

TEMA 2

SERVICIOS Y PROTOCOLOS

DE APLICACIÓN EN INTERNET

Fundamentos de Redes

2018/2019



ugr
Universidad
de Granada

➤ Bibliografía Básica:



Capítulo 2 (2.1, 2.2, 2.4, 2.5), James F. Kurose y Keith W. Ross. **COMPUTER NETWORKING. A TOP-DOWN APPROACH**, 5^a Edición, Addison-Wesley, 2010, ISBN: 9780136079675.



Capítulo 11, Pedro García Teodoro, Jesús Díaz Verdejo y Juan Manuel López Soler.
TRANSMISIÓN DE DATOS Y REDES DE COMPUTADORES, Ed. Pearson, 2017, ISBN: 978-0-273-76896-8.

➤ Para saber más...



Capítulos 7 y 8, James F. Kurose y Keith W. Ross. **COMPUTER NETWORKING. A TOP-DOWN APPROACH**, 5^a Edición, Addison-Wesley, 2010, ISBN: 9780136079675.

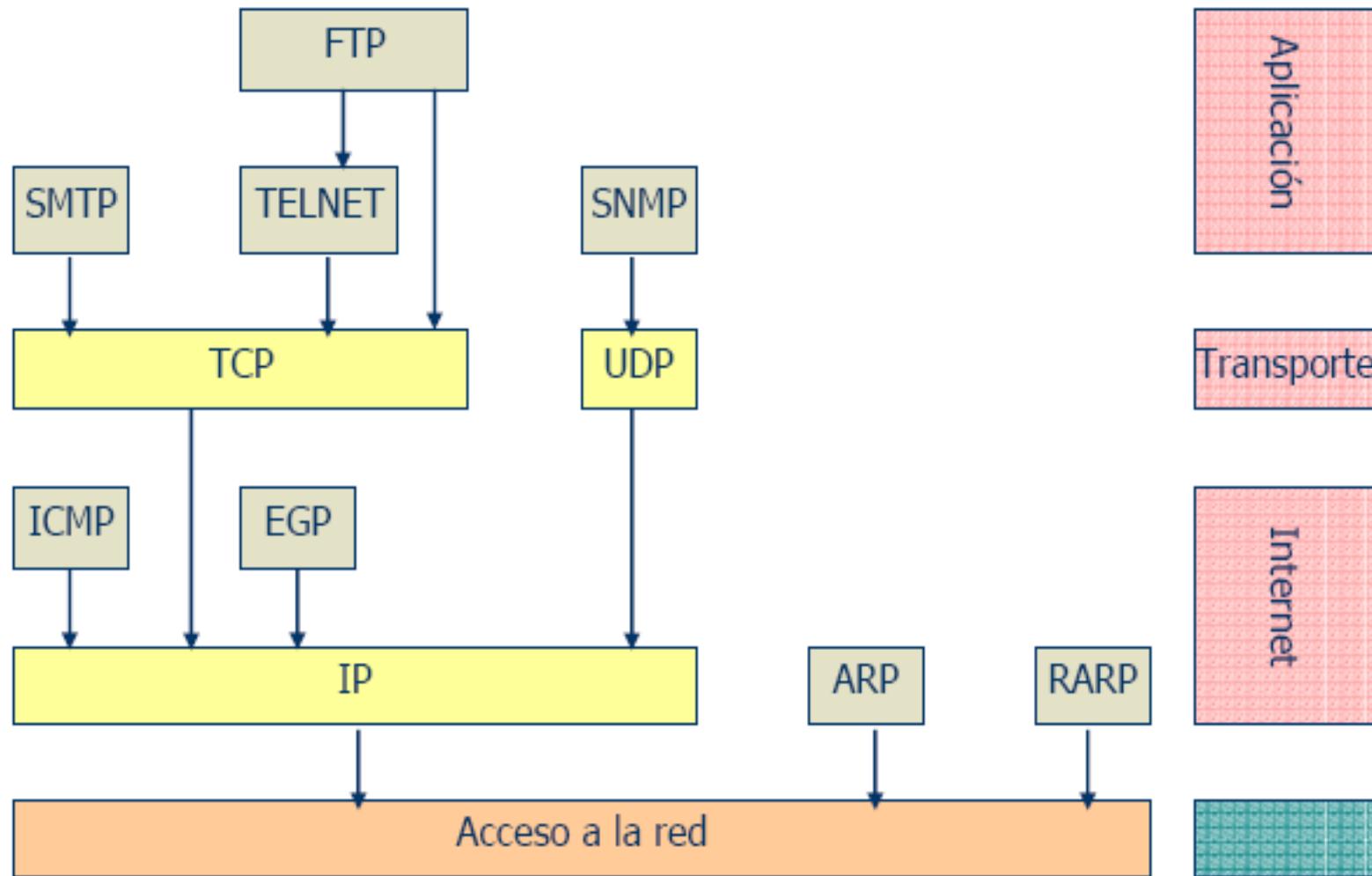
➤ Agradecimientos:

Estas transparencias están inspiradas en las transparencias utilizadas por Kurose y Ross en la Universidad de Massachusetts.

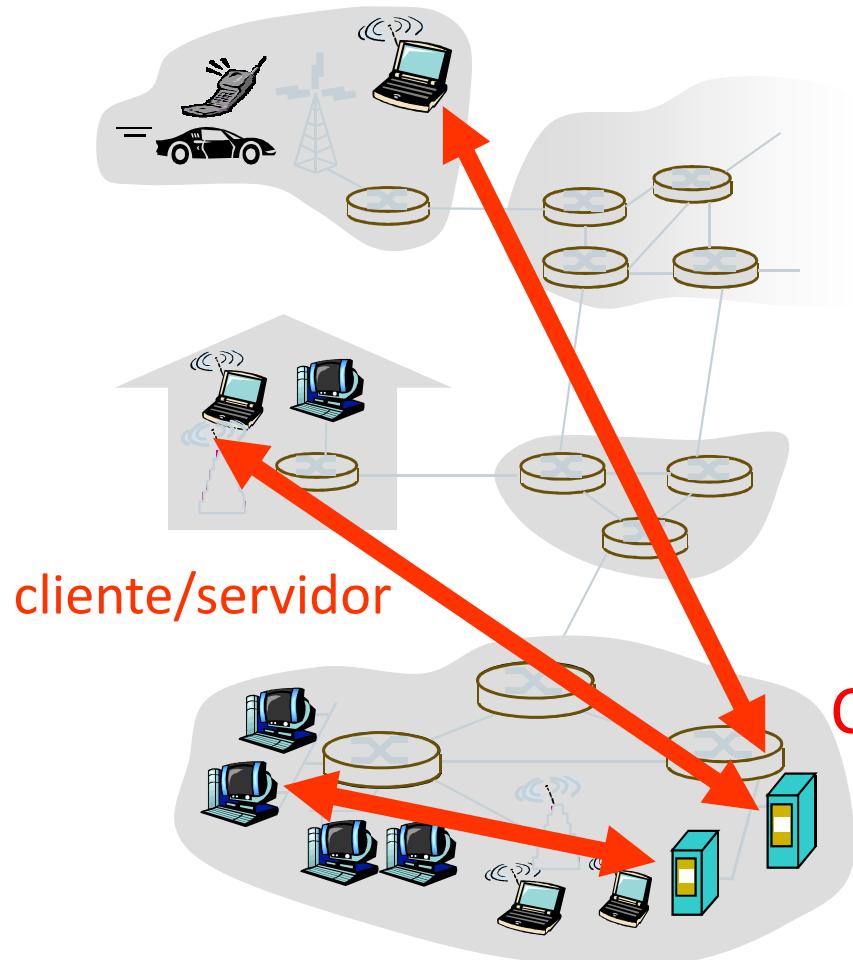
Tema 2. SERVICIOS Y PROTOCOLOS DE APLICACIÓN EN INTERNET

- 1. Introducción a las aplicaciones de red**
2. Servicio de Nombres de Dominio (DNS)
3. La navegación Web
4. El Correo electrónico
5. Protocolos seguros
6. Aplicaciones multimedia
7. Aplicaciones para interconectividad de redes locales
8. Cuestiones y ejercicios

■ Estructura de protocolos



INTRODUCCIÓN A LAS APLICACIONES DE RED: ARQUITECTURA CLIENTE/SERVIDOR

**Servidor:**

- Siempre en funcionamiento
- IP permanente & pública
- Agrupados en “granjas”
- <http://www.xatakandroid.com/mundo-android/la-imagen-de-la-semana-google-muestra-el-corazon-de-internet>
- <https://www.youtube.com/watch?v=zRwPSFpLX8I>

Clientes:

- Funcionando intermitentemente
- Pueden tener IP dinámica & privada
- Se comunican con el servidor
- No se comunican entre sí

INTRODUCCIÓN A LAS APLICACIONES DE RED: PROCESOS CLIENTE Y SERVIDOR

Proceso Cliente : proceso que inicia la comunicación

Proceso Servidor: proceso que espera a ser contactado

→ IP permanente & pública

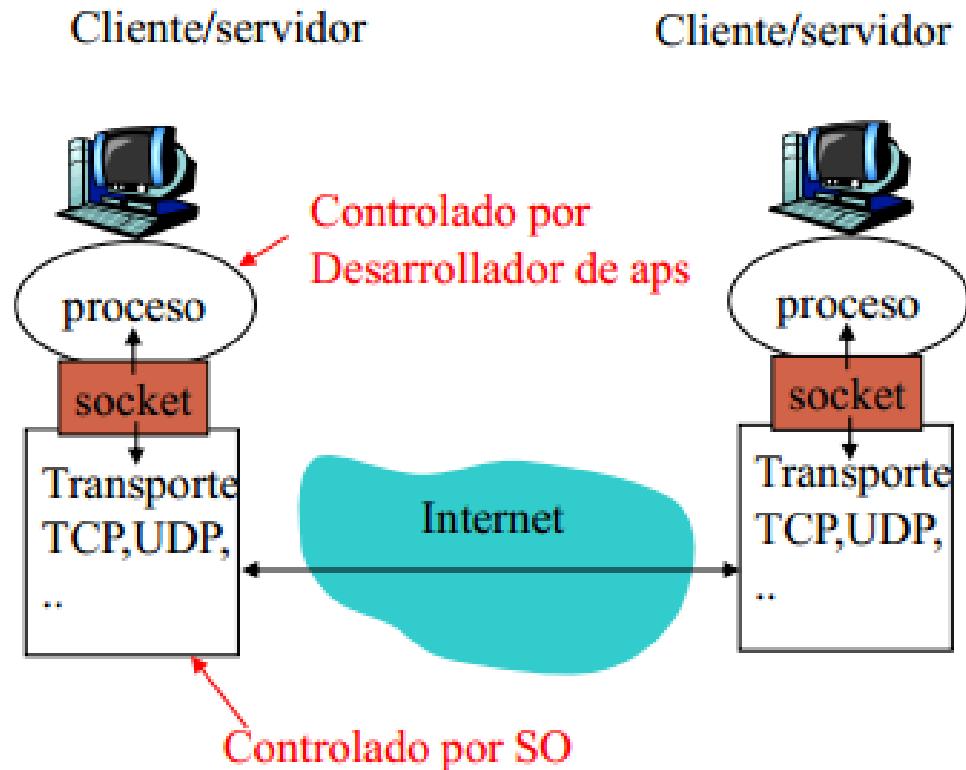
- Proceso envía/recibe mensajes a/desde su **socket**

- Para recibir mensajes un proceso debe tener un **identificador** (IP + puerto)

Ej: servidor web **gaia.cs.umass.edu**:

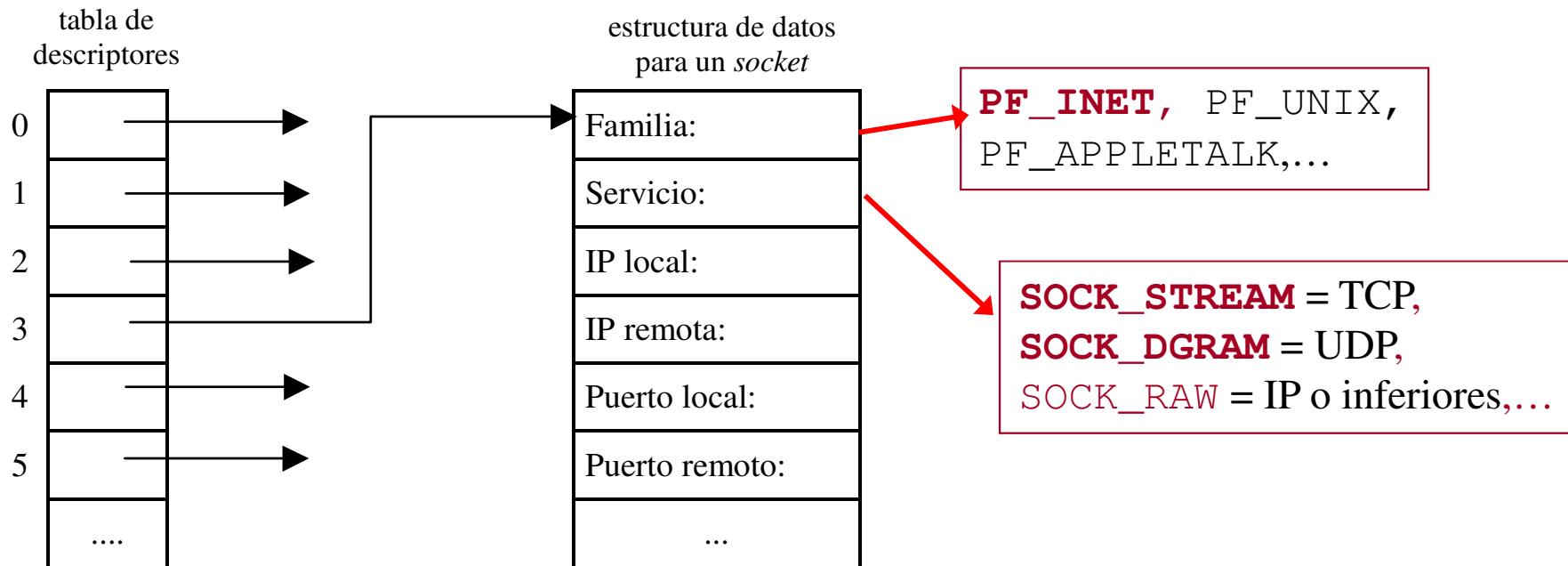
Dirección IP: **128.119.245.12**

Número de puerto: **80**



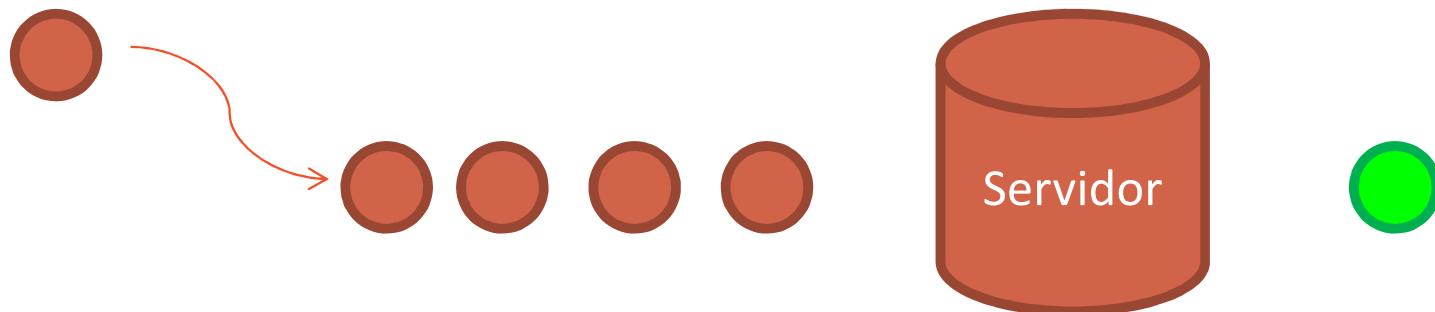
INTRODUCCIÓN A LAS APLICACIONES EN RED: LA INTERFAZ SOCKET

- Definimos **SOCKET** como un **descriptor** de una transmisión a través del cual la aplicación puede enviar y/o recibir información hacia y/o desde otro proceso de aplicación.
- Es una “**puerta**” de acceso entre la **aplicación** y los servicios de **transporte**.
- En la práctica un **socket** es un **puntero** a una estructura:



INTRODUCCIÓN A LAS APLICACIONES DE RED: RETARDO EN COLA

- Para estimar los retardos (tiempos) en cola se usa la teoría de colas:
- El uso de un servidor se modela con un sistema M/M/1 (ver *TRANSMISIÓN DE DATOS Y REDES DE COMPUTADORES*)



➤ El retardo en cola es:

$$R = \frac{\lambda \cdot (T_s)^2}{1 - \lambda \cdot T_s}$$

donde T_s (distribución exponencial) es el tiempo de servicio y λ (Poisson) la ratio de llegada de solicitudes.

- Esta misma expresión se puede utilizar para calcular el retardo en cola en un router.

INTRODUCCIÓN A LAS APLICACIONES DE RED: ¿QUÉ DEFINEN LOS PROTOCOLOS DE APLICACIÓN?

➤ ¿Qué es y qué define un protocolo?

➤ El tipo de servicio

- Orientado o no orientado a conexión
- Realimentado o no

➤ El tipo de mensaje

ej., request, response,

➤ La sintaxis:

Definición y estructura de “campos” en el mensaje

En aplicación generalmente son orientados a texto (HTTP)

Aunque hay excepciones (DNS)

Tendencia : usar formato Type-Length-Value

➤ La semántica:

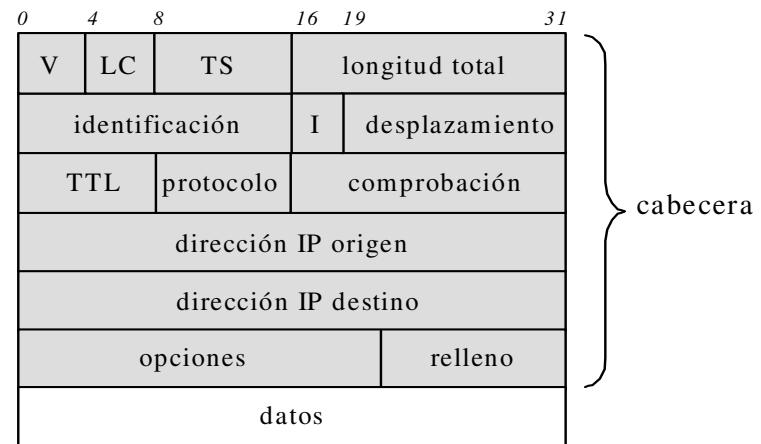
Significado de los “campos”

➤ Las reglas:

Cuándo los procesos envian mensajes/responden a mensajes

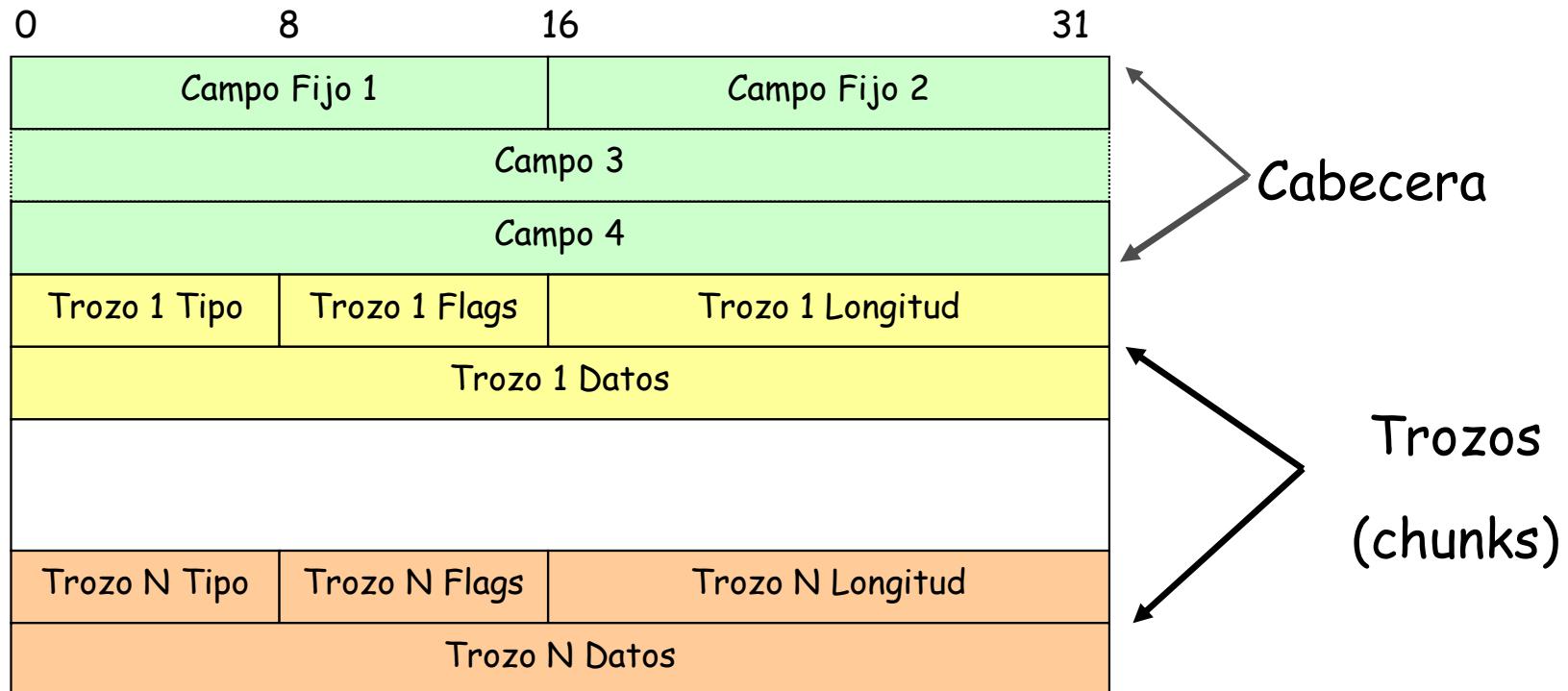
➤ Tipos de protocolos:

- Protocolos de dominio público (Definidos en RFCs (ej., HTTP, SMTP)) **versus** propietarios → (ej., Skype, IGRP)
- Protocolos in-band **versus** out-of-band
- Protocolos stateless **versus** state-full
- Protocolos persistentes **versus** no-persistentes (sobre servicios SOC)



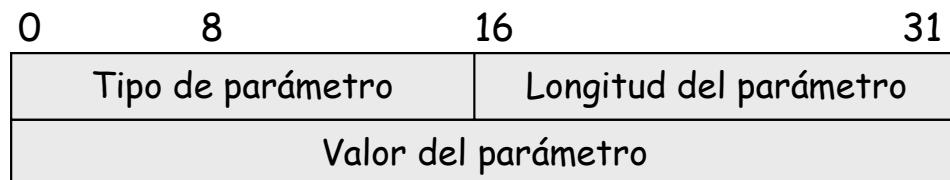
INTRODUCCIÓN A LAS APLICACIONES DE RED: ¿QUÉ DEFINEN LOS PROTOCOLOS DE APLICACIÓN?

- Tendencia: hacer los protocolos **flexibles** con
 - Una cabecera fija
 - Una serie de “trozos” (obligatorios y opcionales)



INTRODUCCIÓN A LAS APLICACIONES DE RED: ¿QUÉ DEFINEN LOS PROTOCOLOS DE APLICACIÓN?

- **Tendencia: hacer los protocolos flexibles con:**
 - **Una cabecera fija**
 - **Una serie de “trozos” (obligatorios y opcionales)**
 - Los trozos pueden incluir una cabecera específica más una serie de datos en forma de parámetros:
 - Parámetros fijos: en orden
 - Parámetros de longitud variable u opcionales.
 - Para los parámetros se usa Formato TLV (*Type-Length-Variable*)



INTRODUCCIÓN A LAS **APLICACIONES DE RED: CARACTERÍSTICAS****Características/requisitos de las aplicaciones:**

Pérdida de datos (errores): Algunas apps (ej., audio) pueden tolerar algunas pérdida de datos; otras (ej. FTP, telnet, HTTP) requieren transferencia 100% fiable

Requisitos temporales: Algunas apps denominadas *inelásticas* (ej., telefonía Internet, juegos interactivos) requieren retardo (*delay*) acotado para ser efectivas, otras aplicaciones no

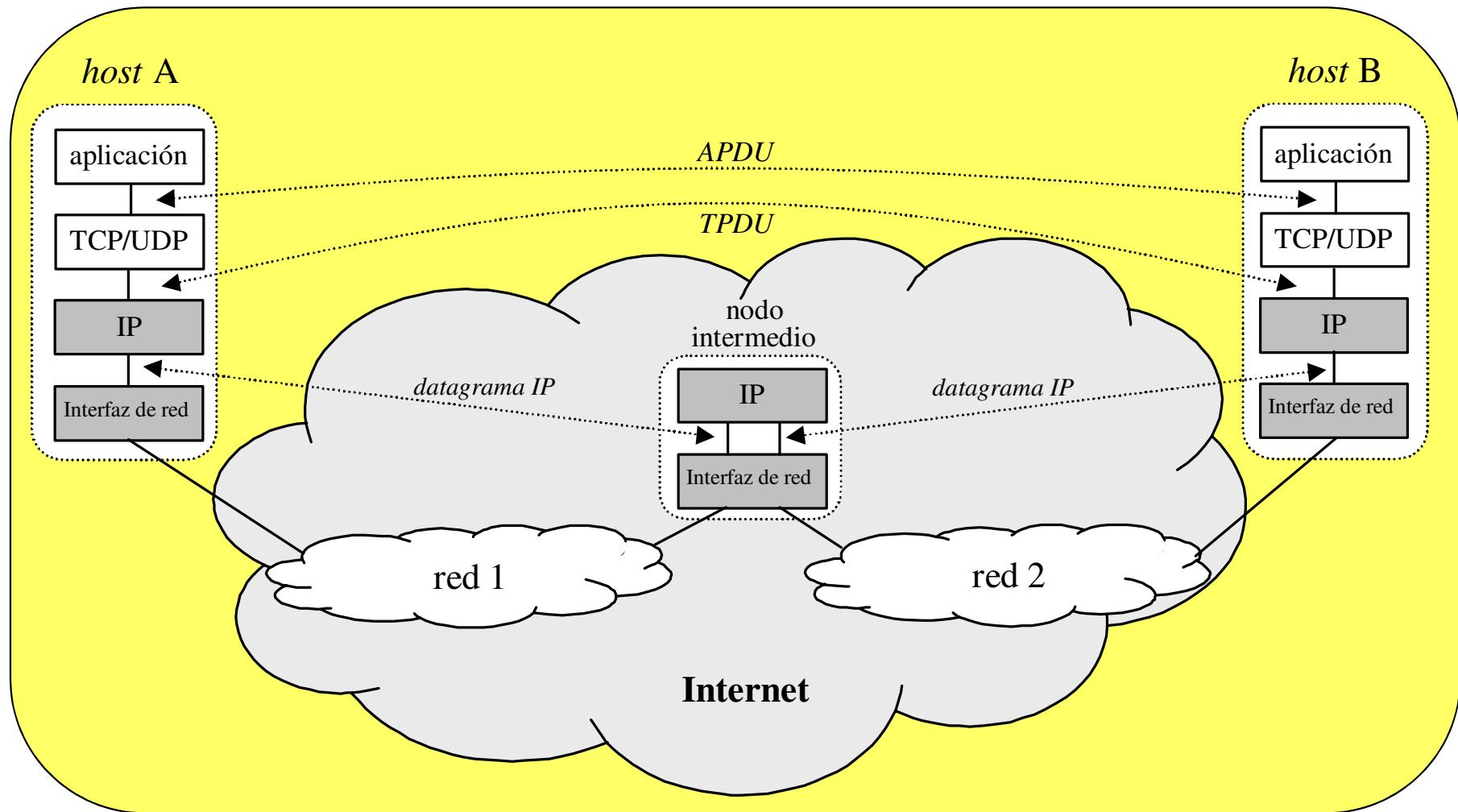
Ancho de banda (tasa de transmisión o *throughput*) Algunas apps requieren envío de datos a una tasa determinada (p. ejemplo un codec de vídeo), otras no

Seguridad: Los requisitos de seguridad son muy variables (Encriptación, autenticación, no repudio, integridad...)

INTRODUCCIÓN A LAS APLICACIONES DE RED: REQUERIMIENTOS DE ALGUNAS APLICACIONES..

Application	Data loss	Throughput	Time Sensitive
file transfer	no loss	elastic	no
e-mail	no loss	elastic	no
Web documents	no loss	elastic	no
real-time audio/video	loss-tolerant	audio: 5kbps-1Mbps video:10kbps-5Mbps	yes, 100's ms
stored audio/video	loss-tolerant	same as above	yes, few s
interactive games	loss-tolerant	few kbps up	yes, 100's ms
instant messaging	no loss	elastic	yes and no

INTRODUCCIÓN A LAS APLICACIONES DE RED: PROTOCOLOS DE TRANSPORTE



Servicio TCP:

Orientado a conexión
Transporte fiable
Control de flujo
Control de congestión

Servicio UDP:

No orientado a conexión
Transporte no fiable
Sin control de flujo
Sin control de congestión,
¿Para qué existe UDP?

- TCP y UDP (capa de transporte) al ser usuarios del protocolo IP (capa de red) **no garantizan Calidad de Servicio (QoS)**, es decir:
 - El **retardo** NO está acotado acotado
 - Las **fluctuaciones en el retardo** NO están acotadas
 - No hay una **velocidad de transmission** mínima garantizada
 - No hay una **probabilidad de pérdidas** acotada
- Tampoco hay garantías de seguridad.

INTRODUCCIÓN A LAS APLICACIONES DE RED

Application	Application layer protocol	Underlying transport protocol
e-mail	SMTP [RFC 2821]	TCP
remote terminal access	Telnet [RFC 854]	TCP
Web	HTTP [RFC 2616]	TCP
file transfer	FTP [RFC 959]	TCP
streaming multimedia	HTTP (eg Youtube), RTP [RFC 1889]	TCP or UDP
Internet telephony	SIP, RTP, proprietary (e.g., Skype)	typically UDP

Tema 2. SERVICIOS Y PROTOCOLOS DE APLICACIÓN EN INTERNET

1. Introducción a las aplicaciones de red
2. **Servicio de Nombres de Dominio (DNS)**
3. La navegación Web
4. El Correo electrónico
5. Protocolos seguros
6. Aplicaciones multimedia
7. Aplicaciones para interconectividad de redes locales
8. Cuestiones y ejercicios

SERVICIO DE NOMBRES DE DOMINIO (DNS)

- La comunicación en Internet precisa de direcciones IP
- Los usuarios prefieren usar “nombres de dominio” (más de 300×10^6)
- DNS: traducción de nombres a direcciones IP (resolución de nombres)

goliat.ugr.es <-----> **150.214.20.3**

- Estructura jerárquica en dominios:
Parte_local.dominio_niveln.dominio_nivel2.dominio_nivel1.
- Al dominio de nivel1 se le denomina **dominio genérico** (.com .es .edu etc).
- El dominio raíz o “.” está gestionado por el **ICANN** (Internet Corporation for Assigned Names and Numbers; <http://www.icann.org>), que suele delegar en centros regionales.

SERVICIO DE NOMBRES DE DOMINIO (DNS)

Lectura recomendadas

<https://www.icann.org/en/system/files/files/domain-names-beginners-guide-06dec10-es.pdf>

<http://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/sobre-registros-de-dominios>

<https://www.tldp.org/HOWTO/DNS-HOWTO.html>

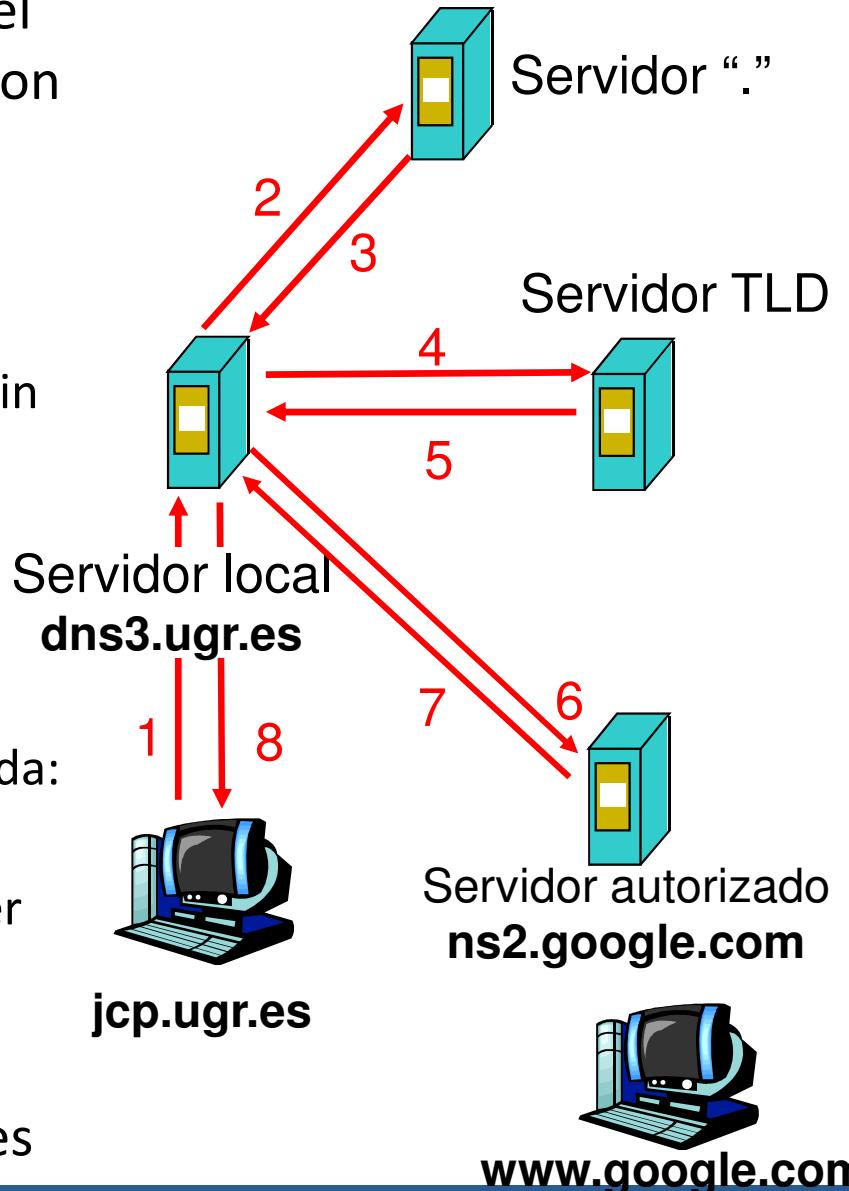
SERVICIO DE NOMBRES DE DOMINIO (DNS)

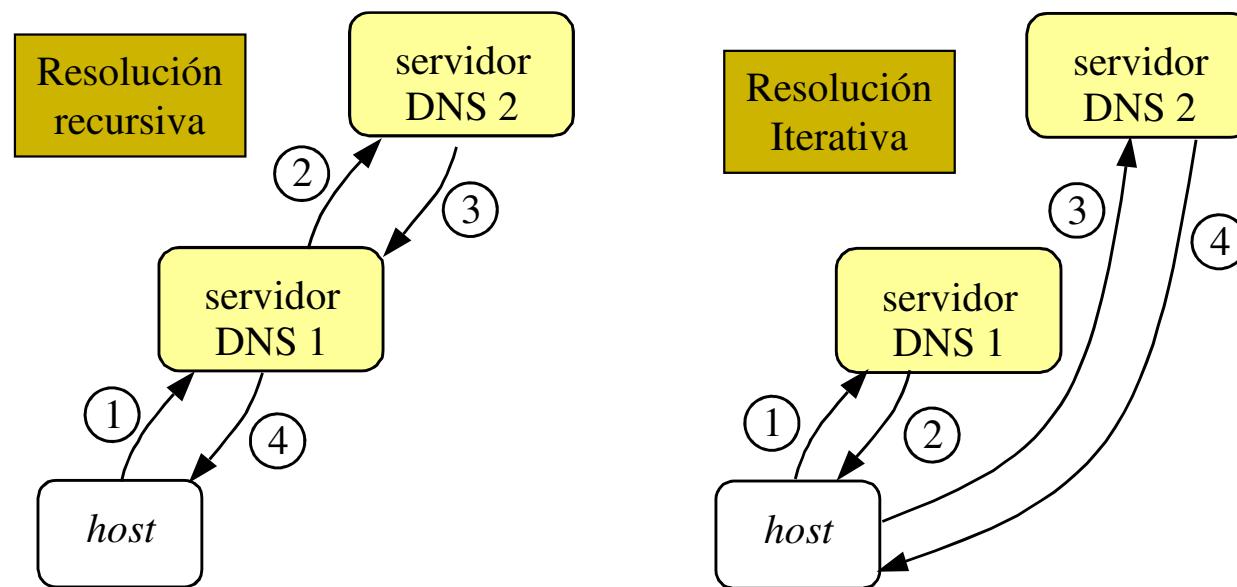
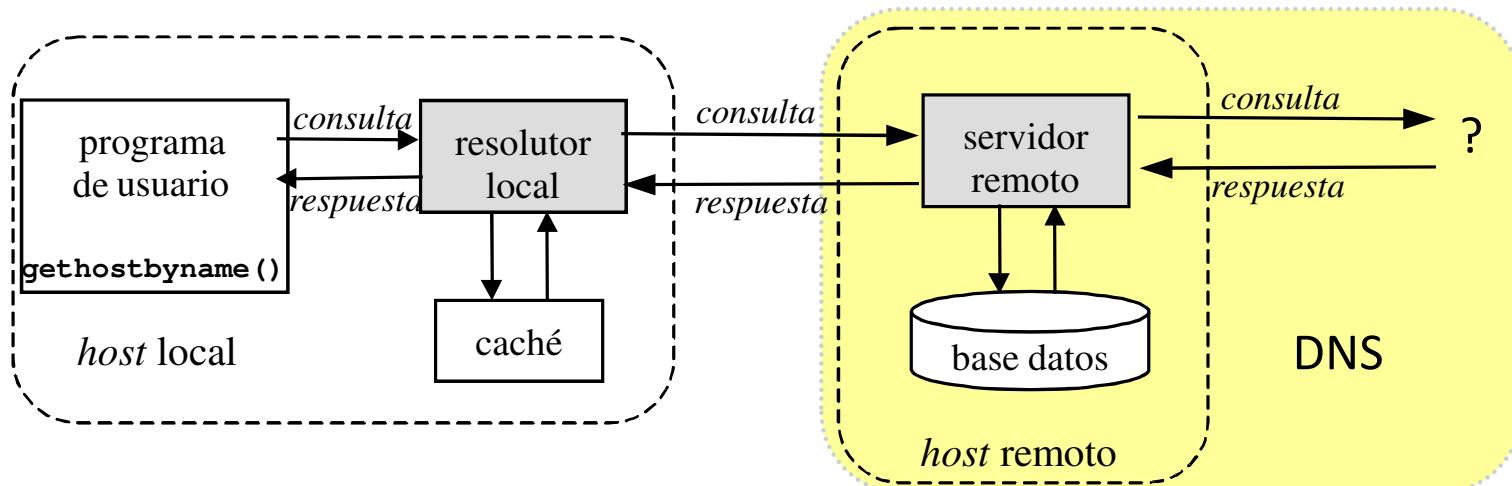
Inicialmente fueron definidos los siguientes 9 dominios genéricos (RFC 1591):

- .com** -> organizaciones comerciales
- .edu** -> instituciones educativas, como universidades, de EEUU.
- .gov** -> instituciones gubernamentales estadounidenses
- .mil** -> grupos militares de estados unidos
- .net** -> proveedores de Internet
- .org** -> organizaciones diversas diferentes de las anteriores
- .arpa**-> propósitos exclusivos de infraestructura de Internet
- .int** -> organizaciones establecidas por tratados internacionales entre gobiernos
- .xy** -> indicativos de la zona geográfica (ej. es (España); pt (portugal); jp (Japón)...

SERVICIO DE NOMBRES DE DOMINIO (DNS)

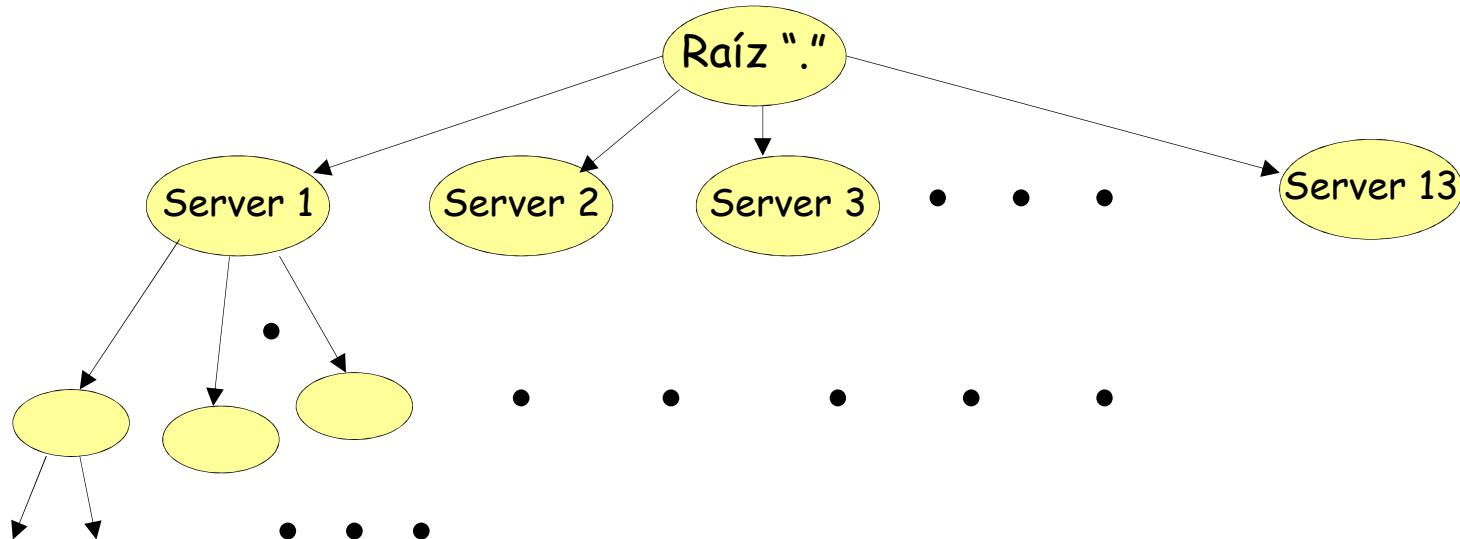
- DNS es un **protocolo** de aplicación para el acceso a una base de datos distribuida con una gestión distribuida.
- 3 niveles de servidores:
 - Servidores raíz “.”
 - Servidores de dominio (Top-Level domain o TLD)
 - Servidores Locales
- **jcp.ugr.es → www.google.com**
 - Consulta al “resolver” local
 - Conexión con DNS local con IP conocida:
¿cómo se conoce?
 - El DNS local realiza la “resolución” (ver página siguiente)
- Resolución iterativa o recursiva
- Para mejorar prestaciones se usan caches





Gestión de la base de datos distribuida y jerárquica:

- Está formada por un conjunto de servidores cooperativos que almacenan parcialmente la base de datos que se denomina (**Berkeley Internet Name Domain**).
- Cada servidor es responsable de lo que se denomina **ZONA**.
- Una *zona* es un conjunto de nombres de dominio contiguos (por debajo de uno dado en el árbol) de los que un servidor tiene toda la información y es su **autoridad**.
- Los *servidores autoridad (Start of Authority Servers)* deben contener **toda** (no “cacheada”) la información de su zona.
- La autoridad puede **delegarse** jerárquicamente a otros servidores



Gestión de la base de datos DNS:

- Cada zona debe tener **al menos** un servidor de autoridad.
- En cada zona hay servidores **primarios** (copia master de la db) y **secundarios** (obtienen la db por transferencia)
- Además, existe un servicio de **cache** para mejorar prestaciones.
- La **topología real** de servidores es complicada: existe **13 servidores** raíz (A-M) (ver <http://www.root-servers.org>)
- El root-server F (y otros) tiene un servidor en Madrid (**Espanix: punto neutro**)
- Cuando un cliente (a través de un *resolver local*) solicita una resolución de nombres a su servidor, puede ocurrir:
 - **Respuesta CON autoridad**: el servidor tiene autoridad sobre la zona en la que se encuentra el nombre solicitado y devuelve la dirección IP.
 - **Respuesta SIN autoridad**: el servidor no tiene autoridad sobre la zona en la que se encuentra el nombre solicitado, pero lo tiene en la cache.
 - **No conoce la respuesta**: el servidor preguntará a otros servidores de forma recursiva o iterativa. Normalmente se “eleva” la petición a uno de los servidores raíz.

Root-servers <http://www.root-servers.org/>

Servidor A: Network Solutions, Herndon, Virginia, USA.

Servidor B: Instituto de Ciencias de la Información de la Universidad del Sur de California, USA.

Servidor C: PSINet, Virginia, USA.

Servidor D: Universidad de Maryland, USA.

Servidor E: NASA, en Mountain View, California, USA.

Servidor F: Internet Software Consortium, Palo Alto, California, USA.

Servidor G: Agencia de Sistemas de Información de Defensa, California, USA.

Servidor H: Laboratorio de Investigación del Ejercito, Maryland, USA.

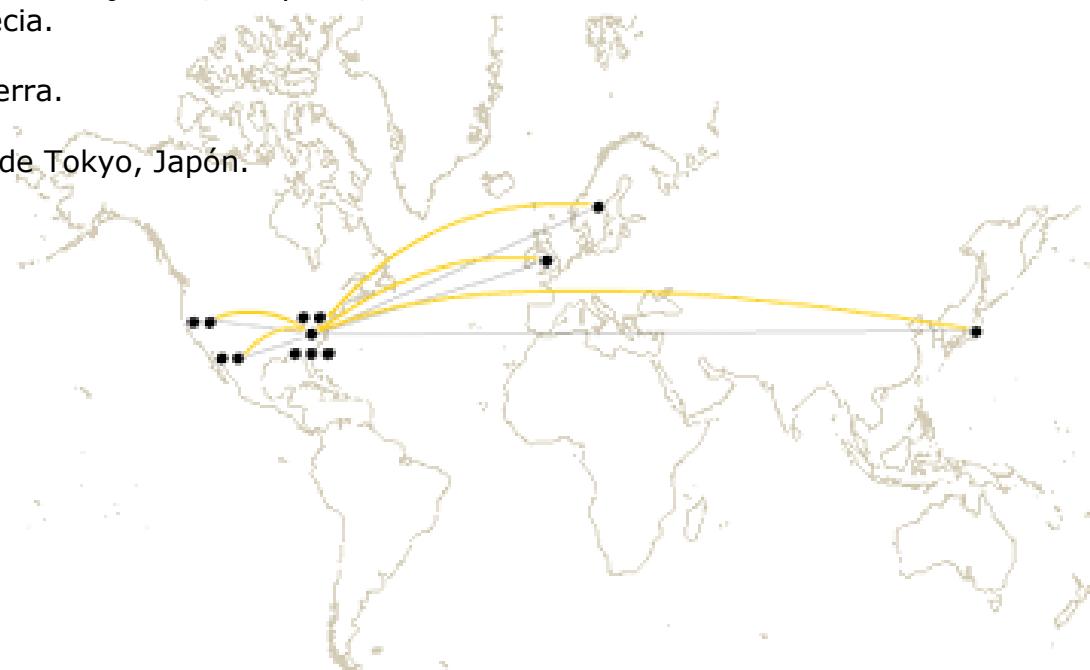
Servidor I: NORDUnet, Estocolmo, Suecia.

Servidor J: (TBD), Virginia, USA.

Servidor K: RIPE-NCC, Londres, Inglaterra.

Servidor L: (TBD), California, USA.

Servidor M: Wide Project, Universidad de Tokyo, Japón.



¿Cómo es la base de datos DNS?

- Todo dominio está asociado al menos a un registro **Resource Record**.
- Cada **RR** es una tupla con 5 campos:

Nombre del dominio: nombre del dominio al que se refiere el RR.

Tiempo de vida: tiempo de validez de un registro (para la cache).

Clase: en Internet siempre IN.

Tipo: Tipo de registro.

SOA	Registro (S tart O f A uthority) con la autoridad de la zona.
NS	Registro que contiene un servidor de nombres.
A	Registro que define una dirección IPv4.
MX	Registro que define un servidor de correo electrónico.
CNAME	Registro que define el nombre canónico de un nombre de dominio.
HINFO	Información del tipo de máquina y sistema operativo.
TXT	Información del dominio.

Valor: Contenido que depende del campo tipo

- Existe una base de datos asociada de **resolución inversa** para traducir direcciones IP en nombres de dominio. (in-addr.arpa)

Formato mensajes DNS:

0	16	31
identificación	parámetro	
nsolicitudes	nrespuestas	
nautoridades	na adicionales	
solicitud		
srespuesta		
autoridad		
adicional		

- Consulta/respuesta.
- Repuesta con/sin autoridad.
- Consulta con/sin recursión deseada.
- Disponible/no disponible respuestas con recursión.
- Consulta directa/inversa.

0	16	31
solicitud		
tipo		clase
recurso		
tipo		clase
tiempo		longitud
datos		

DNS se ofrece en el puerto 53 mediante UDP normalmente o TCP

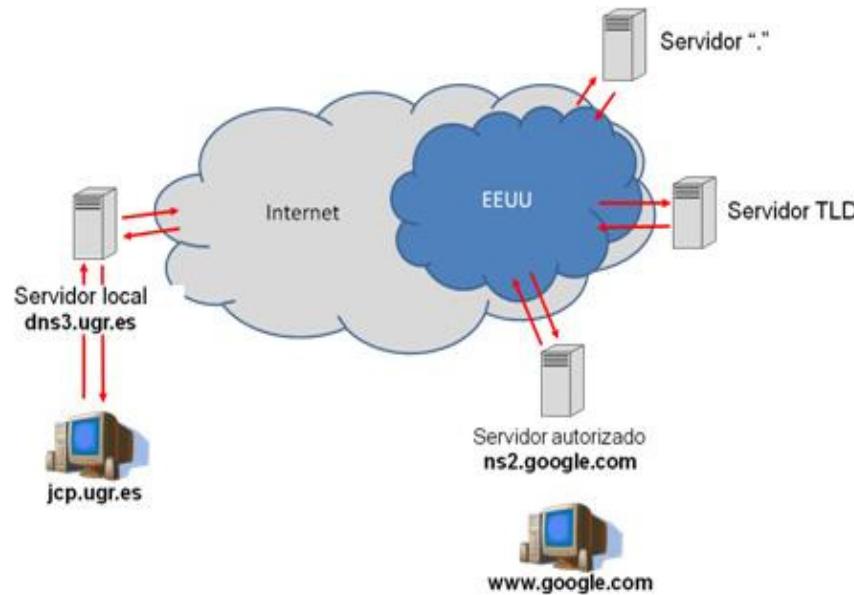
(para respuestas grandes > 512 bytes).

Más información:

- RFC 1034 y RFC 1035 (actualizados 3597 y 3658)
- /usr/doc/HOWTO/trans/es/DNS-COMO
- man named, nslookup, resolver, host.conf, dig
- DNSSEC http://www.dominios.es/dominios/sites/dominios/files/1318333648229_0.pdf

SERVICIO DE NOMBRES DE DOMINIO (DNS)

6. En la siguiente figura se ilustra un ejemplo de acceso DNS por parte de una máquina (jcp.ugr.es) que quiere acceder a los servicios de www.google.com. Para obtener la dirección IP del servidor, es necesario que la consulta pase por todos los servidores del gráfico. Considerando unos retardos promedio de 8 μ s dentro de una red LAN, de 12 ms en cada acceso a través de Internet (4 ms si la conexión se restringe a EEUU) y de 1 ms de procesamiento en cada servidor:



Calcule el tiempo que se tardaría si la solicitud al servidor local es recursiva, pero el propio servidor local realiza solicitudes iterativas.

Especifique una política (recursiva-iterativa) más rápida de solicitudes y el tiempo que tardaría la solicitud en ser respondida. ¿Qué desventaja tiene sobre la solución anterior?

Tema 2. SERVICIOS Y PROTOCOLOS DE APLICACIÓN EN INTERNET

1. Introducción a las aplicaciones de red
2. Servicio de Nombres de Dominio (DNS)
- 3. La navegación Web**
4. El Correo electrónico
5. Protocolos seguros
6. Aplicaciones multimedia
7. Aplicaciones para interconectividad de redes locales
8. Cuestiones y ejercicios

LA NAVEGACIÓN WEB

- Una página Web es un fichero (HTML) formado por objetos:
ficheros HTML, imágenes JPEG, Java applets, ficheros de audio, vídeo, etc
- Cada objeto se direcciona por una URL (o URI):
esquema://[:user[:password]@]dominio[:puerto][/path][/recu
rso][?solicitud][#fragment]
- Protocolo HTTP
 - Modelo cliente-servidor
 - cliente:* browser que solicita, recibe y muestra objetos web
 - servidor:* envía objetos web en respuesta a peticiones

➤ Características HTTP:

- **Usa los servicios de TCP (S.O.C.) en el puerto 80**

Inicio de conexión TCP, envío HTTP, cierre de conexión TCP

- **HTTP es “stateless” ➔ Cookies**

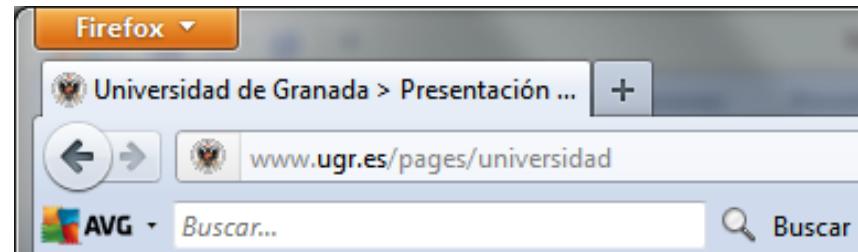
El servidor no mantiene información sobre las peticiones de los clientes

- **Existen dos tipos**

No persistente ➔ Se envía únicamente un objeto en cada conexión TCP.

Persistente ➔ Pueden enviarse multiples objetos sobre una única conexión TCP entre cliente y servidor

LA NAVEGACIÓN WEB: MENSAJES HTTP



- 1a. El Cliente HTTP inicia conexión TCP al servidor HTTP (proceso) en www.ugr.es en el puerto 80 (segmento SYNC de TCP)
2. El Cliente HTTP envía *request message* para el objeto
3. El servidor HTTP devuelve la respuesta
4. Si es persistente → Envío de más objetos
5. Cierre de conexión TCP (liberación de recursos)
6. Nuevas conexiones TCP
- tiempo
- ```
graph LR; 1a[1a.] --> 1b[1b.]; 1a --> 2[2.]; 1b --> 1c[1c.]; 1b --> 3[3.]; 2 --> 4[4.]; 2 --> 5[5.]; 2 --> 6[6.]
```

HTTP define dos tipos de mensajes (*request, response*):

1. *HTTP request message* (solicitudes del cliente al servidor):

Línea de petición

(GET, POST,  
HEAD)

**GET /somedir/page.html HTTP/1.1**

**Host: www.someschool.edu**

**User-agent: Mozilla/4.0**

**Connection: close**

**Accept-language: fr**

Líneas de cabecera

Carriage return +  
line feed

(extra carriage return, line feed)

Indican fin del mensaje

HTTP define dos tipos de mensajes (*request, response*):

## 2. HTTP *response message*: (respuestas del servidor al cliente):

Línea de estado

HTTP/1.1 200 OK

200 OK  
301 Moved Permanently  
400 Bad Request  
404 Not Found  
505 HTTP Version Not Supported

Líneas de cabecera

Connection: close

Date: Thu, 06 Aug 1998 12:00:15 GMT

Server: Apache/1.3.0 (Unix)

Last-Modified: Mon, 22 Jun 1998 .....

Content-Length: 6821

Content-Type: text/html

Datos,  
ej. fichero html

data data data data data ...

## 8. Compare el rendimiento en términos temporales de HTTP persistente y no persistente considerando los siguientes parámetros:

**Descarga de una página web con 10 objetos incrustados**

**Tiempo de Establecimiento de conexión TCP → 5 ms**

**Tiempo de Cierre de conexión TCP → 5 ms**

**Tiempo de solicitud HTTP → 2 ms**

**Tiempo de respuesta HTTP (página web u objeto) → 10 ms**

## LA NAVEGACIÓN WEB: Protocolo HTTP 1.1 (RFC 2616)

- **MÉTODOS (acciones solicitadas en los *request messages*):**
  - **OPTIONS**: solicitud de información sobre las opciones disponibles
  - **GET**: solicitud de un recurso (puede ser condicional)
  - **HEAD**: igual que GET pero el servidor no devuelve el “cuerpo” sólo cabeceras
  - **POST**: solicitud al servidor para que acepte y subordine a la URI especificada, los datos incluidos en la solicitud,
  - **PUT**: solicitud de sustituir la URI especificada con los datos incluidos en la solicitud.
  - **DELETE**: solicitud de borrar la URI especificada.
- **CÓDIGOS DE RESPUESTA (para los *response messages*):**
  - **1xx** indican mensajes exclusivamente informativos
  - **2xx** indican algún tipo de éxito
  - **3xx** redireccion al cliente a otra URL
  - **4xx** indican un error
  - **5xx** indican un error
- **CABECERAS (47 *request headers* y 49 *response headers*)**

From: , User-Agent: , Content-Type: , Content-Length: , .....

[http://en.wikipedia.org/wiki/List\\_of\\_HTTP\\_header\\_fields](http://en.wikipedia.org/wiki/List_of_HTTP_header_fields)

✓ **Cabeceras comunes para peticiones y respuestas**

- **Content-Type:** descripción MIME de la información contenida en este mensaje.
- **Content-Length:** longitud en bytes de los datos enviados, expresado en base decimal.
- **Content-Encoding:** formato de codificación de los datos enviados en este mensaje. Sirve, por ejemplo, para enviar datos comprimidos o encriptados.
- **Date:** fecha local de la operación. Las fechas deben incluir la zona horaria en que reside el sistema que genera la operación. Por ejemplo: Sunday, 12-Dec-96 12:21:22 GMT+01. No existe un formato único en las fechas.

✓ **Cabeceras sólo para peticiones del cliente**

- **Accept**: campo opcional que contiene una lista de tipos MIME aceptados por el cliente.
- **Authorization**: clave de acceso que envía un cliente para acceder a un recurso de uso protegido o limitado. La información incluye el formato de autorización empleado, seguido de la clave de acceso propiamente dicha. La explicación se incluye más adelante.
- **From**: campo opcional que contiene la dirección de correo electrónico del usuario del cliente Web que realiza el acceso.

- **If-Modified-Since**: permite realizar operaciones GET condicionales, en función de si la fecha de modificación del objeto requerido es anterior o posterior a la fecha proporcionada. Puede ser utilizada por los sistemas de almacenamiento temporal de páginas. Es equivalente a realizar un HEAD seguido de un GET normal.
- **Referer**: contiene la URL del documento desde donde se ha activado este enlace. De esta forma, un servidor puede informar al creador de ese documento de cambios o actualizaciones en los enlaces que contiene. No todos los clientes lo envían.
- **User-agent**: cadena que identifica el tipo y versión del cliente que realiza la petición. Por ejemplo, los *browsers* de Netscape envían cadenas del tipo User-Agent: Mozilla/3.0 (WinNT; I)

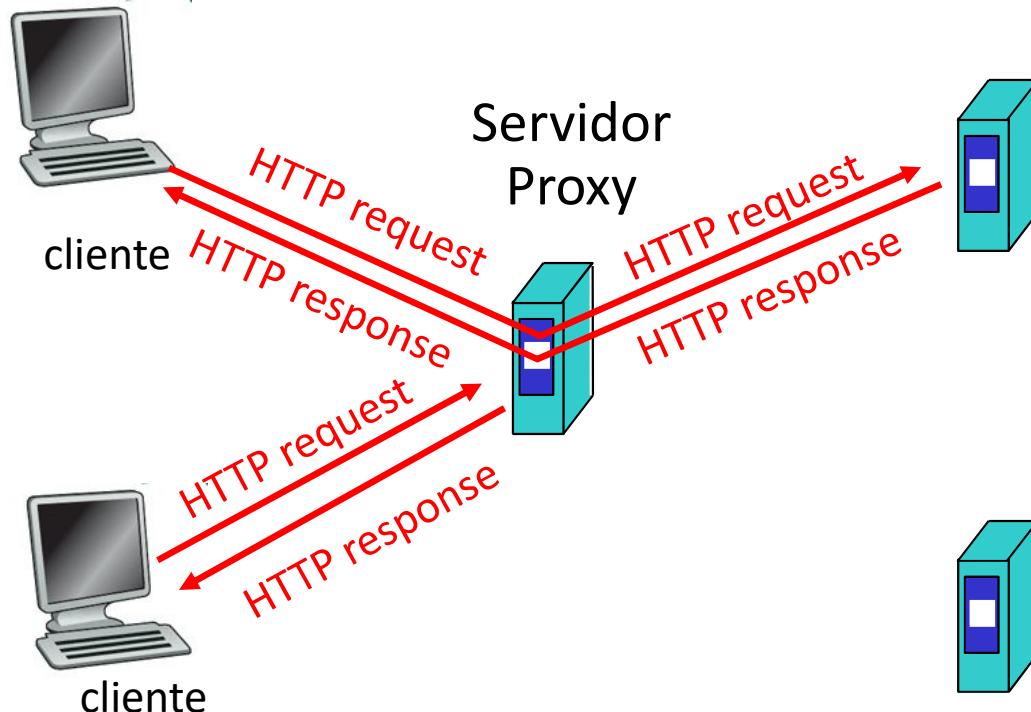
✓ **Cabeceras sólo para respuestas del servidor HTTP**

- **Allow:** informa de los comandos HTTP opcionales que se pueden aplicar sobre el objeto al que se refiere esta respuesta. Por ejemplo, Allow: GET, POST.
- **Expires:** fecha de expiración del objeto enviado. Los sistemas de cache deben descartar las posibles copias del objeto pasada esta fecha. Por ejemplo, Expires: Thu, 12 Jan 97 00:00:00 GMT+1. No todos los sistemas lo envían.
- **Last-modified:** fecha local de modificación del objeto devuelto. Se puede corresponder con la fecha de modificación de un fichero en disco, o, para información generada dinámicamente desde una base de datos, con la fecha de modificación del registro de datos correspondiente.

## LA NAVEGACIÓN WEB: Web cache

**Objetivo:** satisfacer el requerimiento del cliente sin involucrar al servidor destino.

- Usuario configura el browser: Acceso Web vía cache
- browser envía todos los requerimientos HTTP al cache
  - Si objeto está en cache: cache retorna objeto
  - Sino cache requiere los objetos desde el servidor Web, y retorna el objeto al cliente



- Ejemplo de respuesta

HTTP/1.1 200 OK

Date: Fri, 30 Oct 1998 13:19:41 GMT

Server: Apache/1.3.3 (Unix)

Cache-Control: max-age=3600

Expires: Fri, 30 Oct 1998 14:19:41 GMT

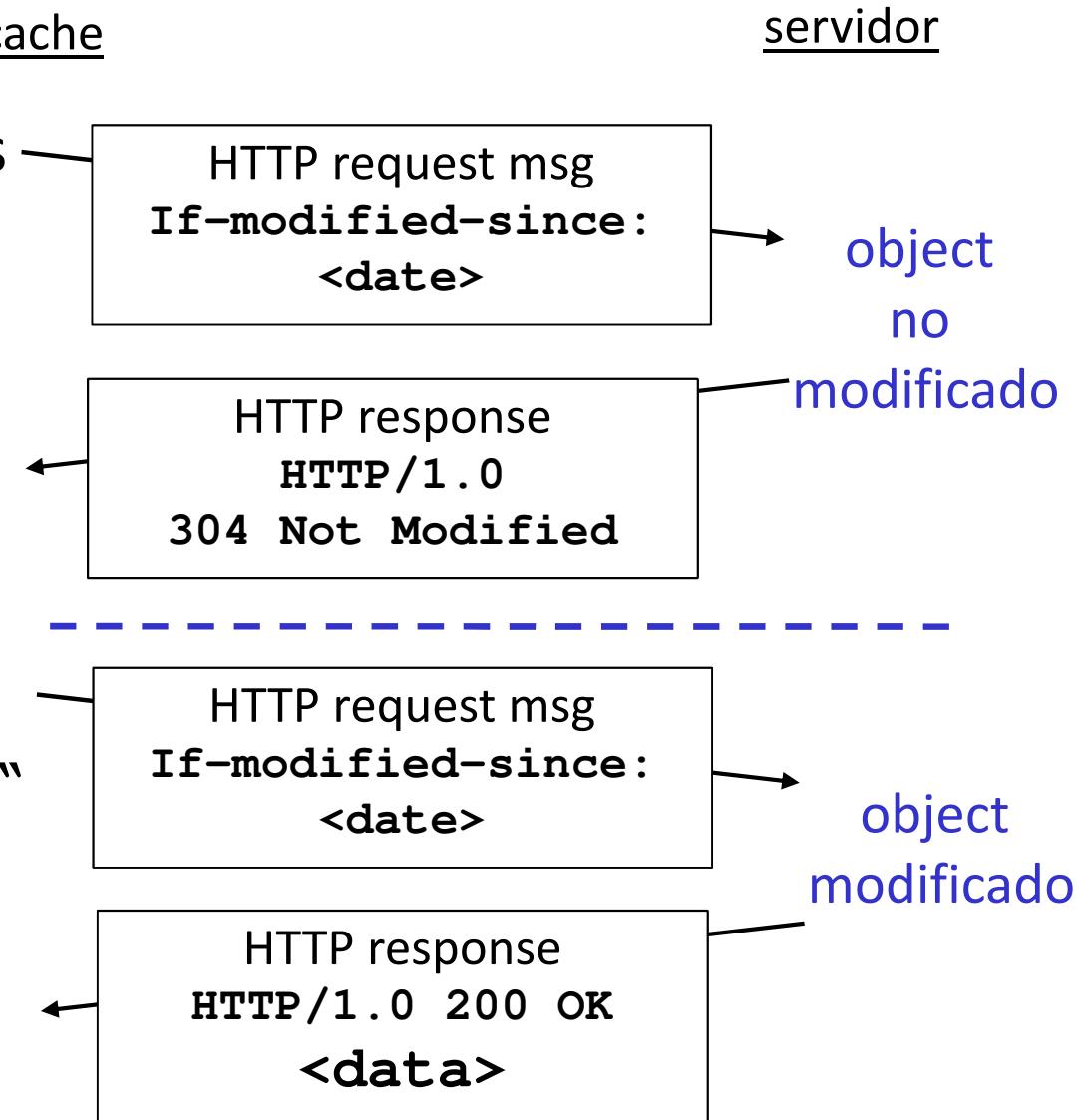
Last-Modified: Mon, 29 Jun 1998 02:28:12 GMT

ETag: "3e86-410-3596fbcc"

Content-Length: 1040

Content-Type: text/html

- **Objetivo:** no enviar objetos si el cache tiene la versión actualizada
- Cache: especifica la fecha de la copia en el requerimiento HTTP
  - If-modified-since:**  
`<date>`
  - If-None-Match:**  
`"686897696a7c876b7e"`
- servidor: responde sin el objeto si la copia de la cache es la última.:  
`HTTP/1.0 304 Not Modified`



## LA NAVEGACIÓN WEB: COOKIES

- ✓ Las **cookies** son pequeños ficheros de texto que se intercambian los clientes y servidores HTTP, para solucionar una de las principales deficiencias del protocolo: la falta de información de estado entre dos transacciones. Fueron introducidas por Netscape, y ahora han sido estandarizadas en el RFC 2109.
- La primera vez que un usuario accede a un determinado documento de un servidor, éste proporciona una *cookie* que contiene datos que relacionarán posteriores operaciones.
  - El cliente almacena la *cookie* en su sistema para usarla después. En los futuros accesos a este servidor, el *navegador* podrá proporcionar la *cookie* original, que servirá de nexo entre este acceso y los anteriores.
  - Todo este proceso se realiza automáticamente, sin intervención del usuario.

## Uso de las *cookies*

- ✓ Una *cookie* es simplemente una serie de líneas de texto, con pares variable/valor. Existe un conjunto predefinido de nombres de variable, necesarias para el correcto funcionamiento de las *cookies*.
  - **Domain**= conjunto de direcciones Internet para el que es válida la *cookie*. Se puede dar una dirección única (www.mitienda.es) o un rango (.netscape.com).
  - **Path**= fija el subconjunto de URLs para las que sirve esta *cookie*.
  - **Version**= Permite seleccionar entre diferentes versiones del modelo de *cookies*.
  - **Expires**= Fecha de expiración de la información. Si no se incluye, los datos son descartados al finalizar la sesión con el cliente Web.

## LA NAVEGACIÓN WEB: COOKIES

- ✓ Un servidor HTTP envía los diferentes campos de una *cookie* con la nueva cabecera HTTP Set-Cookie:

*Set-Cookie: Domain=www.unican.es; Path=/; Nombre=Luis; Expires Fri, 15-Jul-97 12:00:00 GMT*

- Cuando se accede a una URL que verifica el par dominio/path registrado, el cliente enviará automáticamente la información de los diferentes campos de la cookie con la nueva cabecera HTTP Cookie:

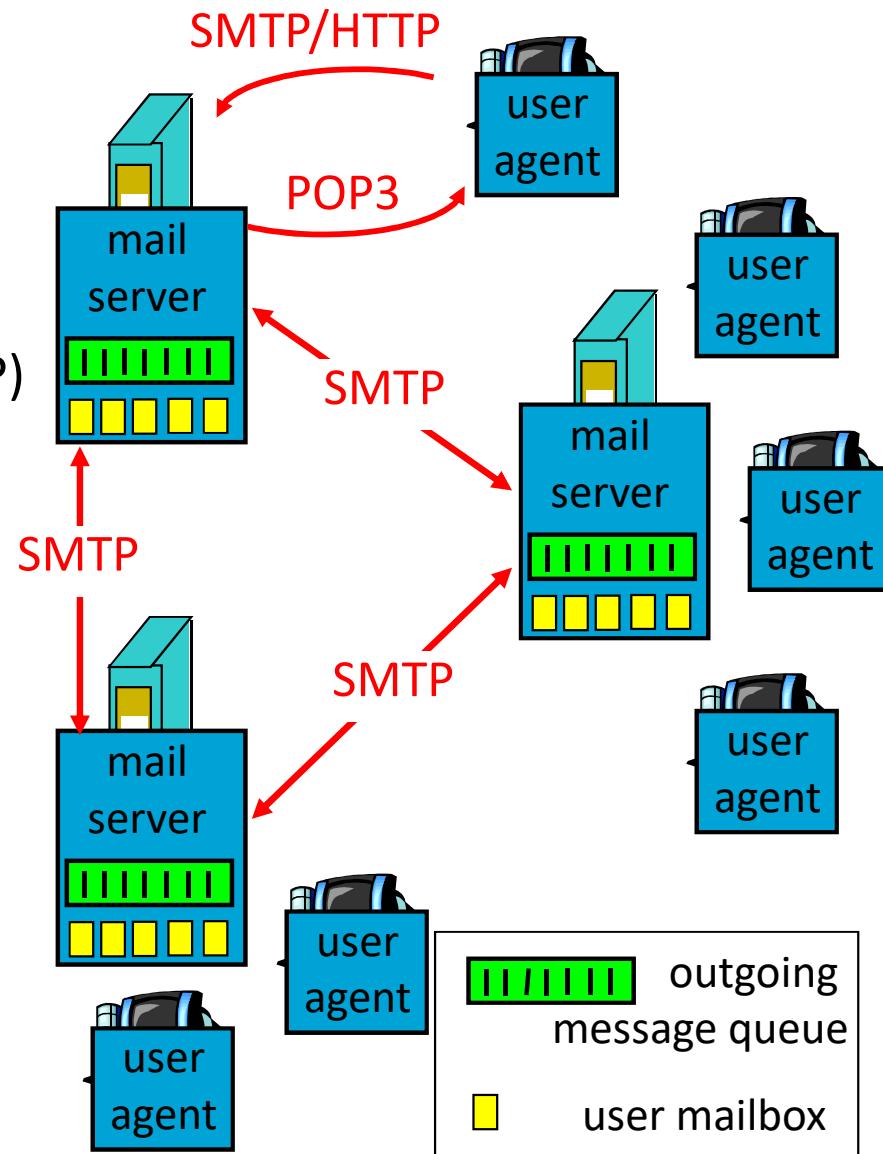
*Cookie: Domain=www.unican.es; Path=/; Nombre=Luis*

## Tema 2. SERVICIOS Y PROTOCOLOS DE APLICACIÓN EN INTERNET

1. Introducción a las aplicaciones de red
2. Servicio de Nombres de Dominio (DNS)
3. La navegación Web
- 4. El Correo electrónico**
5. Protocolos seguros
6. Aplicaciones multimedia
7. Aplicaciones para interconectividad de redes locales
8. Cuestiones y ejercicios

## EL CORREO ELECTRÓNICO

- Elementos y protocolos principales:
  - Cliente de correo (*Mail User Agent*)
  - Servidor de correo (*Mail Server* ó *Mail Transfer Agent*)
  - Protocolo de envío:  
Simple Mail Transfer Protocol (SMTP)
  - Protocolos de descarga (o lectura):  
POP3, IMAP, HTTP
- Agente de usuario (*MUA*):
  - Compone, edita y lee mensajes de correo del buzón. Ej. Outlook, Thunderbird
- Servidor de correo (*MTA*)
  - Reenvía mensajes salientes y almacena en buzones los mensajes entrantes de cada usuario.



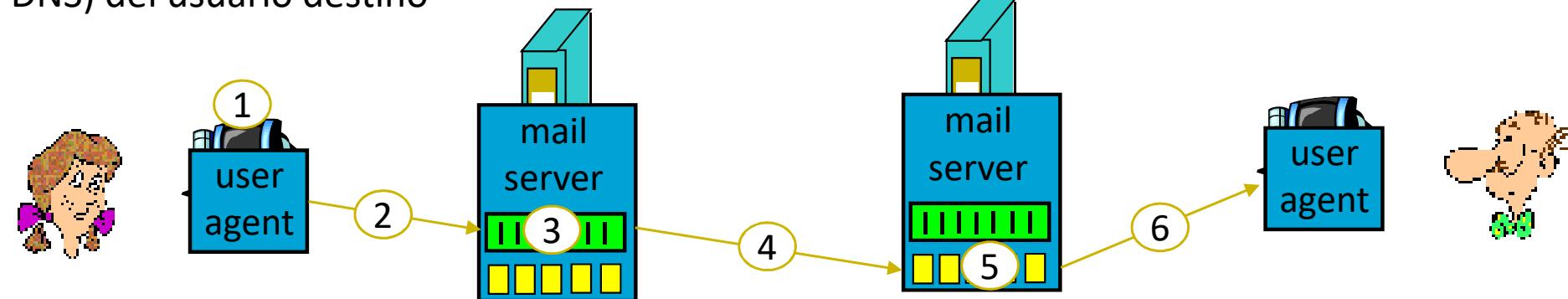
## EL CORREO ELECTRÓNICO: SMTP (RFC 2821)

- SMTP se implementa mediante dos programas (incluidos ambos en cada *mail server*):
  - Cliente SMTP: se ejecuta en el *mail server (MTA)* que está enviando correo
  - Servidor SMTP: se ejecuta en el *mail server (MTA)* que está recibiendo correo
  - "sendmail" <http://en.wikipedia.org/wiki/Sendmail>
- SMTP usa TCP en el puerto 25. Es un protocolo orientado a texto.
- SMTP es un protocolo orientado a conexión, es *in-band* y es *state-full*: implica tres fases
  - *Handshaking* (“saludo”)
  - Transferencia de mensajes
  - Cierre
- La interacción entre cliente SMTP y servidor SMTP se realiza mediante comandos/respuesta
  - **comandos:** texto ASCII
  - **respuestas:** código de estado y frases explicativas
- Los mensajes deben estar codificados en ASCII de 7 bits!! → Extensiones MIME

## EL CORREO ELECTRÓNICO: SMTP (RFC 2821)

## ➤ Pasos en el envío/recepción de correo

- 1) El usuario origen compone mediante su Agente de Usuario (MUA) un mensaje dirigido a la dirección de correo del usuario destino
- 2) Se envía con SMTP (ó HTTP) el mensaje al servidor de correo (MTA) del usuario origen que lo sitúa en la cola de mensajes salientes
- 3) El cliente SMTP abre una conexión TCP con el servidor de correo (MTA) (obtenido por DNS) del usuario destino



## EL CORREO ELECTRÓNICO: SMTP (RFC 2821)

```
S: 220 smtp1.ugr.es
C: HELO ugr.es
S: 250 smtp1.ugr.es
C: MAIL FROM: uno@ugr.es
S: 250 Ok
C: RCPT TO: dos@ugr.es
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: Correo estúpido
C: Tengo ganas de enviarte un correo...
C: ¿Te importa si lo hago?
C: .
S: 250 Ok: queued as KJSADHFFWDF
C: QUIT
S: 221 Bye
```

➤ *Propuesta de ejercicio:  
dibujar el diagrama de  
estados de SMTP*

## EL CORREO ELECTRÓNICO: SMTP (RFC 2821)

## ➤ Comandos SMTP: cliente

| Comando                  | Descripción                                                                                                                                                                                                                                                          |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HELO (ahora EHLO)</b> | Identifica el remitente al destinatario.                                                                                                                                                                                                                             |
| <b>MAIL FROM</b>         | Identifica una transacción de correo e identifica al emisor.                                                                                                                                                                                                         |
| <b>RCPT TO</b>           | Se utiliza para <b>identificar un destinatario individual</b> . Si se necesita identificar múltiples destinatarios es necesario repetir el comando.                                                                                                                  |
| <b>DATA</b>              | Permite enviar una serie de líneas de texto. El tamaño máximo de una línea es de 1.000 caracteres. Cada línea va seguida de un retorno de carro y avance de línea <CR><LF>. <b>La última línea debe llevar únicamente el carácter punto ":"</b> seguido de <CR><LF>. |
| <b>RSET</b>              | Aborta la transacción de correo actual.                                                                                                                                                                                                                              |
| <b>NOOP</b>              | No operación. <b>Indica al extremo que envíe una respuesta positiva. Keepalives</b>                                                                                                                                                                                  |
| <b>QUIT</b>              | Pide al otro extremo que envíe una respuesta positiva y cierre la conexión.                                                                                                                                                                                          |
| <b>VRFY</b>              | Pide al receptor que confirme que un nombre identifica a un destinatario valido.                                                                                                                                                                                     |
| <b>EXPN</b>              | Pide al receptor la <b>confirmación de una lista de correo</b> y que devuelva los nombres de los usuarios de dicha lista.                                                                                                                                            |
| <b>HELP</b>              | Pide al otro extremo información sobre los comandos disponibles.                                                                                                                                                                                                     |
| <b>TURN</b>              | El emisor pide que se <b>inviertan los papeles</b> , para poder actuar como receptor. El receptor puede negarse a dicha petición.                                                                                                                                    |
| <b>SOML</b>              | Si el destinatario está conectado, entrega el mensaje directamente al terminal, en caso contrario lo entrega como correo convencional.                                                                                                                               |
| <b>SAML</b>              | Entrega del mensaje en el buzón del destinatario. En caso de estar conectado también lo hace al terminal.                                                                                                                                                            |
| <b>SEND</b>              | Si el destinatario está conectado, entrega el mensaje directamente al terminal.                                                                                                                                                                                      |

## ➤ Códigos de respuesta SMTP: servidor

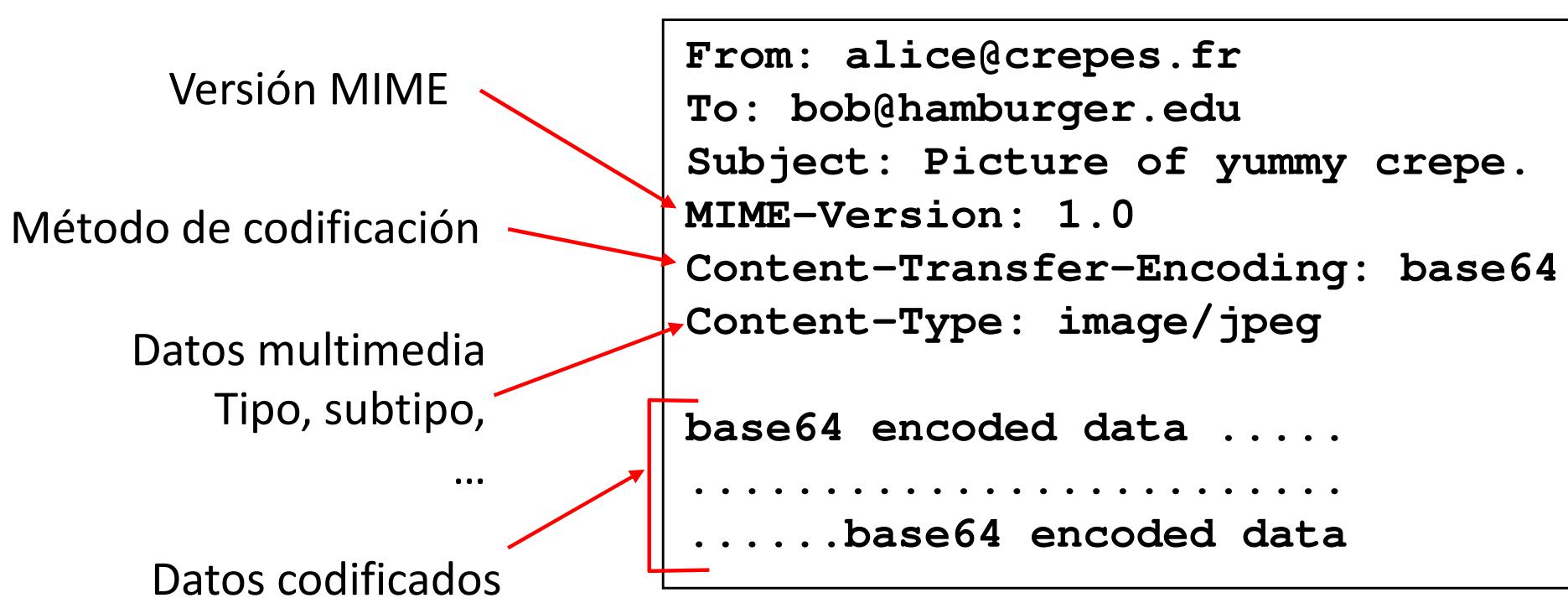
| <u>Código</u> | <u>Descripción</u>                                                                  |
|---------------|-------------------------------------------------------------------------------------|
| 211           | Estado del sistema.                                                                 |
| 214           | Mensaje de ayuda.                                                                   |
| <b>220</b>    | <b>Servicio preparado.</b>                                                          |
| <b>221</b>    | <b>Servicio cerrando el canal de transmisión.</b>                                   |
| <b>250</b>    | <b>Solicitud completada con éxito.</b>                                              |
| 251           | Usuario no local, se enviará a <dirección de reenvío>                               |
| <b>354</b>    | <b>Introduzca el texto, finalice con &lt;CR&gt;&lt;LF&gt;.&lt;CR&gt;&lt;LF&gt;.</b> |
| 421           | Servicio no disponible.                                                             |
| 450           | Solicitud de correo no ejecutada, servicio no disponible (buzón ocupado).           |
| 451           | Acción no ejecutada, error local de procesamiento.                                  |
| 452           | Acción no ejecutada, insuficiente espacio de almacenamiento en el sistema.          |
| 500           | Error de sintaxis, comando no reconocido.                                           |
| <b>501</b>    | <b>Error de sintaxis. P.ej contestación de SMTP a ESMTP</b>                         |
| 502           | Comando no implementado.                                                            |
| 503           | Secuencia de comandos errónea.                                                      |
| 504           | Parámetro no implementado.                                                          |
| 550           | Solicitud no ejecutada, buzón no disponible.                                        |
| <b>551</b>    | <b>Usuario no local, pruebe &lt;dirección de reenvío&gt;. Si no se tiene cuenta</b> |
| 552           | Acción de correo solicitada abortada.                                               |
| 553           | Solicitud no realizada (error de sintaxis).                                         |
| 554           | Fallo en la transacción.                                                            |

## Multipurpose Internet Mail Protocol Extensions (MIME):

- Nada cambia respecto a la arquitectura de correo anterior.
- Las extensiones de MIME van encaminadas a soportar:
  - Texto en conjuntos de caracteres distintos de US-ASCII;
  - Adjuntos que no son de tipo texto;
  - Cuerpos de mensajes con múltiples partes (multi-part);
  - Información de encabezados con conjuntos de caracteres distintos de ASCII.
- MIME está especificado en seis RFCs: RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289 y RFC 2077.

## EL CORREO ELECTRÓNICO: EXTENSIONES MIME

- No confundir los mensajes del protocolo con el formato de almacenamiento.



## EL CORREO ELECTRÓNICO: EXTENSIONES MIME

## ➤ Cabeceras de mensajes MIME

| Cabecera                   | Descripción                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| MIME-Version:              | Identifica la versión de MIME. Si no existe se considera que el mensaje es texto normal en inglés.                                              |
| Content-Description:       | Cadena de texto que describe el contenido. Esta cadena es necesaria para que el destinatario sepa si desea descodificar y leer el mensaje o no. |
| Content-Id:                | Identificador único, usa el mismo formato que la cabecera estándar Message-Id.                                                                  |
| Content-Transfer-Encoding: | Indica la manera en que está envuelto el cuerpo del mensaje.                                                                                    |
| Content-Type:              | Especifica la naturaleza del cuerpo del mensaje.                                                                                                |

## ➤ Content-Transfer-Encoding

- Indica la manera en que está envuelto el cuerpo para su transmisión, ya que podría haber problemas con la mayoría de los caracteres distintos de letras, números y signos de puntuación.
- Existen 5 tipos de codificación (RFC1521) : *ASCII 7, ASCII 8, codificación binaria, base64 y entrecomillada-imprimible.7.2*

## EL CORREO ELECTRÓNICO: EXTENSIONES MIME

**MIME: Content-Type: tipos y subtipos**

- La lista inicial de tipos y subtipos especificada por el RFC 1521 es:

| <b>Tipo</b> | <b>Subtipo</b> | <b>Descripción</b>                              |
|-------------|----------------|-------------------------------------------------|
| Text        | Plain          | Texto sin formato.                              |
|             | Richtext       | Texto con comandos de formato sencillos.        |
| Image       | Gif            | Imagen fija en formato GIF.                     |
|             | Jpeg           | Imagen fija en formato JPEG.                    |
| Audio       | Basic          | Sonido.                                         |
| Video       | Mpeg           | Película en formato MPEG.                       |
| Application | Octet-stream   | Secuencia de bytes no interpretada.             |
|             | Postscript     | Documento imprimible PostScript.                |
| Message     | Rfc822         | Mensaje MIME RFC 822.                           |
|             | Partial        | Mensaje dividido para su transmisión.           |
|             | External-body  | El mensaje mismo debe obtenerse de la red.      |
| Multipart   | Mixed          | Partes independientes en el orden especificado. |
|             | Alternative    | Mismo mensaje en diferentes formatos.           |
|             | Parallel       | Las partes deben verse simultáneamente.         |
|             | Digest         | Cada parte es un mensaje RFC 822 completo.      |

## MIME: Content-Type: tipo application:

- El tipo **application** es un tipo general para los formatos que requieren procesamiento externo no cubierto por ninguno de los otros tipos.
- El subtipo **octet-stream** simplemente es una secuencia de bytes no interpretados, tal que a su recepción, un agente de usuario debería *presentarla en la pantalla sugiriendo al usuario que se copie en un archivo y solicitando un nombre de archivo*.
- El subtipo **postscript**, se refiere al lenguaje PostScript de Adobe Systems. Aunque un agente de usuario puede llamar a un intérprete PostScript externo para visualizarlo, hacerlo no está exento de riesgos al ser PostScript un lenguaje de programación completo.

## EL CORREO ELECTRÓNICO: EXTENSIONES MIME

## MIME: Content-Type: tipo message:

- El tipo ***message*** permite que un mensaje esté encapsulado por completo dentro de otro. Este esquema es útil para reenviar, correo electrónico.
- El subtipo ***rfc822*** se utiliza cuando se encapsula un mensaje RFC 822 completo en un mensaje exterior.
- El subtipo ***partial*** hace posible dividir un mensaje encapsulado en pedazos y enviarlos por separado. **Los parámetros hacen posible ensamblar correctamente todas las partes en el destino.** Ej: 1/3, 2/3, 3/3.
- El subtipo ***external-body*** puede usarse para mensajes muy grandes, por ejemplo películas de vídeo. En lugar de incluir el archivo mpeg en el mensaje, se da una dirección de FTP y el agente de usuario del receptor puede obtenerlo a través de la red cuando se requiera.

## EL CORREO ELECTRÓNICO: EXTENSIONES MIME

**MIME: Content-Type: tipo multipart:**

- El tipo es ***multipart***, que permite que un mensaje contenga más de una parte, con el comienzo y el fin de cada parte claramente delimitados.
- El subtipo ***mixed*** permite que cada parte sea diferente.
- El subtipo ***alternative*** indica que cada parte contiene el mismo mensaje, pero expresado en un medio o codificación diferente.
- El subtipo ***parallel*** se usa cuando todas las partes deben “verse” simultáneamente, por ejemplo, en los canales de audio y vídeo de las películas.
- El subtipo ***digest*** se usa cuando se juntan muchos mensajes en un mensaje compuesto.

## EL CORREO ELECTRÓNICO: PROTOCOLOS DE ACCESO (POP3)

Ej: POP3 PROTOCOL TCP PORT = 110

Fase de autorización

Comandos del cliente:

**user**: nombre de usuario

**pass**: contraseña

Respuestas del servidor

+OK

-ERR

Fase de transacción, cliente:

**list**: lista mensajes por número

**retr**: obtiene mensajes por num.

**dele**: borra

**quit**

Fase de actualización del servidor  
(tras desconexión)

```
S: +OK POP3 server ready
C: user bob
S: +OK
C: pass hungry
S: +OK user successfully logged on
C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: <message 1 contents>
S: .
C: dele 1
C: retr 2
S: <message 1 contents>
S: .
C: dele 2
C: quit
S: +OK POP3 server signing off
```

## EL CORREO ELECTRÓNICO: PROTOCOLOS DE ACCESO (POP3)

## Comandos POP3

| Comando             | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| USER identification | Este comando permite la autenticación. Debe estar seguido del nombre de usuario, es decir, una cadena de caracteres que identifique al usuario en el servidor. El comando USER debe preceder al comando PASS.                                                                                                                                                                                                                                                                                             |
| PASS password       | El comando PASS permite especificar la contraseña del usuario cuyo nombre ha sido especificado por un comando USER previo.                                                                                                                                                                                                                                                                                                                                                                                |
| STAT                | Información acerca de los mensajes del servidor                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| RETR                | Número del mensaje que se va a recoger                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| DELE                | Número del mensaje que se va a eliminar                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| LIST [msg]          | Número del mensaje que se va a mostrar                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| NOOP                | Permite mantener la conexión abierta en caso de inactividad                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| TOP <messageID> <n> | Comando que muestra <i>n</i> líneas del mensaje, cuyo número se da en el argumento. En el caso de una respuesta positiva del servidor, éste enviará de vuelta los encabezados del mensaje, después una línea en blanco y finalmente las primeras <i>n</i> líneas del mensaje.                                                                                                                                                                                                                             |
| UIDL [msg]          | Solicitud al servidor para que envíe una línea que contenga información sobre el mensaje que eventualmente se dará en el argumento. Esta línea contiene una cadena de caracteres denominada <i>unique identifier listing (lista de identificadores únicos)</i> que permite identificar de manera única el mensaje en el servidor, independientemente de la sesión. El argumento opcional es un número relacionado con un mensaje existente en el servidor POP, es decir, un mensaje que no se ha borrado. |
| QUIT                | El comando QUIT solicita la salida del servidor POP3. Lleva a la eliminación de todos los mensajes marcados como eliminados y envía el estado de esta acción.                                                                                                                                                                                                                                                                                                                                             |

## EL CORREO ELECTRÓNICO: PROTOCOLOS DE ACCESO

## ➤ Ventajas de IMAP4:

- Permite organización en carpetas en el lado del servidor (MTA)
- Para ello, mantiene información entre sesiones (asociando *flags* a los mensajes).
- Permite la descarga de partes de los mensajes.
- Posible acceder con varios clientes (POP también, pero en modo descargar y guardar)

## ➤ Ventajas de Web MAIL:

- Organización total en el servidor, accesible desde cualquier cliente con HTTP.
- Seguridad: Uso extendido de HTTPS

➤ Listado de puertos relacionados con e-mail:

POP3 - port 110

IMAP - port 143

SMTP - port 25

HTTP - port 80

Secure SMTP (SSMTP) - port 465

Secure IMAP (IMAP4-SSL) - port 585

IMAP4 over SSL (IMAPS) - port 993

Secure POP3 (SSL-POP) - port 995

## Tema 2. SERVICIOS Y PROTOCOLOS DE APLICACIÓN EN INTERNET

1. Introducción a las aplicaciones de red
2. Servicio de Nombres de Dominio (DNS)
3. La navegación Web
4. El Correo electrónico
- 5. Seguridad & protocolos seguros**
6. Aplicaciones multimedia
7. Aplicaciones para interconectividad de redes locales
8. Cuestiones y ejercicios

## ➤ Primitivas (dimensiones) de seguridad

- **Confidencialidad**
  - Sólo accede a la información quien debe hacerlo.
- **Responsabilidad**
  - Autenticación: las entidades son quien dicen ser.
  - No repudio: no se puede negar el autor de una determinada acción.
  - Control de accesos: garantía de identidad para el acceso.
- **Integridad**
  - Detección de alteraciones (intencionadas o no) de la información.
- **Disponibilidad**
  - Mantener las prestaciones de los servicios con independencia de la demanda.

## ➤ Mecanismos de Seguridad

- **Cifrado Simétrico:**  $C = K(P) \& P = K(C)$ 
  - DES, 3DES, AES, RC4
- **Cifrado Asimétrico:**  $C = K^+(P) \& P = K^-(C)$ 
  - RSA
- **Funciones Hash.**  $M \rightarrow H(M)$  ejemplos de funciones HASH: MD5, SHA-1, SHA-512
- **Hash Message Authentication Code (HMAC):** integridad + autenticación  
 $M + H(K|M)$  pero para evitar ataques de extensión se usa  $M + H(K | H(K | M))$
- **Firma Digital:**

A -----> B:  $K^{+B}(K^{-A}(M)) \rightarrow$  confidencialidad+ autenticación + no repudio

$K^{+B}(K^{-A}(M | H(M))) \rightarrow$  + integridad

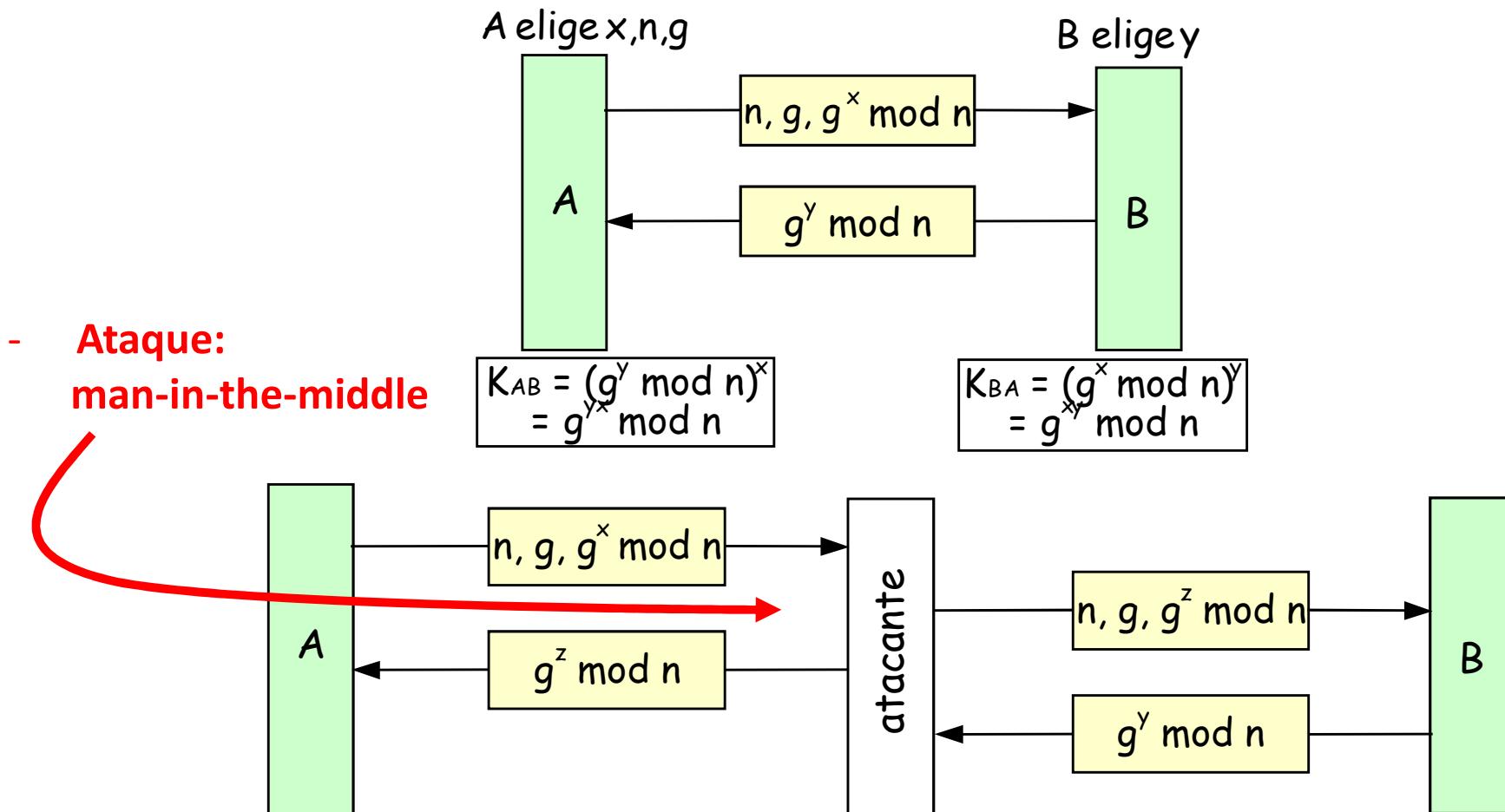
$M | K^{+B}(K^{-A}(H(M))) \rightarrow$  ?

- **Certificado:**  $(ID, K^{+ID}) + K^{-CA} (ID, K^{+ID})$  CA: Autoridad de Certificación.

## PROTOCOLOS SEGUROS

## ➤ Mecanismos de Seguridad

- **Intercambio de Diffie-Hellman:** permite establecer una clave secreta entre dos entidades a través de un canal no seguro.



## PROTOCOLOS SEGUROS

- Seguridad:
  - Seguridad Perimetral:
    - Firewalls, sistemas de detección de intrusiones (IDS) y de respuesta (IRS)
  - Seguridad (criptográfica) en protocolos (¿dónde poner la seguridad?):
    - Capa de aplicación
      - Pretty Good Privacy (PGP)
      - Secure Shell (SSH)
    - Capa de sesión (entre aplicación y transporte)
      - Transport Secure Layer (TSL) (antes SSL) → HTTPS, IMAPS, SSL-POP, VPN.  
TSL = Handshake (negociar) + Record Protocol (operación).  
TSL → Confidencialidad ( $K_{\text{secreta negociada}}$ ) + Autenticación (para el server por defecto con  $K_{\text{PÚBLICA}}$ ) + integridad (Con HMAC)
      - Capa de Red → IPSec (VPN)

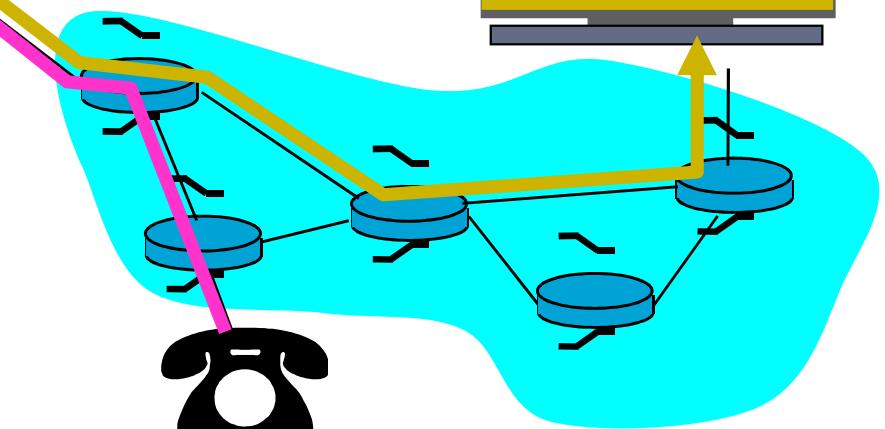
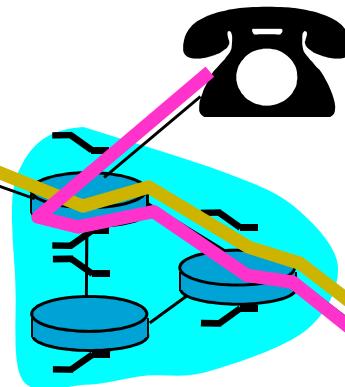
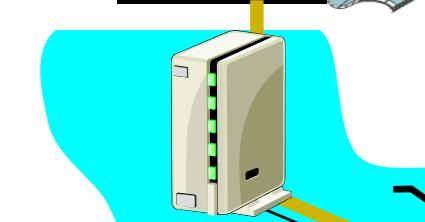
## Tema 2. SERVICIOS Y PROTOCOLOS DE APLICACIÓN EN INTERNET

1. Introducción a las aplicaciones de red
2. Servicio de Nombres de Dominio (DNS)
3. La navegación Web
4. El Correo electrónico
5. Protocolos seguros
- 6. Aplicaciones multimedia**
7. Aplicaciones para interconectividad de redes locales
8. Cuestiones y ejercicios

➤ Conceptos: IP = “*tecnología de convergencia*” →



Aplicaciones Multimedia: audio, vídeo, juegos, real-time



Calidad de servicio (QoS): capacidad de ofrecer el rendimiento requerido para una aplicación

IP ofrece Mejor esfuerzo (*best effort*): sin garantías de QoS

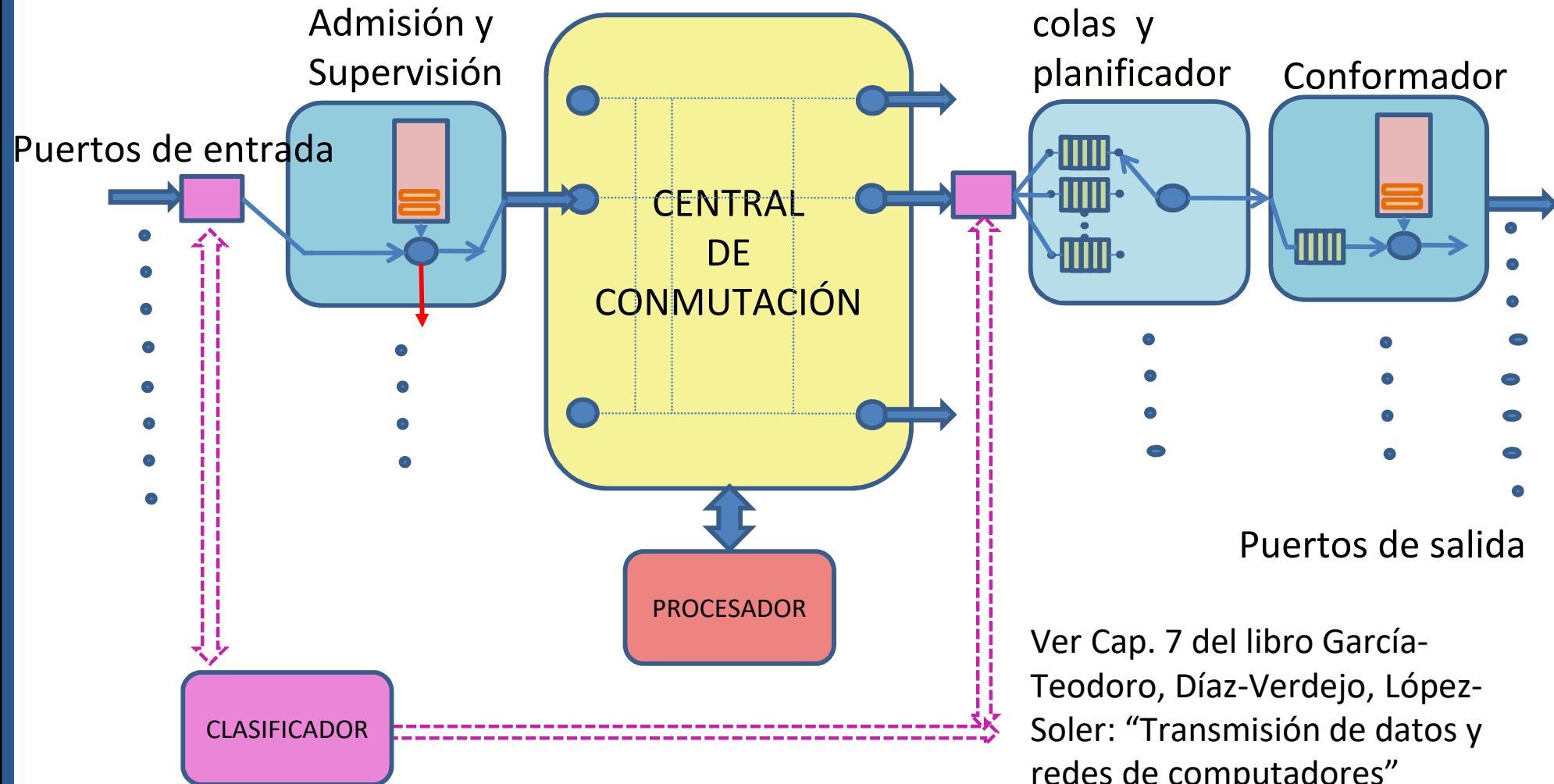
## ➤ Tipos de aplicaciones

- Flujo de audio y vídeo (*streaming*) almacenado ➔ Ej. YouTube
- Flujo de audio y vídeo en vivo ➔ Ej. emisoras de radio o IPTV
- Audio y vídeo interactivo ➔ Ej. Skype

## ➤ Características fundamentales

- Elevado ancho de banda
- Tolerantes relativamente a la pérdida de datos
- Exigen *Delay* (retardo) acotado
- Exigen *Jitter* (fluctuación del retardo) acotado
- Se pueden beneficiar de usar de *multicast* (*direcciones destino de grupo*)

➤ ¿Cómo es un *router* con QoS?



## Tema 2. SERVICIOS Y PROTOCOLOS DE APLICACIÓN EN INTERNET

1. Introducción a las aplicaciones de red
2. Servicio de Nombres de Dominio (DNS)
3. La navegación Web
4. El Correo electrónico
5. Protocolos seguros
6. Aplicaciones multimedia
- 7. Aplicaciones para interconectividad de redes locales**
8. Cuestiones y ejercicios

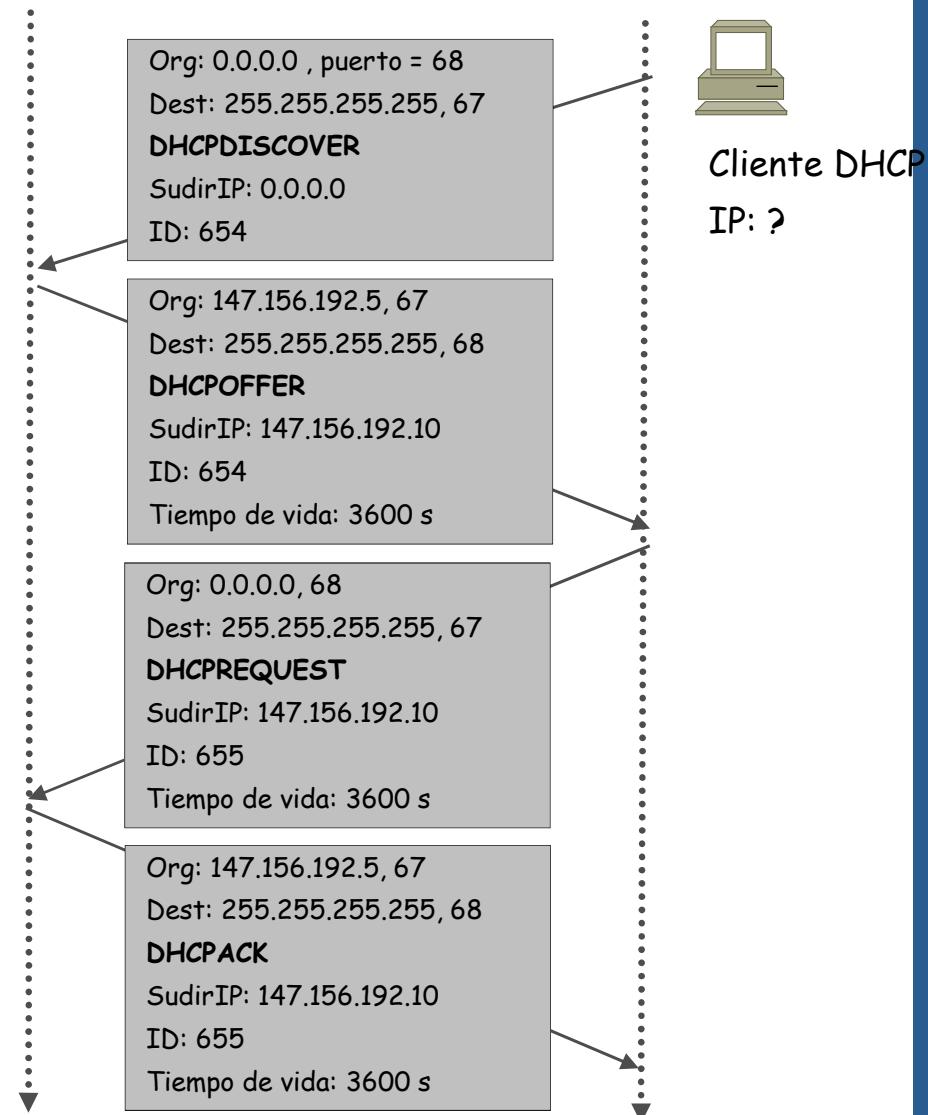
## APLICACIONES PARA INTERCONECTIVIDAD DE REDES LOCALES: DHCP

## DHCP (Dynamic Host Configuration Protocol)



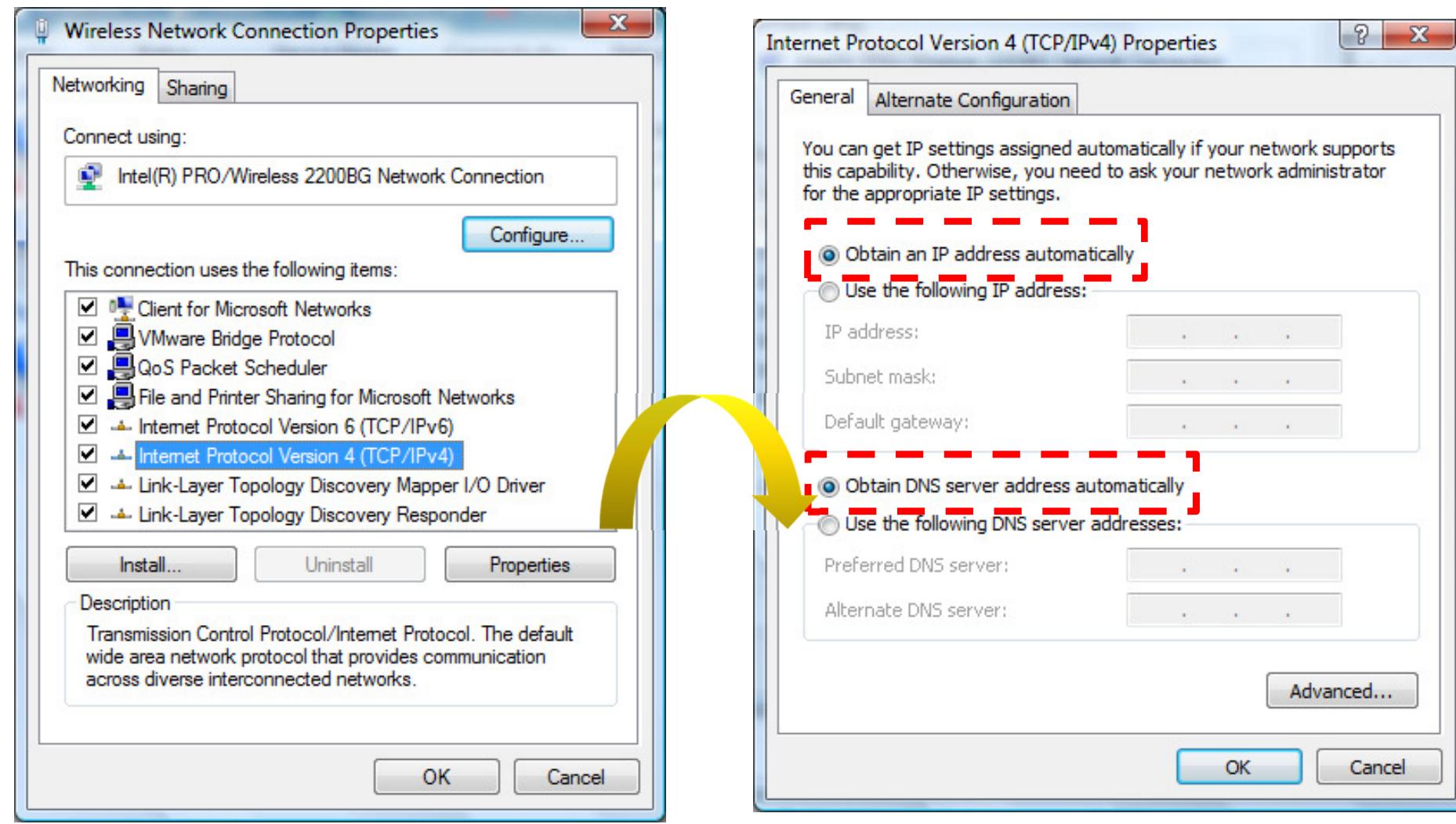
Para asignar las direcciones se usa **DHCP** (RFC 2131-3396), protocolo usuario de UDP (**puerto 67**)

- El host (cliente) envía un mensaje *broadcast*: "DHCP discover"
- El server DHCP responde con un mensaje "DHCP offer"
- El host solicita una dirección IP, mensaje "DHCP request"
- El server DHCP envía la dirección IP: mensaje "DHCP ack"



## APLICACIONES PARA INTERCONECTIVIDAD DE REDES LOCALES: DHCP

## Configuración de un cliente MS Windows:



## APLICACIONES PARA INTERCONECTIVIDAD DE REDES LOCALES: DHCP

### Configuración de un cliente Linux (Fedora Core distribution):

```
Sample /etc/sysconfig/network-scripts/ifcfg-eth0 :

DEVICE=eth0
BOOTPROTO=dhcp
HWADDR=00:0C:29:CE:63:E3
ONBOOT=yes
TYPE=Ethernet
```

### Configuración de un servidor de Linux (*dhcpd*):

```
Sample /etc/dhcpd.conf

default-lease-time 600;max-lease-time 7200;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option routers 192.168.1.254;
option domain-name-servers 192.168.1.1, 192.168.1.2;
option domain-name "mydomain.org";
subnet 192.168.1.0 netmask 255.255.255.0 {
 range 192.168.1.10 192.168.1.100;
 range 192.168.1.150 192.168.1.200;
}

Static IP address assignment
host haagen {
 hardware ethernet 08:00:2b:4c:59:23;
 fixed-address 192.168.1.222;
}
```

## Tema 2. SERVICIOS Y PROTOCOLOS DE APLICACIÓN EN INTERNET

1. Introducción a las aplicaciones de red
2. Servicio de Nombres de Dominio (DNS)
3. La navegación Web
4. El Correo electrónico
5. Protocolos seguros
6. Aplicaciones multimedia
7. Aplicaciones para interconectividad de redes locales
- 8. Cuestiones y ejercicios**



## CUESTIONES Y EJERCICIOS

**3. Discuta las características de las siguientes aplicaciones en términos de su tolerancia a la pérdida de datos, los requisitos temporales, la necesidad de rendimiento mínimo y la seguridad.**

**La telefonía móvil**

**WhatsApp**

**YouTube**

**Spotify**

**Comercio electrónico**

## CUESTIONES Y EJERCICIOS

**9. Una sucursal con 50 empleados en Granada tiene una red interna basada en *FastEthernet* (100Mbps) que se conecta a Internet con una red de acceso ADSL de 0,5 Mbps de subida y 1,5 Mbps de bajada. Cada empleado, en el desempeño de su trabajo, realiza un promedio de 2000 solicitudes de información a la hora a un servidor de Base de Datos ubicado en la central del banco, en Madrid, donde cada solicitud supone el envío por parte del servidor de 10 registros de 1KB cada uno. Adicionalmente, la modificación de datos tras algunas de estas solicitudes supone el envío de 100 actualizaciones, de 10 registros, a la hora desde la sucursal al servidor. El resto de los servicios telemáticos se restringe.**

- a. Calcule la velocidad de transmisión requerida. ¿Es la velocidad del enlace de acceso suficiente?
- b. ¿y si se dobla la velocidad del enlace? ¿cuál sería el tiempo de cola que esperaría en promedio cada solicitud en el enlace descendente antes de ser enviada? Considere que cada registro se envía por separado, con una cabecera de tamaño despreciable
- c. Si, alternativamente, se diseña una caché que permite evitar un 70% de los accesos a la BD ¿cuál sería el tiempo de cola que esperaría en promedio cada solicitud en el enlace descendente? ¿qué solución es mejor, la b. o esta?



## CUESTIONES Y EJERCICIOS

1. Explicar por qué cuando solicitamos <http://www.google.com> desde nuestro navegador, se muestra la URL servida desde ([www.google.es](http://www.google.es))

¿qué relación tienen esos 2 nombres de dominio?

¿guarda google información sobre nuestra localización? ¿cómo se obtiene?

¿qué herramientas e información se necesita?

¿qué ocurre y cómo influye si configuro en mi navegador como lenguaje preferido “francés”?

¿pueden servirse páginas dependiendo de nuestra localización? ¿en su caso, con qué precisión?

Sugerencia: Usar el analizador <http://www.wireshark.org> para mostrar trazas