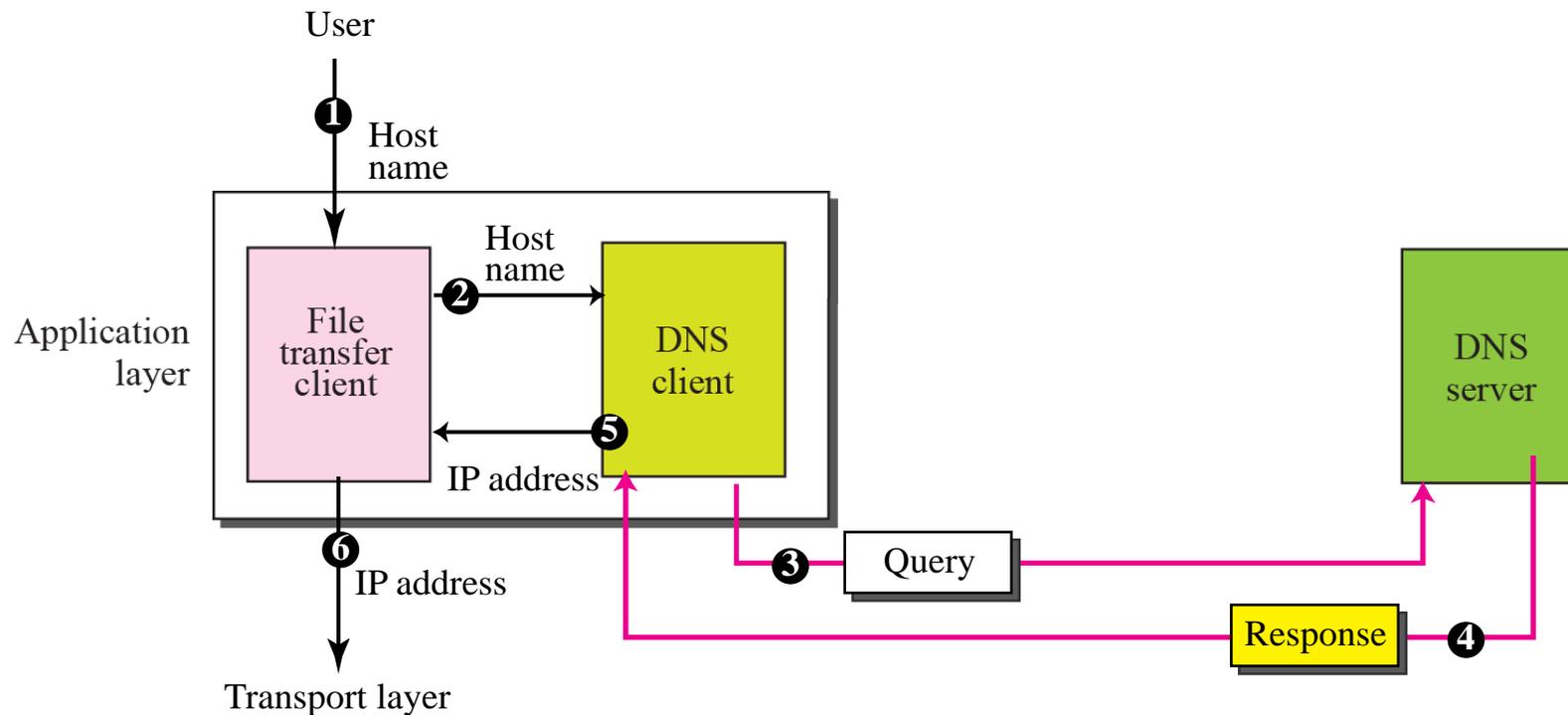
- Las direcciones IP identifican unívocamente cualquier máquina en Internet (por ejemplo, el servidor web de la UPNA 130.206.159.45)
- Para evitar que tener que “aprender” direcciones IP, se asignan alias de esas direcciones IP en forma de nombres simbólicos o de DNS más fáciles de recordar (por ejemplo, el servidor web de la UPNA [www.unavarra.es](http://www.unavarra.es))
  - Deberán ser nombres únicos. Registro en ICANN/IANA.
- Se hace necesario un sistema de mapeo
  - De nombre de simbólico a dirección IP: resolución directa
    - que hace el navegador cuando coloco [www.unavarra.es](http://www.unavarra.es) en la barra de navegación
  - De dirección IP a nombre simbólico: resolución inversa
    - que puede hacer el servidor para tratar de identificar datos del cliente que se le conecta a partir de su dirección IP

## Resolución de nombres DNS

- DNS (Domain Name Service): protocolo de resolución de nombres
- RFC1034
- Encapsulado en UDP/TCP con puerto de servidor 53
  - Para peticiones cortas ( $\leq 512$ bytes): UDP
  - Para intercambios de información mayores: TCP
- Se trata de una base de datos distribuida con servidores organizados jerárquicamente
  - Escalabilidad: evita
    - Un solo punto de fallo
    - Alto volumen de tráfico en ese punto
    - Tener el servidor DNS lejos del cliente
    - Facilita el mantenimiento/actualizaciones
- Realiza una función fundamental para el funcionamiento del resto de protocolos de nivel de aplicación

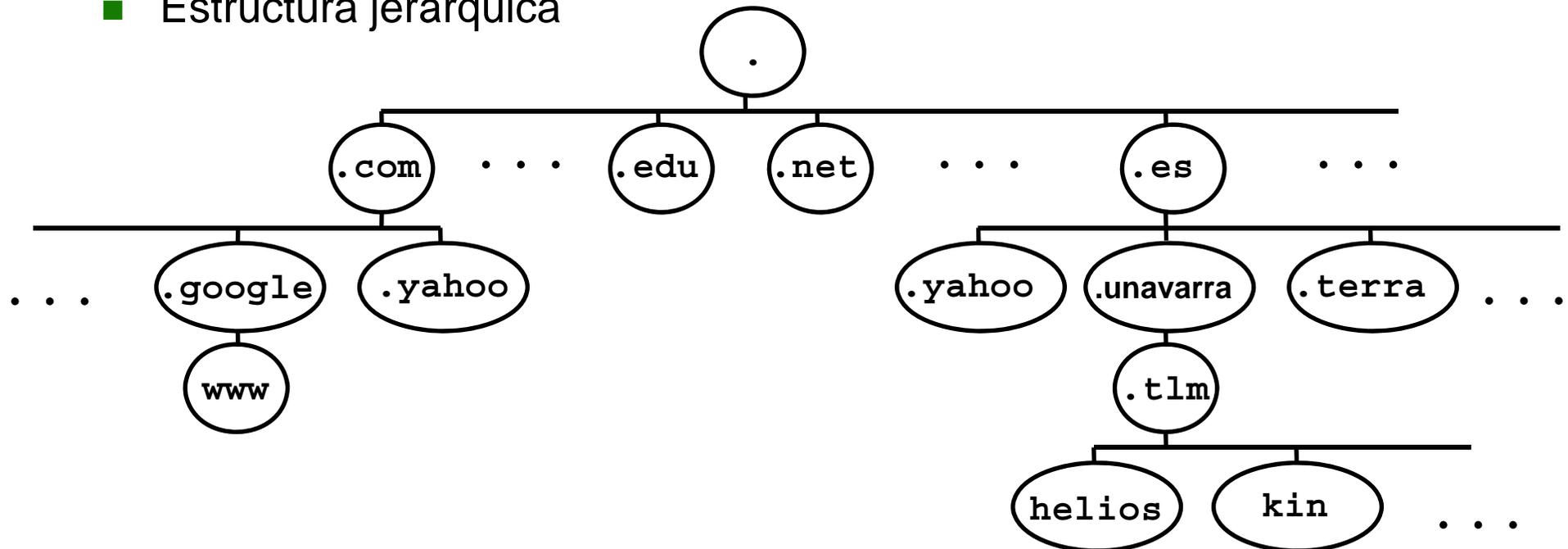
## Cliente/servidor DNS

- EL cliente DNS puede ser una aplicación (específica como nslookup o dig) o un servicio proporcionado por el sistema operativo
- El servidor DNS es una aplicación capaz de resolver la petición de DNS con información local o acudiendo a otros servidores



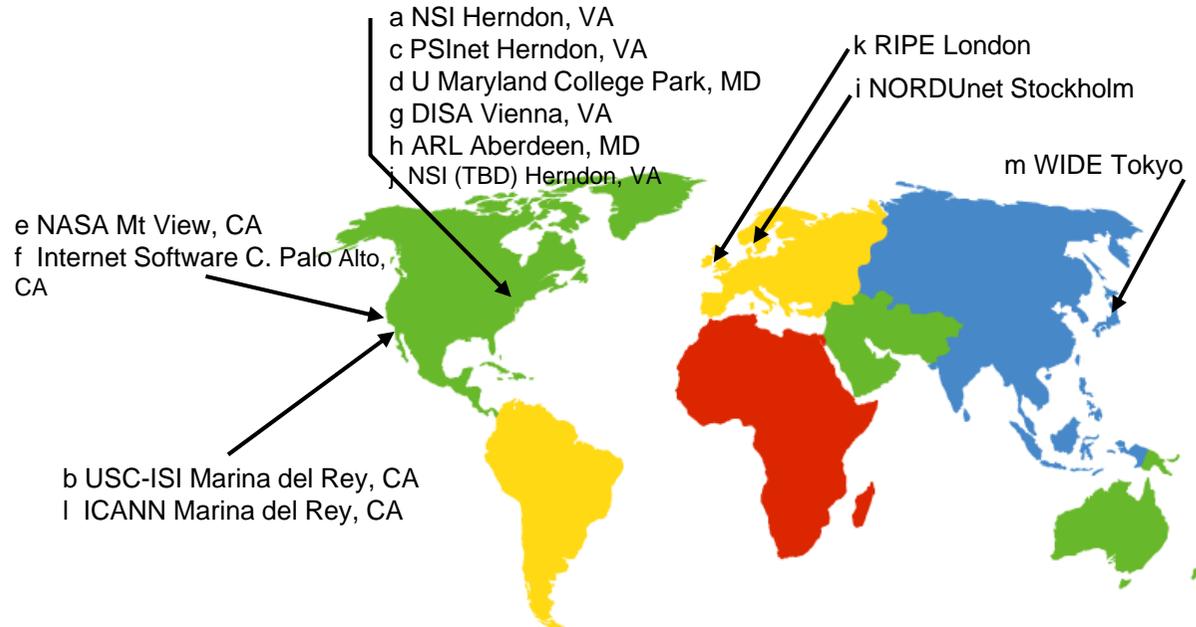
# Dominios DNS

- Los nombres de DNS están formados por segmentos alfanuméricos separados por puntos (no distingue mayúsculas)
- Ejemplo: kin.tlm.unavarra.es
  - kin: nombre de la máquina en el dominio
  - tlm.unavarra.es: nombre del dominio
- Estructura jerárquica



## 3.1 Tipos de servidores de nombres

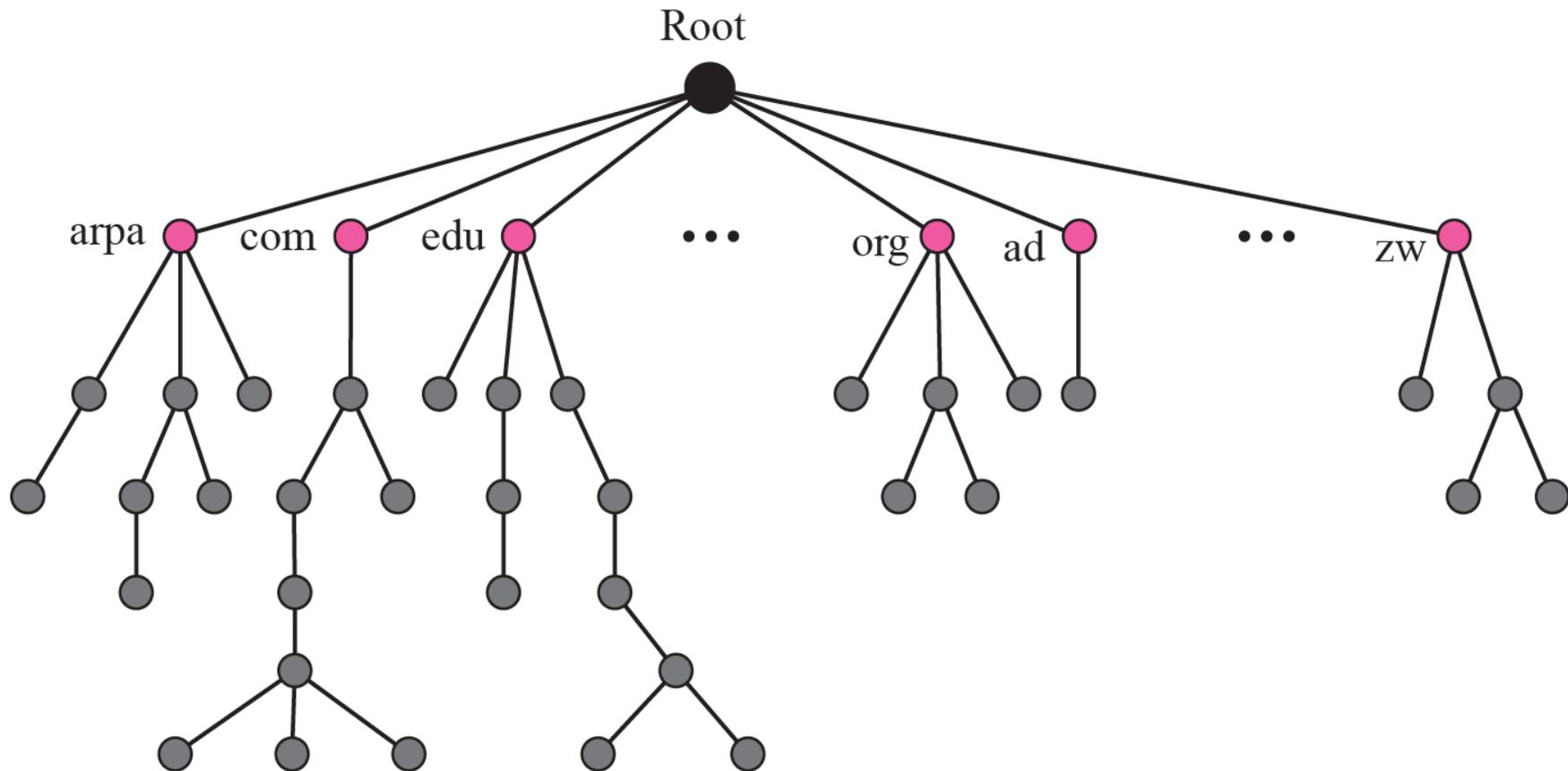
- Servidores de nombres raiz
  - 13 en el mundo: a.root-servers.net - m.root-servers.net
  - En el fichero de configuración del resto de servidores de DNS (autoritativos y locales)



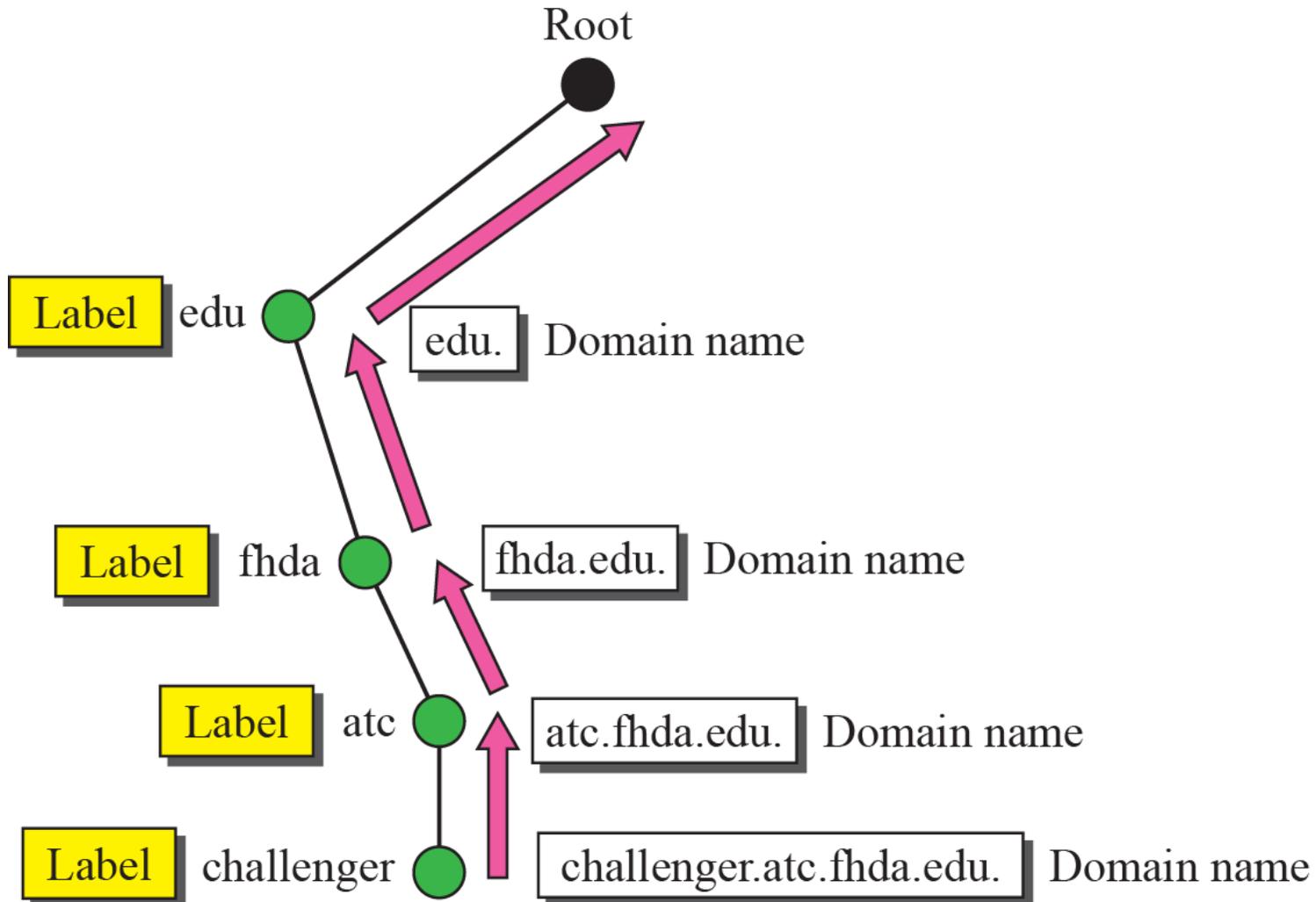
## Tipos de servidores de nombres

- Servidor de nombres autoritativo (authoritative server)
  - Responsables de alojar el registro (mapeo autorizado) para los nombres de determinado dominio DNS
  - Para un host: almacena la dirección IP y el nombre de ese host
  - Puede hacer la traducción de nombre a dirección IP para ese host
- Servidor de nombres local
  - Cada ISP o compañía tiene un local (default) name server
  - Las consultas que realizan los nodos primero se hacen con el local name server

# Base de datos jerárquica y distribuida



# Base de datos jerárquica y distribuida

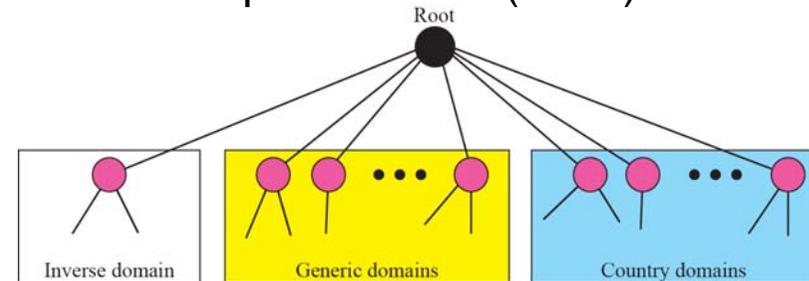


## 3.2 Top-level domains

- Fully Qualified Domain Name (FQDN)
  - En realidad la raíz del árbol tiene también “nombre” pero es nulo
  - Un FQDN incluye el nombre hasta la raíz, o sea, termina en un “.”
    - Ej: www.tlm.unavarra.es.

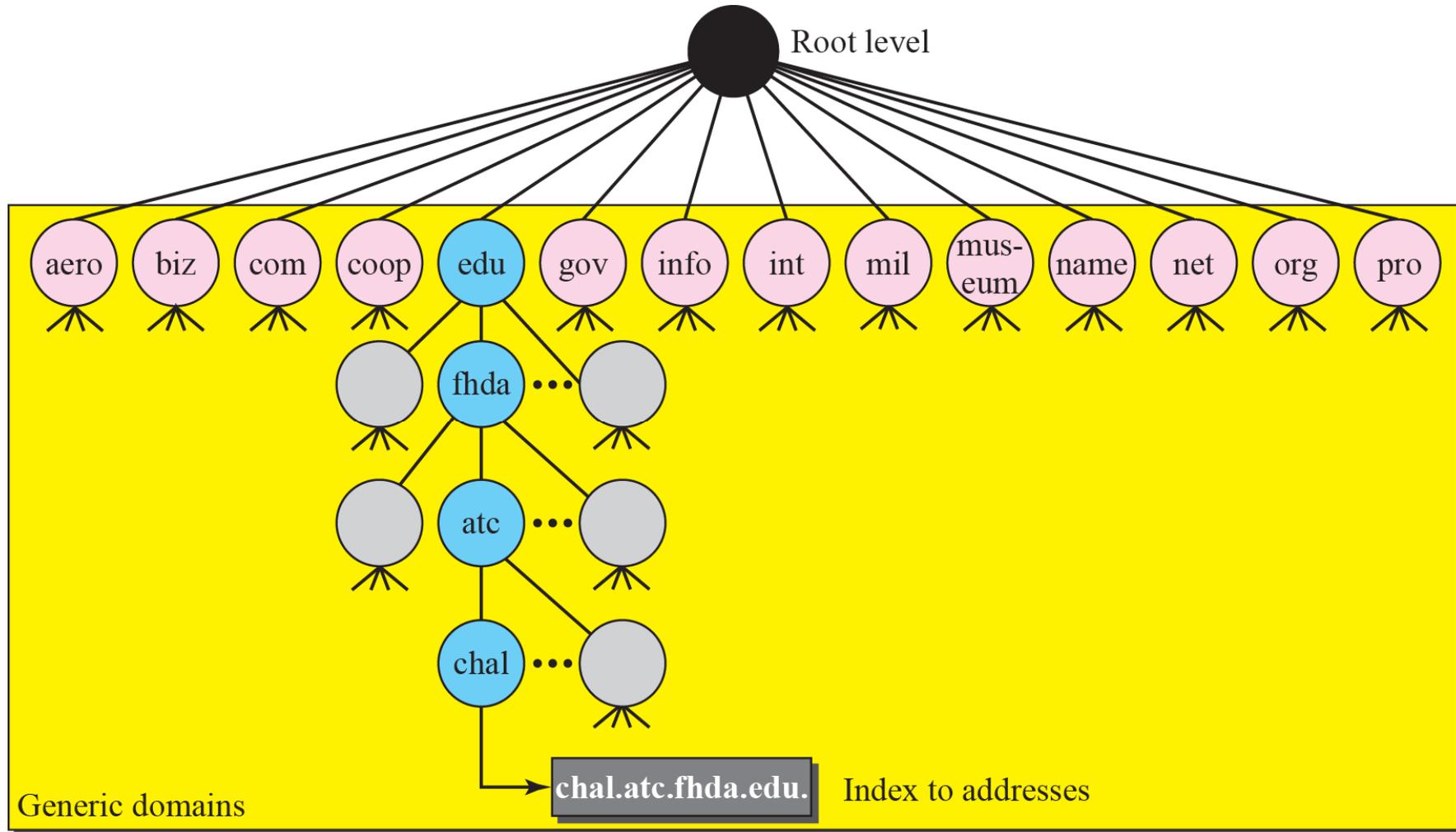
- Servidores autoritarios de Top-Level Domains (TLD)
  - Corresponden a los segmentos de dominio de primer nivel (.com)

- Tipos de Top-Level Domains
  - Genéricos: .com, .net, .org, etc.
  - De países: .us, .es, .fr, .eu, etc.
  - Inversos: resolución inversa



- Cualquiera puede registrar un subdominio dentro del TLD que elija
  - Entidades registradoras de dominios, acreditadas por la ICANN
  - ESNIC para el TLD .es (<http://www.nic.es>)

# TLDs

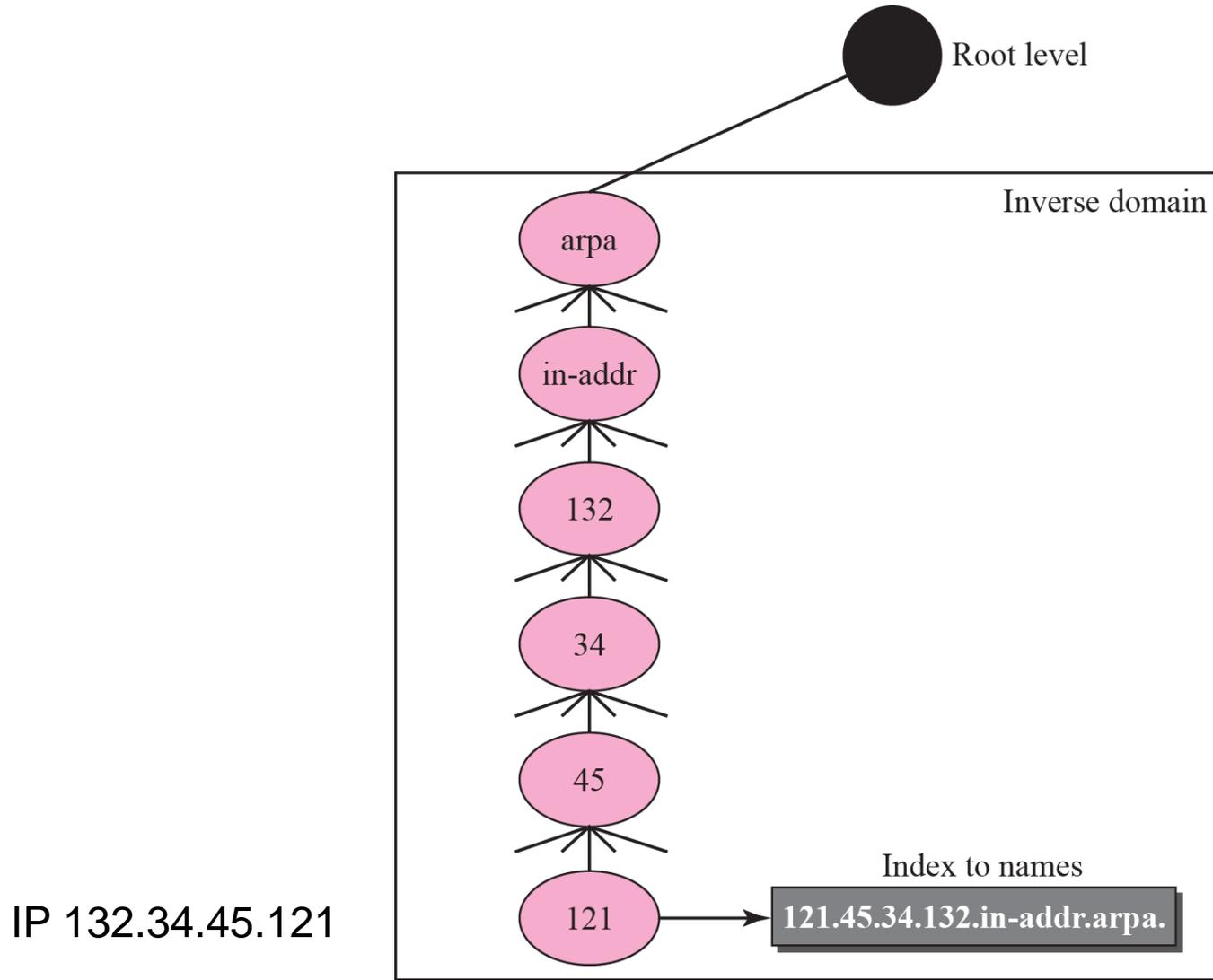


# TLDs

**Table 19.1** *Generic domain labels*

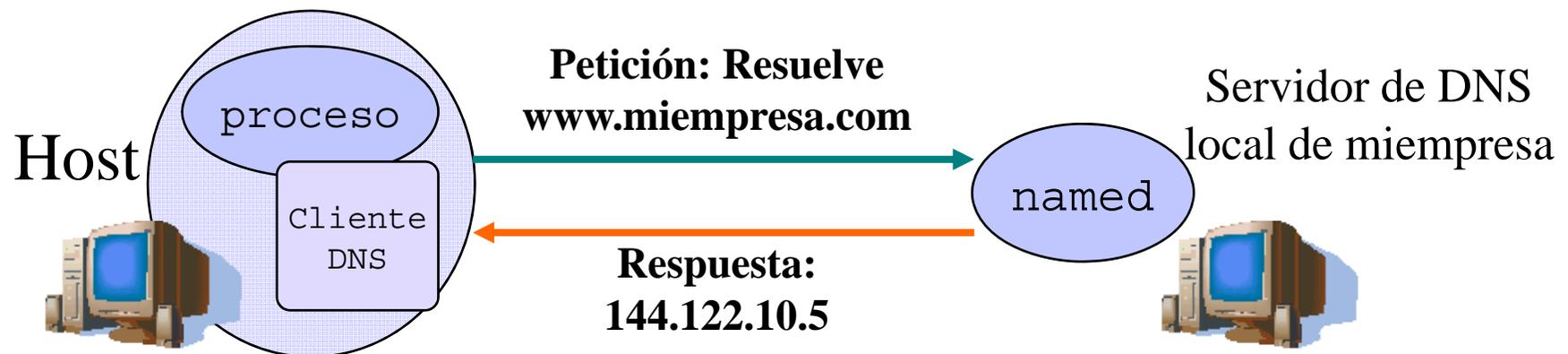
<i>Label</i>	<i>Description</i>
<b>aero</b>	Airlines and aerospace companies
<b>biz</b>	Businesses or firms (similar to “com”)
<b>com</b>	Commercial organizations
<b>coop</b>	Cooperative business organizations
<b>edu</b>	Educational institutions
<b>gov</b>	Government institutions
<b>info</b>	Information service providers
<b>int</b>	International organizations
<b>mil</b>	Military groups
<b>museum</b>	Museums and other non-profit organizations
<b>name</b>	Personal names (individuals)
<b>net</b>	Network support centers
<b>org</b>	Nonprofit organizations
<b>pro</b>	Professional individual organizations

# TLDs, resoluciones inversas



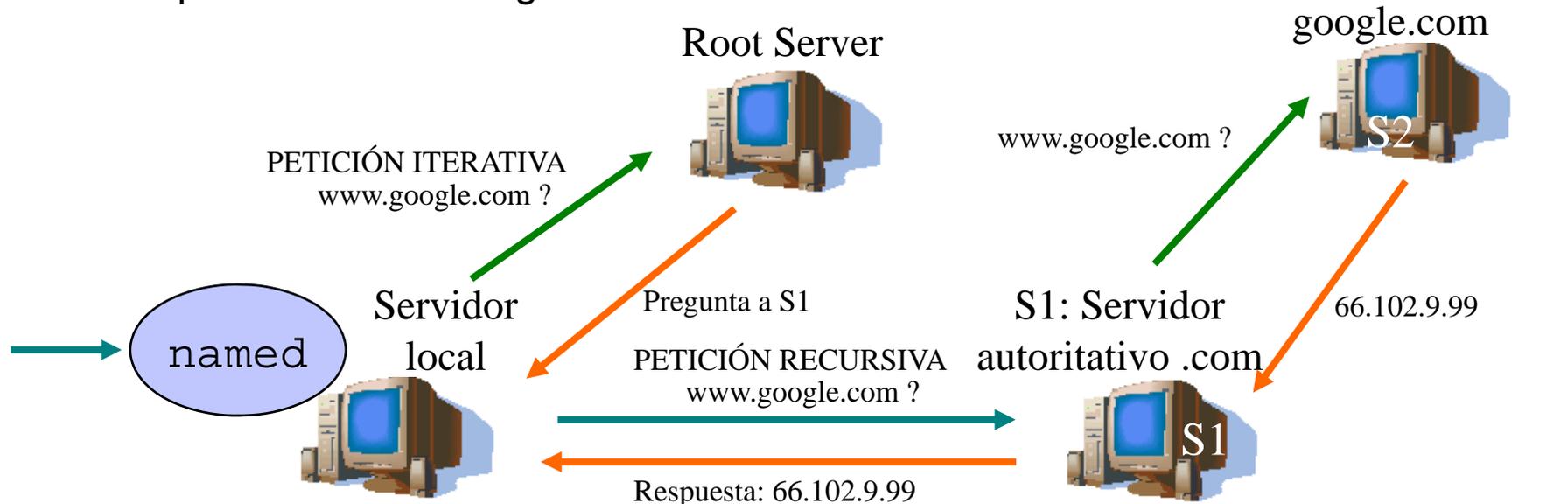
## 3.3 Proceso de consulta DNS

- Los hosts tienen configurado a su servidor de nombres local (proporcionado por el ISP, la empresa u organización)
- Cuando un host desea resolver un nombre hace la petición a su servidor local el cual le devuelve la respuesta
- ¿Cómo conoce la respuesta el servidor local?
  - Si es el servidor autoritario para el dominio que se solicita, él tiene la porción de la base de datos distribuida en la que está el mapeo
  - Si no lo es preguntará a un Root Server



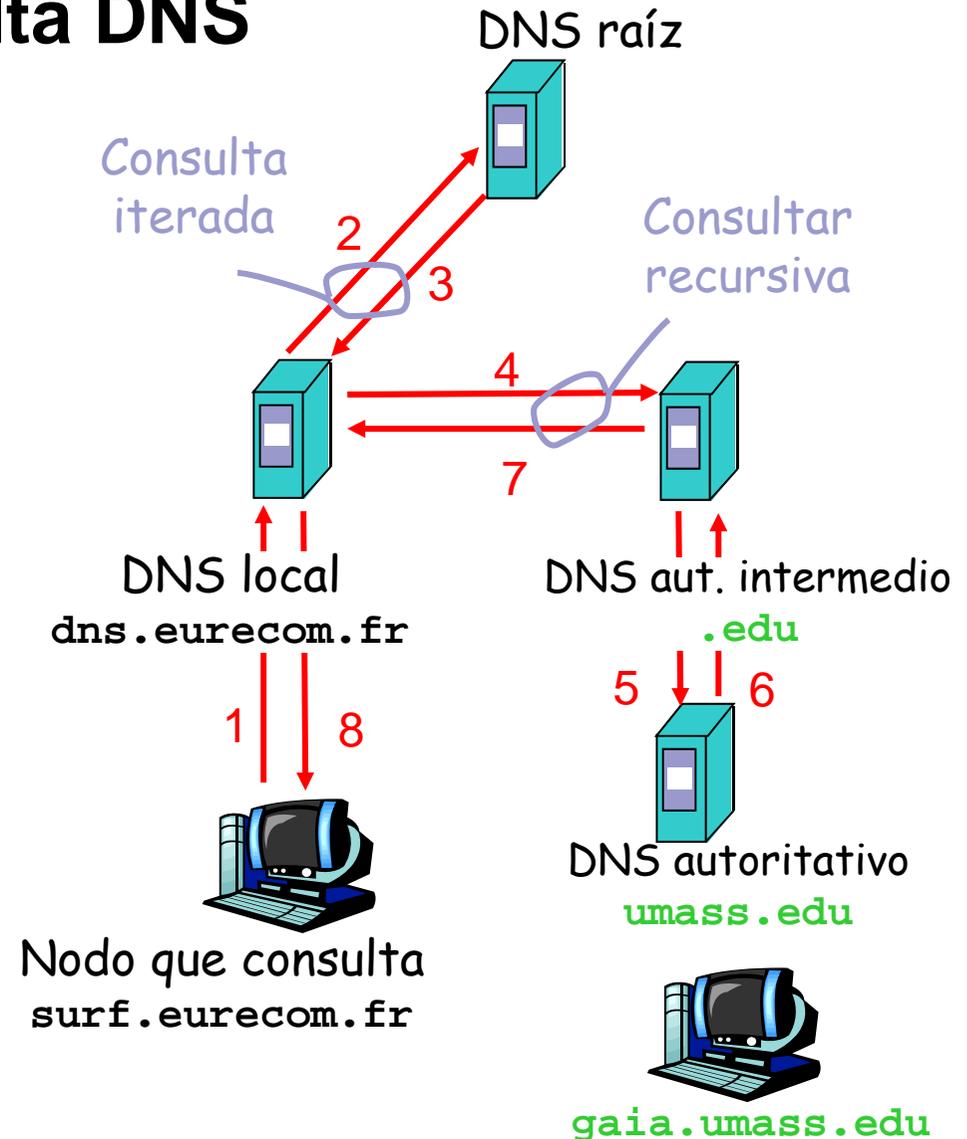
# Proceso de consulta DNS

- El servidor local pregunta a un Root Server...
  - Éste le devuelve la dirección de un servidor intermedio (**petición iterativa**)
  - El servidor local hace una petición recursiva a ese servidor intermedio
  - Ese servidor continuará haciendo la petición (**recursiva**) hasta que llegue un servidor autoritativo
  - Todas las peticiones son recursivas menos la petición al Root Server para reducir la carga sobre los Root



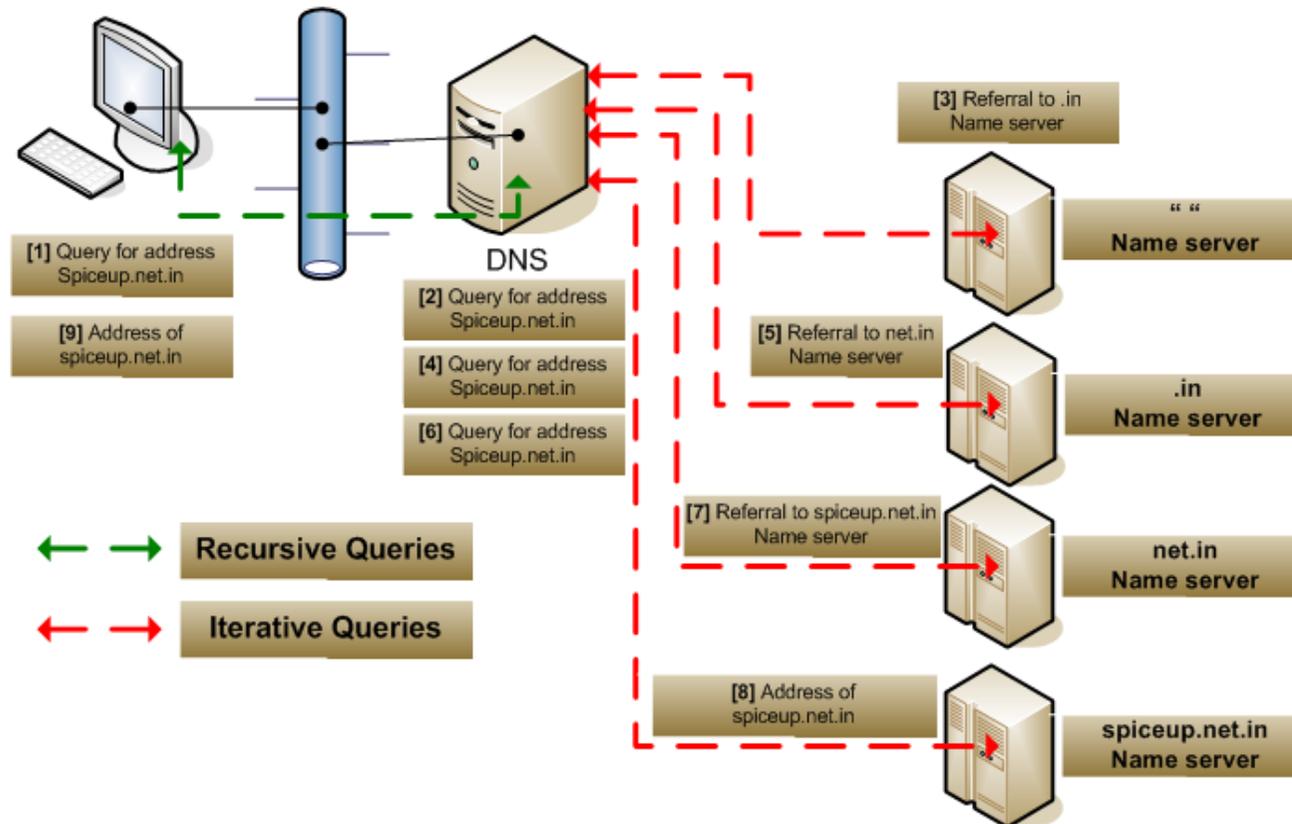
## Proceso de consulta DNS

- Consulta iterada:
  - El servidor contactado responde con el nombre del servidor autoritativo de siguiente nivel que se debe contactar
  - Ej: servidor raíz devuelve la IP del DNS autoritativo intermedio de .edu
- Consulta recursiva:
  - Coloca una consulta de resolución de nombres sobre el servidor de nombres contactado esperando la resolución final
  - Carga extra
  - Ej: servidor autoritativo intermedio dns.umass.edu se preocupa de realizar las consultas necesarias para resolver el nombre gaia.cs.umass.edu



# Proceso de consulta DNS

- Debido a la carga que supone la resolución recursiva para servidores DNS habitualmente está desactivada excepto para servidores DNS de la propia organización o de tu ISP



## Mapeo nombre-IP

- El mapeo de nombre a dirección IP puede ser múltiple (a múltiples direcciones IP)
- El mapeo de dirección IP a nombre es único (aparte alias)

```
#nslookup
> www.google.com
Servidor: resolv3.ono.com
Address: 62.81.29.254

Respuesta no autoritativa:
Nombre: www.l.google.com
Addresses: 74.125.132.104
          74.125.132.103
          74.125.132.106
          74.125.132.147
          74.125.132.105
          74.125.132.99
Alias: www.google.com
```

```
#nslookup
> 74.125.132.104
Servidor: resolv3.ono.com
Address: 62.81.29.254

Nombre: wb-in-f104.1e100.net
Address: 74.125.132.104
```

## 3.4 Registros de recursos DNS

- En un servidor DNS se almacenan Registros de Recursos (RR)
- Formato RR: (name, value, type, ttl)
- Type=A
  - name es un nombre de hosts
  - value es una dirección IP
- Type=NS
  - name es un dominio (por ejemplo, sitio.com)
  - value es una dirección IP de un DNS autoritativo para este dominio
- Type=CNAME
  - name es un alias para algún nombre “canónico” (el nombre real)
  - www.tlm.unavarra.es es realmente pluto.tlm.unavarra.es
  - value es el nombre canónico
- Type=MX
  - value es el nombre de un servidor de correo asociado con name

## 3.5 Cabecera DNS

- Protocolo DNS: mensajes de petición y respuesta, ambos tienen el mismo formato de mensaje
- Cabecera
  - identificación: 16 bits que identifica la consulta; la respuesta a la consulta utiliza el mismo identificador
  - flags:
    - Consulta o respuesta
    - Recursión deseada
    - Recursión disponible
    - La respuesta es autoritativa

# Cabecera DNS

Nombre, campos tipo  
 Para una consulta

RRs en respuesta  
 A una consulta (\*)

Registros para  
 servidores autoritativos (\*)

Información adicional  
 útil que puede usarse (\*)

identificación	Flags
número de consultas	número de RRs respondidos (*)
Número de RRs autoritativos (*)	Número de RRs adicionales (*)
Consultas (número variable de consultas)	
Respuestas (número variable de registros de recursos)	
Autoritativas (número variable de registros de recursos)	
Información adicional (Número variable de registros de recursos)	

(\*) a 0 o vacío para la petición

## 3.6 Cache DNS

- Una vez que un cliente de DNS aprende un mapeo lo cachea
  - Las entradas en la cache caducan tras un tiempo: TTL de validez del mapeo nombre DNS con IP que se devuelve con cada petición DNS
  - Normalmente los servidores de los TLD van a estar cacheados en los servidores locales, al tener tiempos de vida bastante largos (del orden de días)
  - Así que los servidores DNS Root no se suelen visitar

## 3.7 DDNS

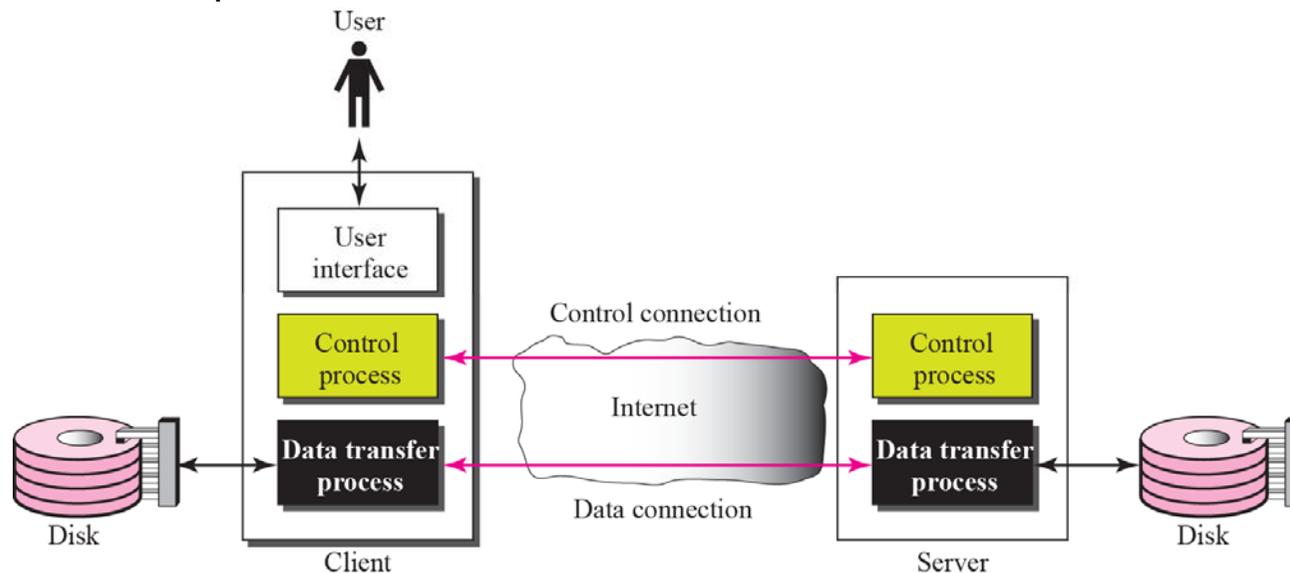
- En sus orígenes los mapeos IP-nombre de DNS eran casi estáticos, con escasos cambios a lo largo del tiempo
- En la actualidad, por ejemplo con accesos a Internet que asignan IP por DHCP, puede interesar asociar un nombre de dominio a una IP de un equipo que cambia de manera frecuente
- Dynamic DNS
  - Permite actualizar la información de los RR almacenadas por un servidor autoritativo con un proceso automatizado
  - Cada vez que un equipo cambia de dirección IP se actualiza el mapeo en el RR correspondiente
  - RFC 2136

## 3.8 DNSSEC

- El DNS es uno de los sistemas cruciales de Internet y por tanto objetivo de ataques para poder acceder a otros servicios
  - Ejemplo: Si se es capaz de interceptar el DNS se puede redirigir el tráfico de Internet a servidores señuelo
- DNS Security (DNSSEC)
  - Provee autenticación y control de integridad en los mensajes petición/respuesta
  - RFC4033

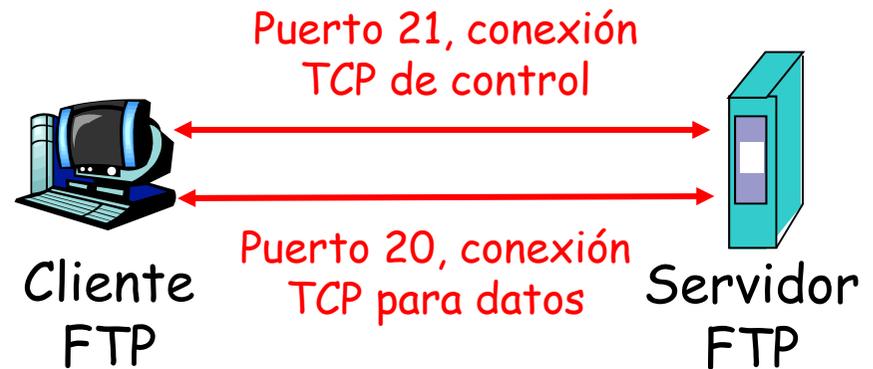
## 4 Transferencia de ficheros FTP

- FTP (File Transfer Protocol): protocolo de transferencia de ficheros
- RFC 959, RFC1123
- Encapsulado en TCP con puertos de servidor 20 y 21
  - Puerto 21: conexión de control
  - Puerto 20: conexión de datos
- Usa el modelo cliente/servidor
  - cliente: quien inicia la transferencia (para transferir hacia/desde la máquina remota)
  - servidor: máquina remota



## Transferencia de ficheros FTP

- El cliente FTP hace una conexión TCP con el servidor FTP en el puerto 21
- El cliente obtiene autorización sobre la conexión de control
- El cliente permite listar el directorio remoto al enviar comandos sobre la conexión de control
- Cuando el servidor recibe una comando para transferir un archivo, el servidor abre una conexión TCP para datos con el cliente
- Después de transferir el archivo, el servidor cierra la conexión.

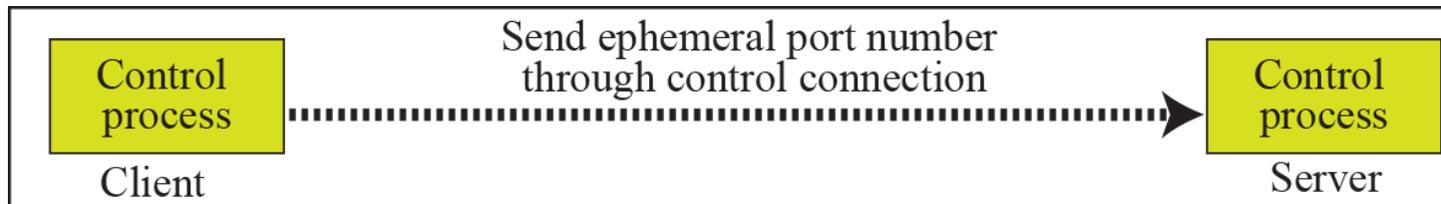


- El servidor abre una segunda conexión de datos para transferir otro archivo.
- Conexión de control: "out of band"
- El servidor FTP mantiene información "de estado": directorio actual, la autenticación inicial, etcétera

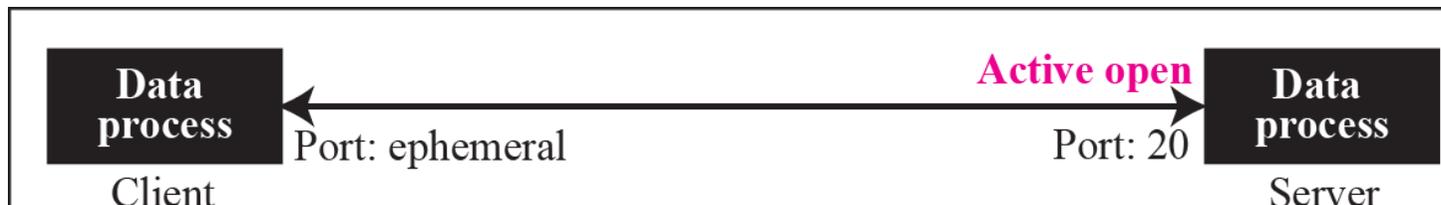
# Conexión de datos



a. First, passive open by client



b. Second, sending of ephemeral port

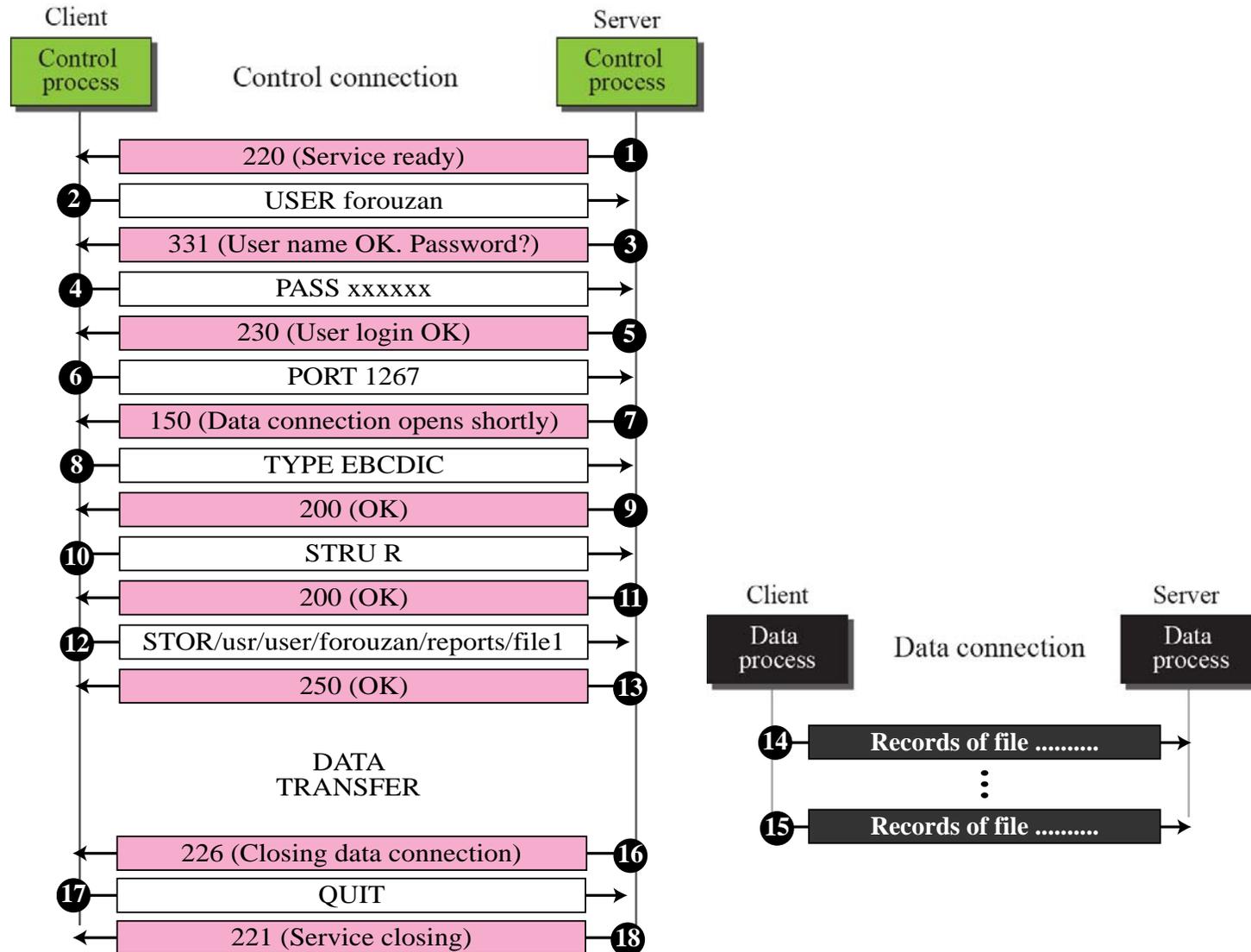


c. Third, active open by server

## 4.1 Comandos y códigos FTP

- Algunos comandos: enviados como texto ASCII sobre el canal de control
  - **USER username**
  - **PASS password**
  - **LIST** retorna una lista de los archivos en el directorio actual
  - **RETR filename** recupera (trae) el archivo
  - **STOR filename** almacena (coloca) el archivo en el host remoto
- Ejemplo de códigos de retorno: utiliza un código de estado y una descripción del código
  - 331 Username OK, password required
  - 125 data connection already open; transfer starting
  - 425 Can't open data connection
  - 452 Error writing file

# Ejemplo de transferencia FTP



## 4.2 TFTP

- Trivial FTP
- Protocolo FTP simplificado para:
  - Dispositivos con pocos recursos
  - Descarga de ficheros de configuración
  - Descarga del código de arranque de una máquina sin disco duro
- Incorpora un subset muy reducido de los comandos de FTP
  - No permite listar ficheros ni directorios
  - No permite autenticación del usuario
    - Normalmente se implementa la seguridad delimitando las direcciones IP desde la que se permite el acceso
- Sobre UDP puerto 69

## Resumen

- El servicio DNS es fundamental para el funcionamiento del resto de aplicaciones de Internet, facilitando el mapeo entre dirección IP y nombre-dominio de la máquina
- Los nombres de DNS deben ser únicos
  - Registro en ICANN
- Organización jerárquica de DNS permite su escalabilidad
- DNS encapsulado normalmente sobre UDP por su funcionamiento de petición/respuesta cortas, habitualmente en un solo paquete en cada sentido
- FTP permite la transferencia de ficheros mediante 2 conexiones: control y datos
  - El cliente debe permitir el establecimiento de la conexión de datos contra él

## Referencias

- [Forouzan]
  - Capítulo 19, “Domain Name System”
  - Capítulo 21, “File Transfer: FTP and TFTP”, sección 21.1
- [Stevens]
  - Capítulo 14, “DNS: The Domain Name System”
  - Capítulo 27, “FTP: File Transfer Protocol”