TEMA 2
SERVICIOS Y PROTOCOLOS DE APLICACIÓN EN INTERNET

Fundamentos de Redes
2017/2018

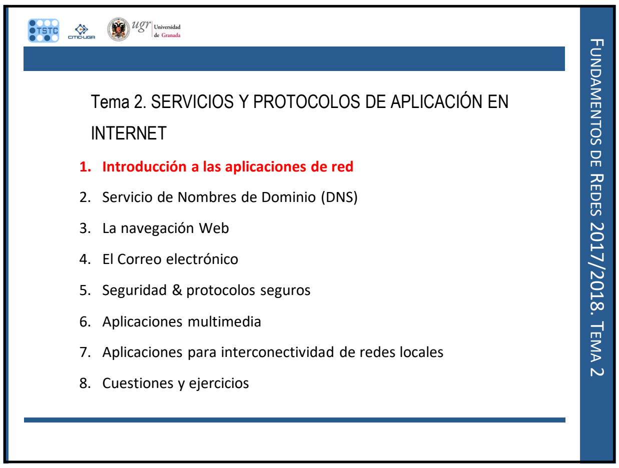
➢Bibliografía Básica:

Capítulo 2 (2.1, 2.2, 2.4, 2.5) & 8 (8.2, 8.3), James F. Kurose y Keith W. Ross. ***COMPUTER NETWORKING. A TOP-DOWN APPROACH***, 5ª Edición, Addison-Wesley, 2010, ISBN: 9780136079675.

Capítulo 11 y 12.3 Pedro García Teodoro, Jesús Díaz Verdejo y Juan Manuel López Soler. ***TRANSMISIÓN DE DATOS Y REDES DE COMPUTADORES***, 2ª Ed. ,Pearson, 2014, ISBN: 978-0-273-76896-8

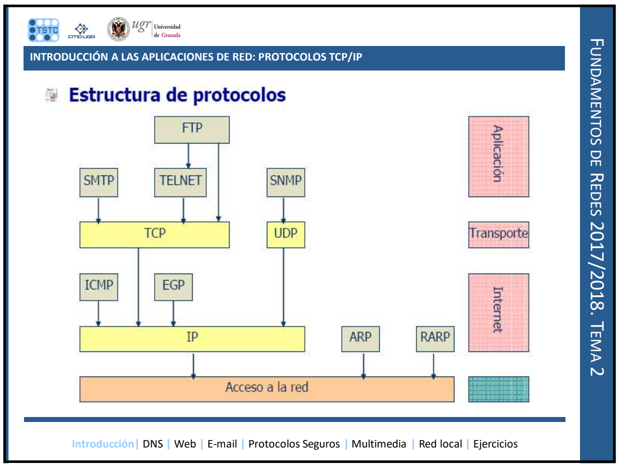
➢ Agradecimientos:

Parte de estas transparencias están inspiradas en las transparencias utilizadas por Kurose y Ross en de 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. Seguridad & protocolos seguros
6. Aplicaciones multimedia
7. Aplicaciones para interconectividad de redes locales
8. Cuestiones y ejercicios

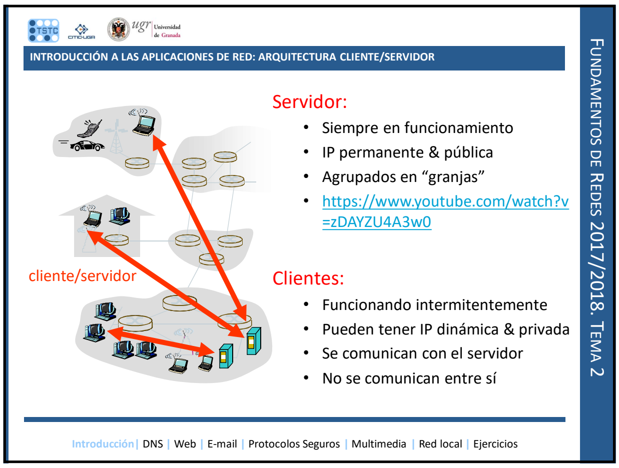


INTRODUCCIÓN A LAS APLICACIONES DE RED: PROTOCOLOS TCP/IP

Estructura de protocolos

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



INTRODUCCIÓN A LAS APLICACIONES DE RED: ARQUITECTURA CLIENTE/SERVIDOR

Servidor:

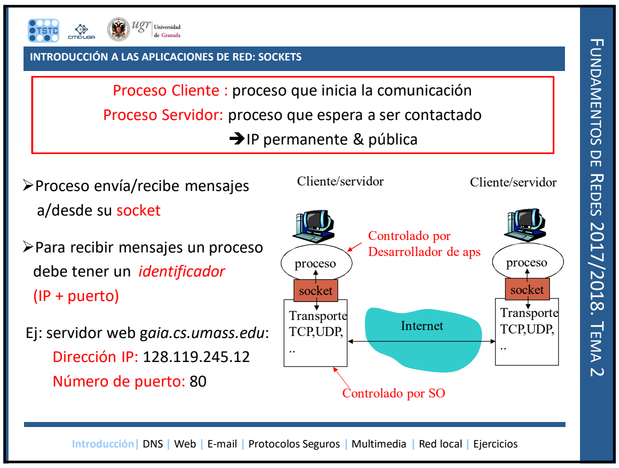
- Siempre en funcionamiento
- IP permanente & pública
- Agrupados en "granjas"
- https://www.youtube.com/watch?v=zDAYZU4A3w0

Clientes:

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

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



INTRODUCCIÓN A LAS APLICACIONES DE RED: SOCKETS

Proceso Cliente : proceso que inicia la comunicación
Proceso Servidor: proceso que espera a ser contactado
➔IP permanente & pública

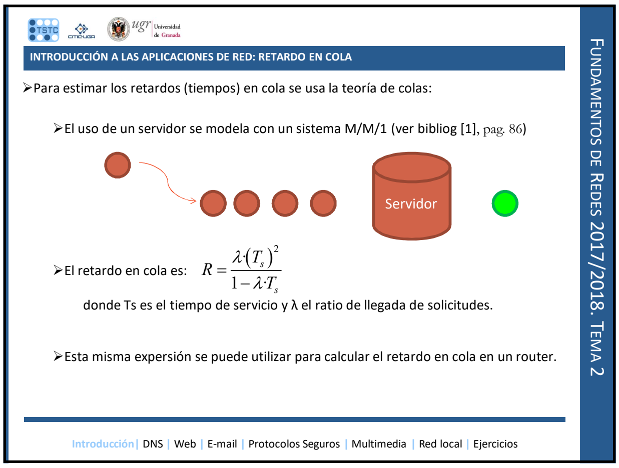
➢Proceso envía/recibe mensajes a/desde su socket

➢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

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



INTRODUCCIÓN A LAS APLICACIONES DE RED: RETARDO EN COLA

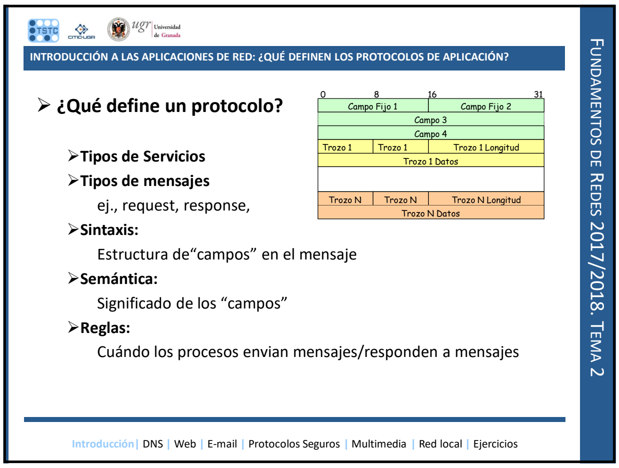
- Para estimar los retardos (tiempos) en cola se usa la teoría de colas:
  - El uso de un servidor se modela con un sistema M/M/1 (ver bibliog [1], pag. 86)

  - El retardo en cola es: $R = \frac{\lambda (T_s)^2}{1 - \lambda \cdot T_s}$

    donde Ts es el tiempo de servicio y λ el ratio de llegada de solicitudes.
  - Esta misma expersión se puede utilizar para calcular el retardo en cola en un router.

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



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

- **¿Qué define un protocolo?**
  - **Tipos de Servicios**
  - **Tipos de mensajes**

    ej., request, response,
  - **Sintaxis:**

    Estructura de“campos” en el mensaje
  - **Semántica:**

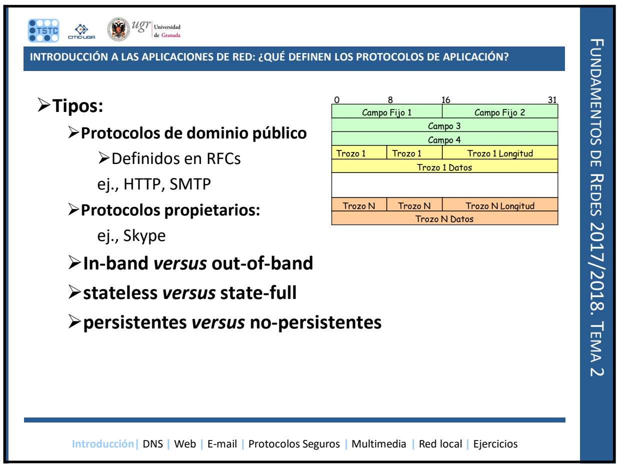
    Significado de los “campos”
  - **Reglas:**

    Cuándo los procesos envian mensajes/responden a mensajes

0	8	16	31
Campo Fijo 1		Campo Fijo 2	
Campo 3			
Campo 4			
Trozo 1	Trozo 1	Trozo 1 Longitud	
Trozo 1 Datos			
Trozo N	Trozo N	Trozo N Longitud	
Trozo N Datos			

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



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

- **Tipos:**
  - **Protocolos de dominio público**
    - Definidos en RFCs

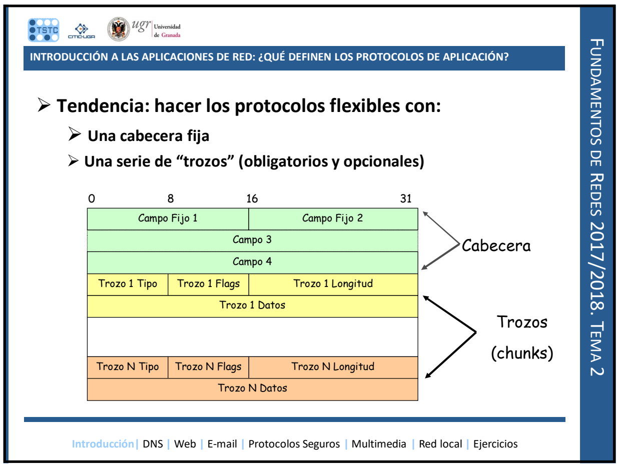
    ej., HTTP, SMTP
  - **Protocolos propietarios:**

    ej., Skype
  - **In-band *versus* out-of-band**
  - **stateless *versus* state-full**
  - **persistentes *versus* no-persistentes**

0	8	16	31
Campo Fijo 1		Campo Fijo 2	
Campo 3			
Campo 4			
Trozo 1	Trozo 1	Trozo 1 Longitud	
Trozo 1 Datos			
Trozo N	Trozo N	Trozo N Longitud	
Trozo N Datos			

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



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)**

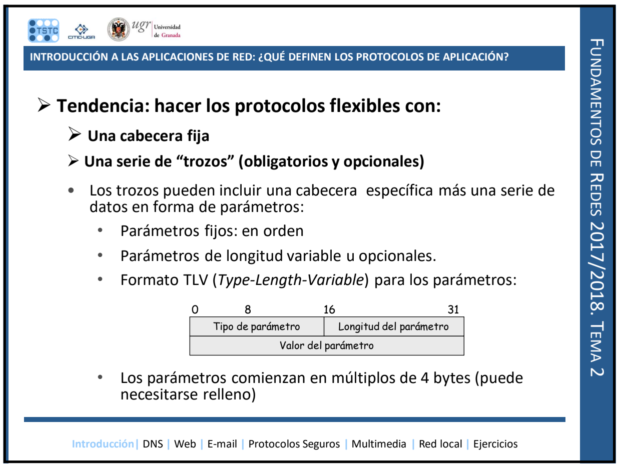
0	8	16	31
Campo Fijo 1		Campo Fijo 2	
Campo 3			
Campo 4			
Trozo 1 Tipo	Trozo 1 Flags	Trozo 1 Longitud	
Trozo 1 Datos			
Trozo N Tipo	Trozo N Flags	Trozo N Longitud	
Trozo N Datos			

Cabecera

Trozos (chunks)

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

FUNDAMENTOS DE REDES 2017/2018. TEMA 2



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

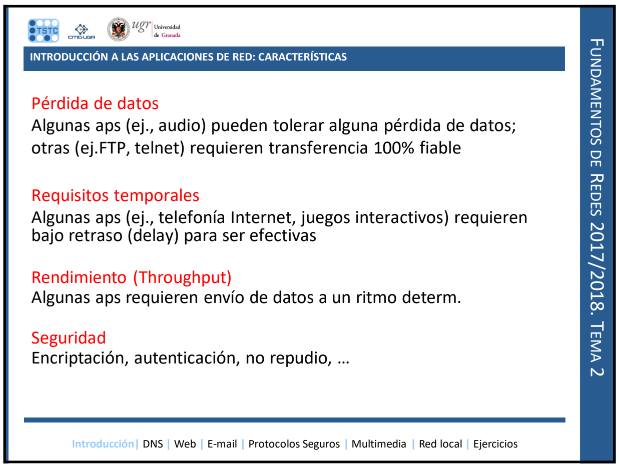
- **Tendencia: hacer los protocolos flexibles con:**
  - **Una cabecera fija**
  - **Una serie de “trozos” (obligatorios y opcionales)**
  - Los trozos pueden incluir una cabecera específica más una serie de datos en forma de parámetros:
    - Parámetros fijos: en orden
    - Parámetros de longitud variable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

0	8	16	31
Tipo de parámetro		Longitud del parámetro	
Valor del parámetro			

    - Los parámetros comienzan en múltiplos de 4 bytes (puede necesitarse relleno)

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

FUNDAMENTOS DE REDES 2017/2018. TEMA 2



INTRODUCCIÓN A LAS APLICACIONES DE RED: CARACTERÍSTICAS

Pérdida de datos
Algunas aps (ej., audio) pueden tolerar alguna pérdida de datos; otras (ej.FTP, telnet) requieren transferencia 100% fiable

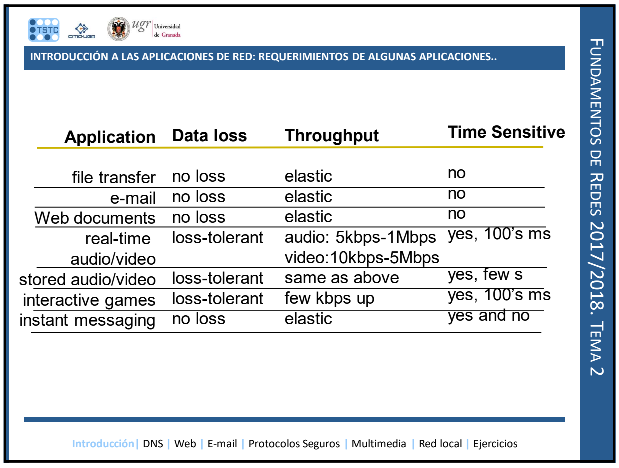
Requisitos temporales
Algunas aps (ej., telefonía Internet, juegos interactivos) requieren bajo retraso (delay) para ser efectivas

Rendimiento (Throughput)
Algunas aps requieren envío de datos a un ritmo determ.

Seguridad
Encriptación, autenticación, no repudio, …

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

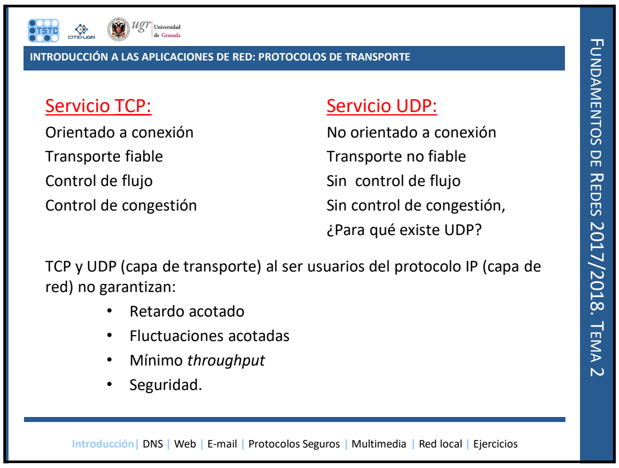


INTRODUCCIÓN A LAS APLICACIONES DE RED: REQUERIMIENTOS DE ALGUNAS APLICACIONES..

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 | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

FUNDAMENTOS DE REDES 2017/2018. TEMA 2



INTRODUCCIÓN A LAS APLICACIONES DE RED: PROTOCOLOS DE TRANSPORTE

Servicio TCP:
Orientado a conexión
Transporte fiable
Control de flujo
Control de congestión

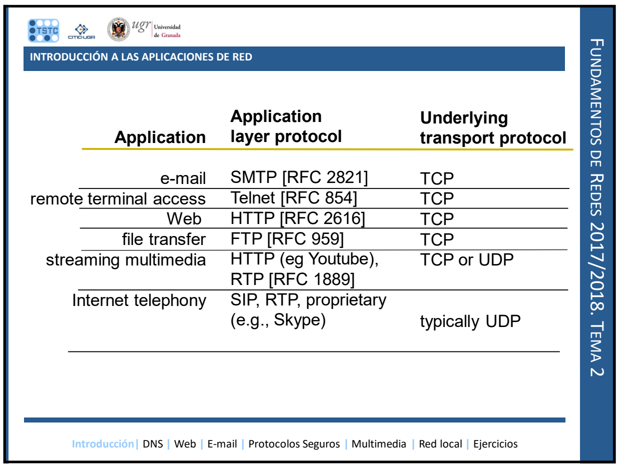
Servicio UDP:
No orientado a conexión
Transporte no fiable
Sin control de flujo
Sin control de congestión,
¿Para qué existe UDP?

TCP y UDP (capa de transporte) al ser usuarios del protocolo IP (capa de red) no garantizan:

- Retardo acotado
- Fluctuaciones acotadas
- Mínimo *throughput*
- Seguridad.

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

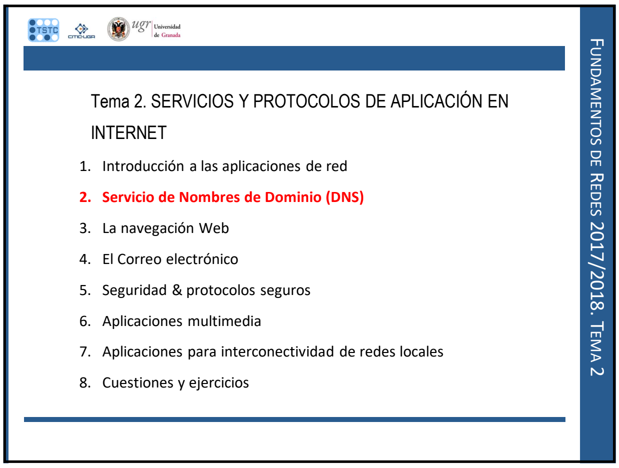


INTRODUCCIÓN A LAS APLICACIONES DE RED

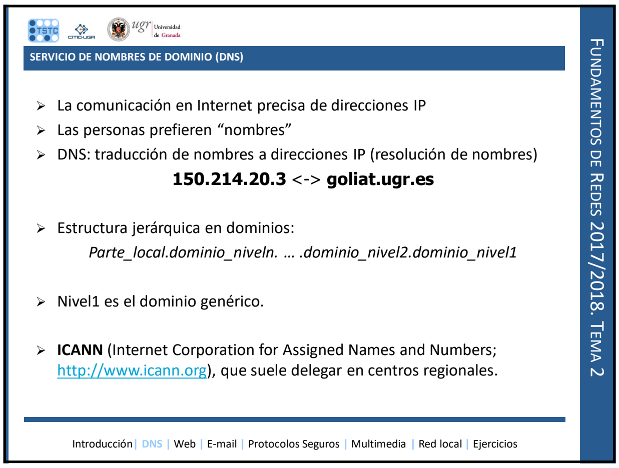
Application	Application layer protocol	Underlying transport protocol
e-mail	SMTP [RFC 2821]	TCP
remote terminal access	Telnet [RFC 854]	TCP
Web	HTTP [RFC 2616]	TCP
file transfer	FTP [RFC 959]	TCP
streaming multimedia	HTTP (eg Youtube), RTP [RFC 1889]	TCP or UDP
Internet telephony	SIP, RTP, proprietary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

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

FUNDAMENTOS DE REDES 2017/2018. TEMA 2



Tema 2. SERVICIOS Y PROTOCOLOS DE APLICACIÓN EN INTERNET



SERVICIO DE NOMBRES DE DOMINIO (DNS)

- La comunicación en Internet precisa de direcciones IP
- Las personas prefieren “nombres”
- DNS: traducción de nombres a direcciones IP (resolución de nombres)

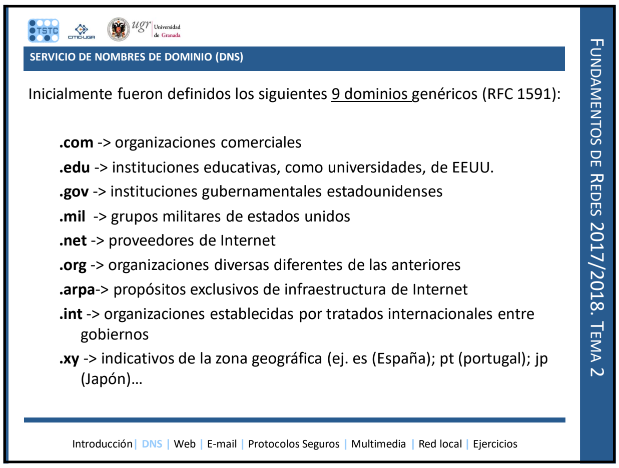
  150.214.20.3 <-> **goliat.ugr.es**

- Estructura jerárquica en dominios:

  Parte_local.dominio_niveln. … .dominio_nivel2.dominio_nivel1

- Nivel1 es el dominio genérico.

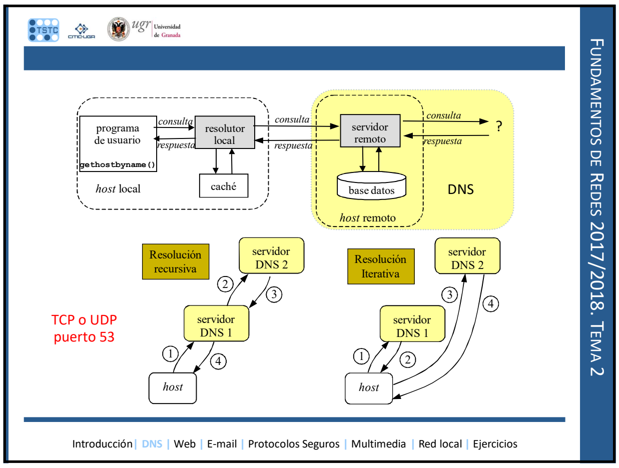
- **ICANN** (Internet Corporation for Assigned Names and Numbers; http://www.icann.org), que suele delegar en centros regionales.



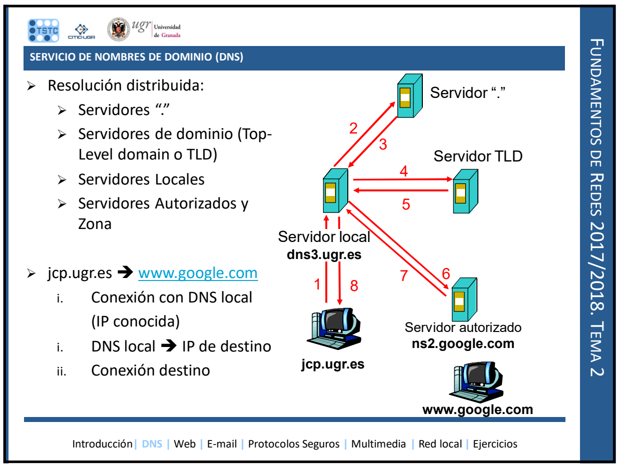
SERVICIO DE NOMBRES DE DOMINIO (DNS)

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)…

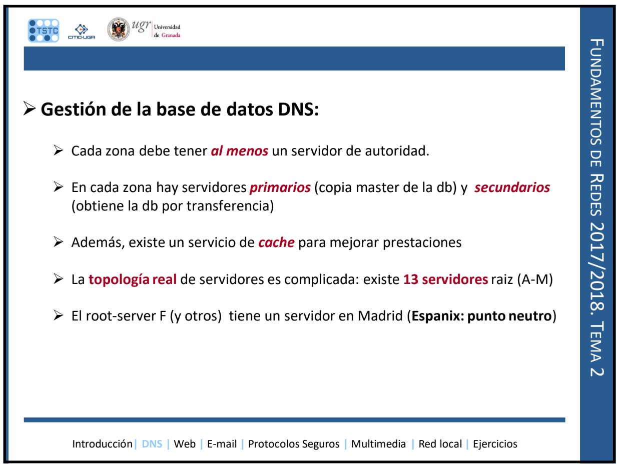


TCP o UDP
puerto 53

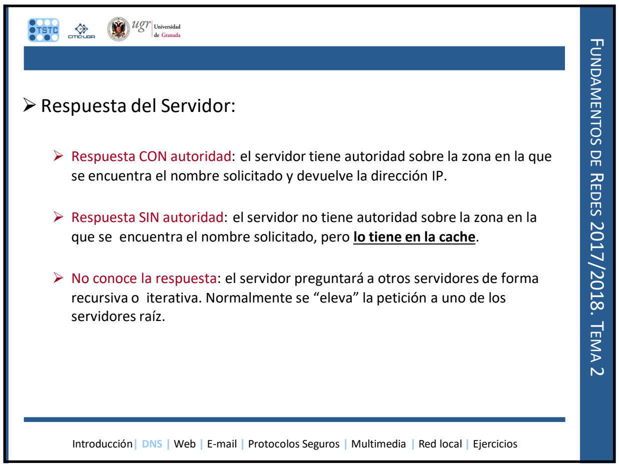


SERVICIO DE NOMBRES DE DOMINIO (DNS)

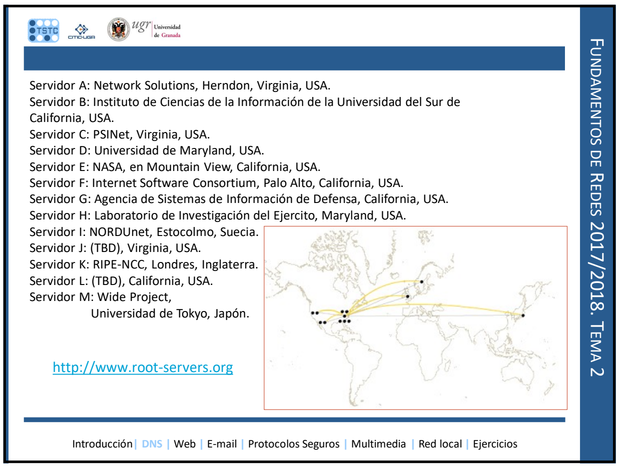
- Resolución distribuida:
  - Servidores “.”
  - Servidores de dominio (Top-Level domain o TLD)
  - Servidores Locales
  - Servidores Autorizados y Zona
- jcp.ugr.es ➔ www.google.com
  i. Conexión con DNS local (IP conocida)
  i. DNS local ➔ IP de destino
  ii. Conexión destino



- **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*** (obtiene la db por transferencia)
  - Además, existe un servicio de ***cache*** para mejorar prestaciones
  - La **topología real** de servidores es complicada: existe **13 servidores** raiz (A-M)
  - El root-server F (y otros) tiene un servidor en Madrid (**Espanix: punto neutro**)

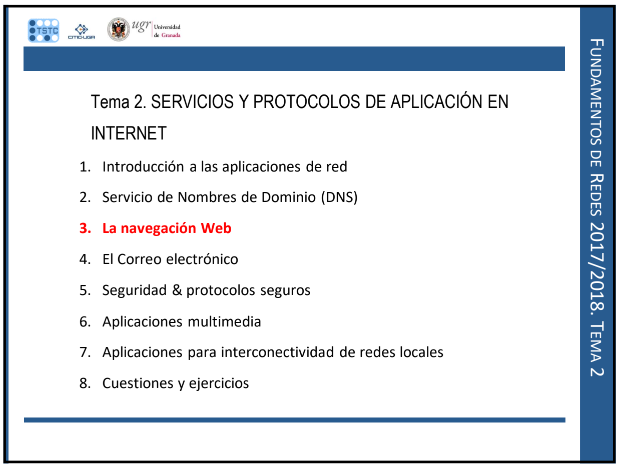


- Respuesta del Servidor:
  - Respuesta CON autoridad: el servidor tiene autoridad sobre la zona en la que se encuentra el nombre solicitado y devuelve la dirección IP.
  - Respuesta SIN autoridad: el servidor no tiene autoridad sobre la zona en la que se encuentra el nombre solicitado, pero **lo tiene 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.



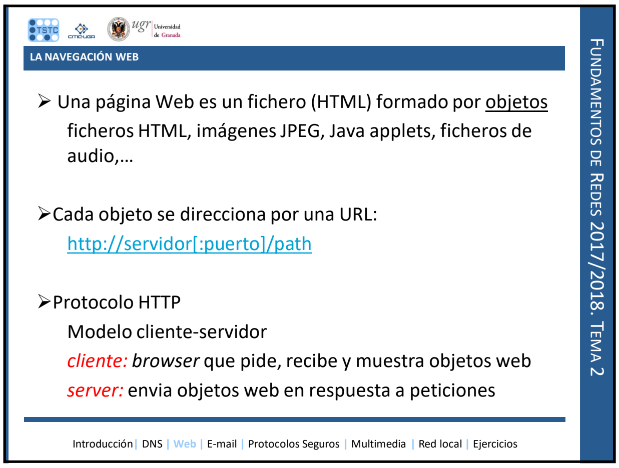
Servidor A: Network Solutions, Herndon, Virginia, USA.
Servidor B: Instituto de Ciencias de la Información de la Universidad del Sur de California, USA.
Servidor C: PSINet, Virginia, USA.
Servidor D: Universidad de Maryland, USA.
Servidor E: NASA, en Mountain View, California, USA.
Servidor F: Internet 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.

http://www.root-servers.org



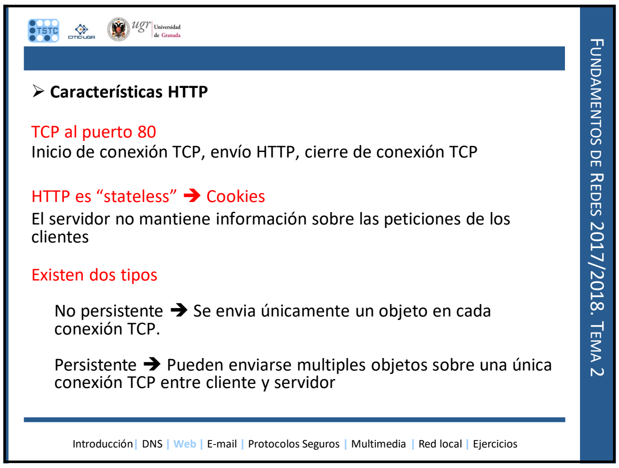
Tema 2. SERVICIOS Y PROTOCOLOS DE APLICACIÓN EN INTERNET

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



LA NAVEGACIÓN WEB

- Una página Web es un fichero (HTML) formado por objetos
  ficheros HTML, imágenes JPEG, Java applets, ficheros de audio,…
- Cada objeto se direcciona por una URL:
  http://servidor[:puerto]/path
- Protocolo HTTP
  Modelo cliente-servidor
  cliente: browser que pide, recibe y muestra objetos web
  server: envia objetos web en respuesta a peticiones



- **Características HTTP**

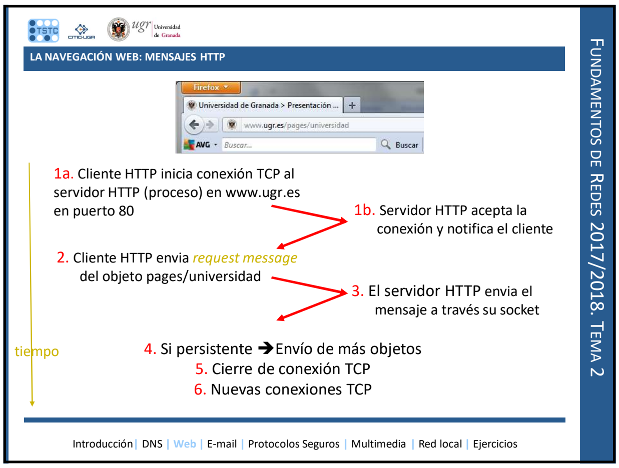
TCP al puerto 80
Inicio de conexión TCP, envío HTTP, cierre de conexión TCP

HTTP es “stateless” ➔ Cookies
El servidor no mantiene información sobre las peticiones de los clientes

Existen dos tipos

No persistente ➔ Se envia 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

Firefox
Universidad de Granada > Presentación ...
www.ugr.es/pages/universidad
AVG
Buscar...
Buscar

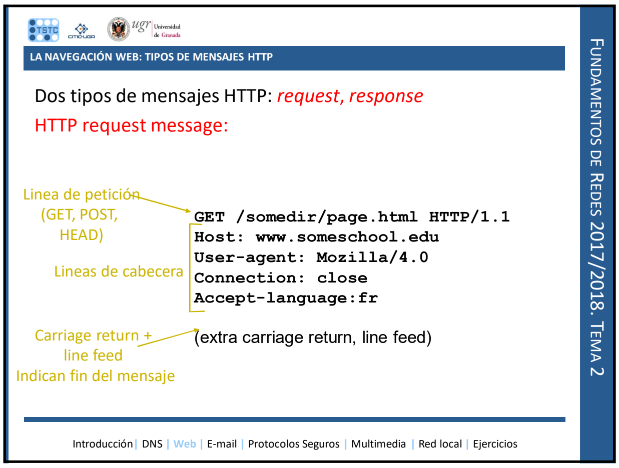
1a. Cliente HTTP inicia conexión TCP al servidor HTTP (proceso) en www.ugr.es en puerto 80

1b. Servidor HTTP acepta la conexión y notifica el cliente

2. Cliente HTTP envia *request message* del objeto pages/universidad

3. El servidor HTTP envia el mensaje a través su socket

4. Si persistente ➔Envío de más objetos
5. Cierre de conexión TCP
6. Nuevas conexiones TCP



LA NAVEGACIÓN WEB: TIPOS DE MENSAJES HTTP

Dos tipos de mensajes HTTP: *request, response*

HTTP request message:

Linea de petición (GET, POST, HEAD)

Lineas de cabecera

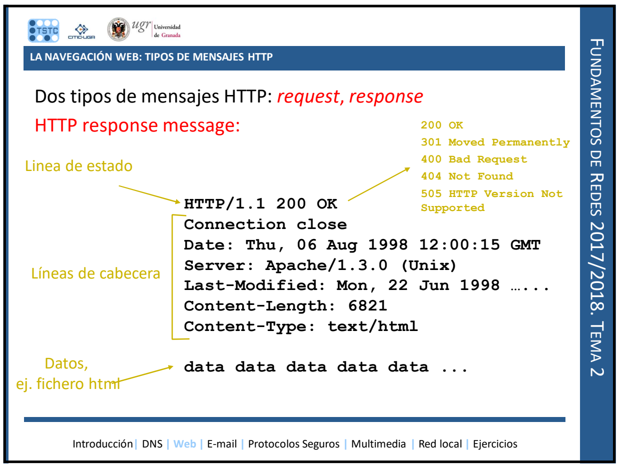
```
GET /somedir/page.html HTTP/1.1
Host: www.someschool.edu
User-agent: Mozilla/4.0
Connection: close
Accept-language:fr
```

Carriage return + line feed
Indican fin del mensaje

(extra carriage return, line feed)

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

Introducción| DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



LA NAVEGACIÓN WEB: TIPOS DE MENSAJES HTTP

Dos tipos de mensajes HTTP: *request, response*

HTTP response message:

Linea de estado

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

Líneas de cabecera

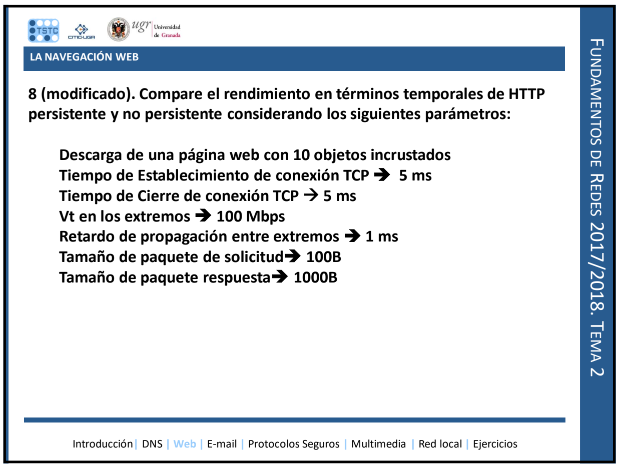
```
HTTP/1.1 200 OK
Connection close
Date: Thu, 06 Aug 1998 12:00:15 GMT
Server: Apache/1.3.0 (Unix)
Last-Modified: Mon, 22 Jun 1998 …...
Content-Length: 6821
Content-Type: text/html

data data data data data ...
```

Datos,
ej. fichero html

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

Introducción| DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



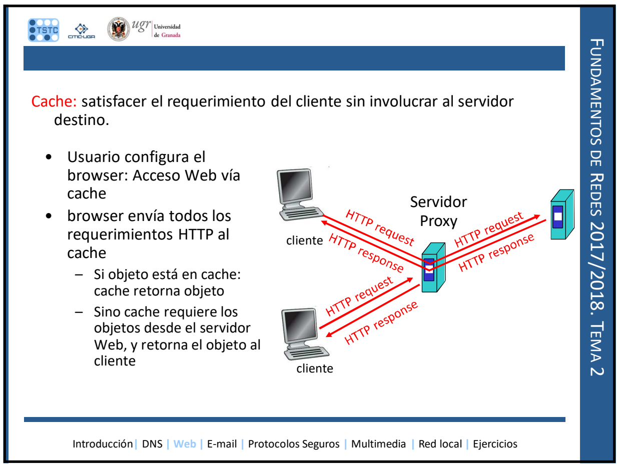
LA NAVEGACIÓN WEB

8 (modificado). 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
Vt en los extremos → 100 Mbps
Retardo de propagación entre extremos → 1 ms
Tamaño de paquete de solicitud→ 100B
Tamaño de paquete respuesta→ 1000B

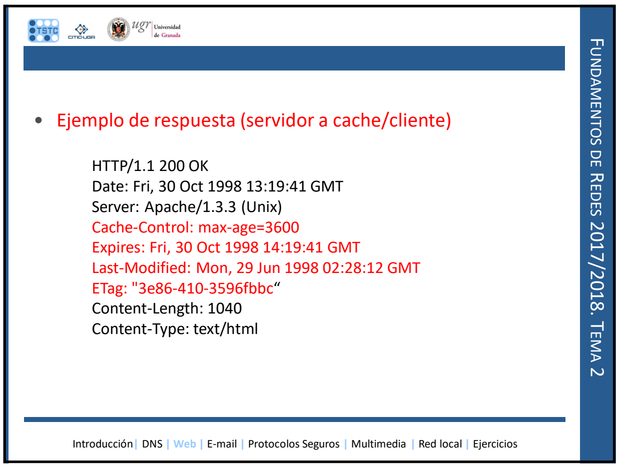
FUNDAMENTOS DE REDES 2017/2018. TEMA 2

Introducción| DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



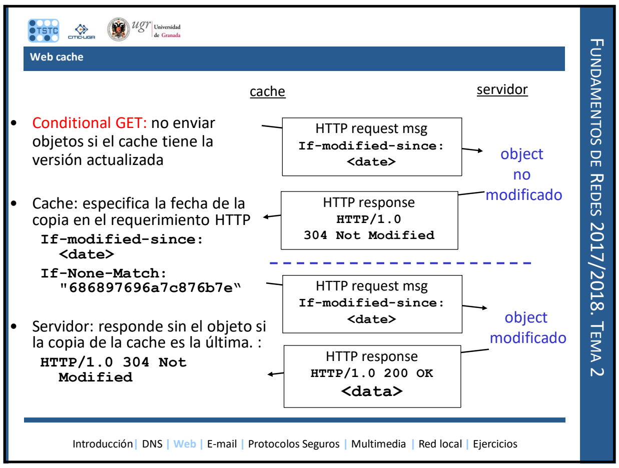
Cache: satisfacer el requerimiento del cliente sin involucrar al servidor destino.

- 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



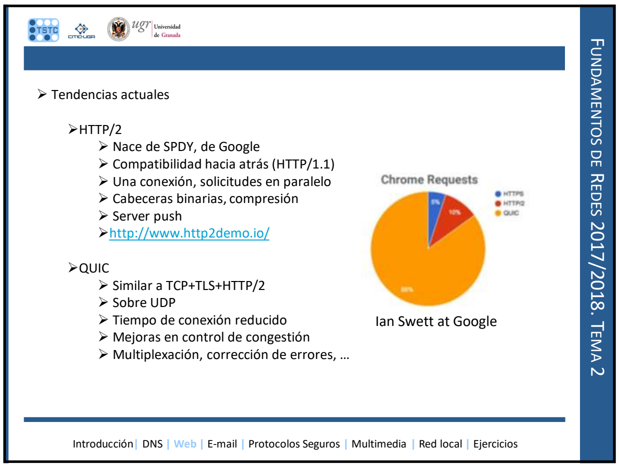
- Ejemplo de respuesta (servidor a cache/cliente)

```
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: "3e86-410-3596fbbc“
Content-Length: 1040
Content-Type: text/html
```



Web cache

- Conditional GET: 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`

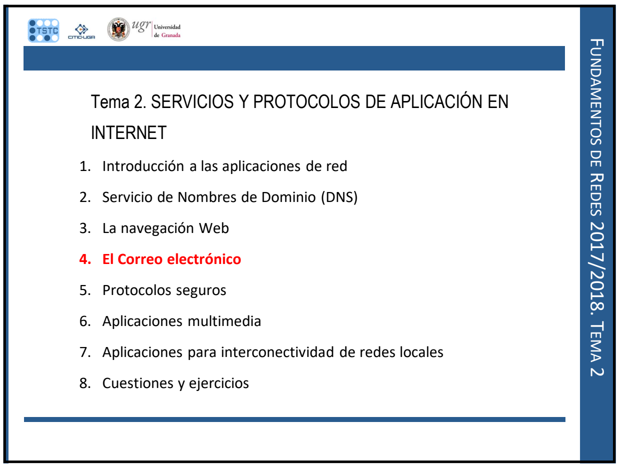


FUNDAMENTOS DE REDES 2017/2018. TEMA 2

- Tendencias actuales
  - HTTP/2
    - Nace de SPDY, de Google
    - Compatibilidad hacia atrás (HTTP/1.1)
    - Una conexión, solicitudes en paralelo
    - Cabeceras binarias, compresión
    - Server push
    - http://www.http2demo.io/
  - QUIC
    - Similar a TCP+TLS+HTTP/2
    - Sobre UDP
    - Tiempo de conexión reducido
    - Mejoras en control de congestión
    - Multiplexación, corrección de errores, …

Ian Swett at Google

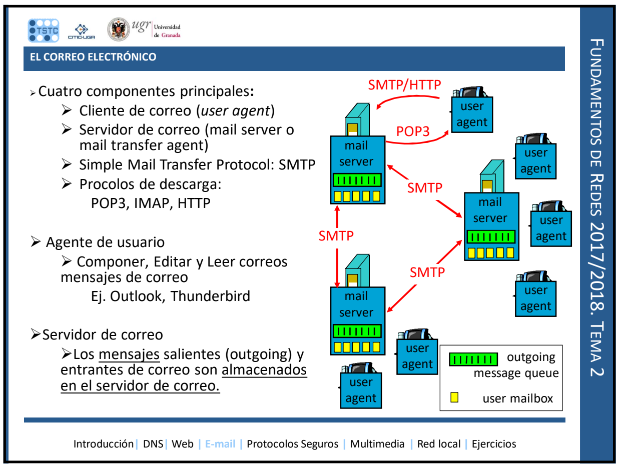
Introducción| DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



FUNDAMENTOS DE REDES 2017/2018. TEMA 2

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

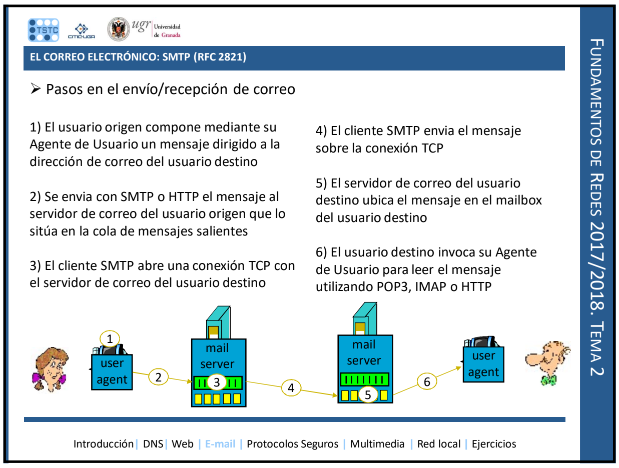


FUNDAMENTOS DE REDES 2017/2018. TEMA 2

EL CORREO ELECTRÓNICO

- Cuatro componentes principales:
  - Cliente de correo (*user agent*)
  - Servidor de correo (mail server o mail transfer agent)
  - Simple Mail Transfer Protocol: SMTP
  - Procolos de descarga: POP3, IMAP, HTTP
- Agente de usuario
  - Componer, Editar y Leer correos mensajes de correo Ej. Outlook, Thunderbird
- Servidor de correo
  - Los mensajes salientes (outgoing) y entrantes de correo son almacenados en el servidor de correo.

Introducción| DNS| Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



EL CORREO ELECTRÓNICO: SMTP (RFC 2821)

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

➢ Pasos en el envío/recepción de correo

1) El usuario origen compone mediante su Agente de Usuario un mensaje dirigido a la dirección de correo del usuario destino

2) Se envia con SMTP o HTTP el mensaje al servidor de correo del usuario origen que lo sitúa en la cola de mensajes salientes

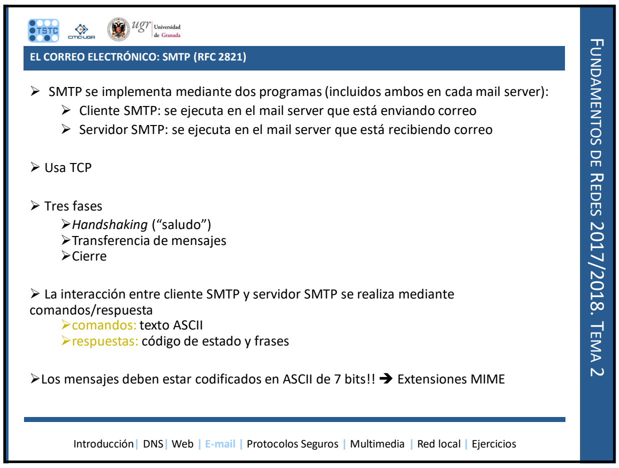
3) El cliente SMTP abre una conexión TCP con el servidor de correo del usuario destino

4) El cliente SMTP envia el mensaje sobre la conexión TCP

5) El servidor de correo del usuario destino ubica el mensaje en el mailbox del usuario destino

6) El usuario destino invoca su Agente de Usuario para leer el mensaje utilizando POP3, IMAP o HTTP

Introducción| DNS| Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



EL CORREO ELECTRÓNICO: SMTP (RFC 2821)

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

- ➢ SMTP se implementa mediante dos programas (incluidos ambos en cada mail server):
  - ➢ Cliente SMTP: se ejecuta en el mail server que está enviando correo
  - ➢ Servidor SMTP: se ejecuta en el mail server que está recibiendo correo

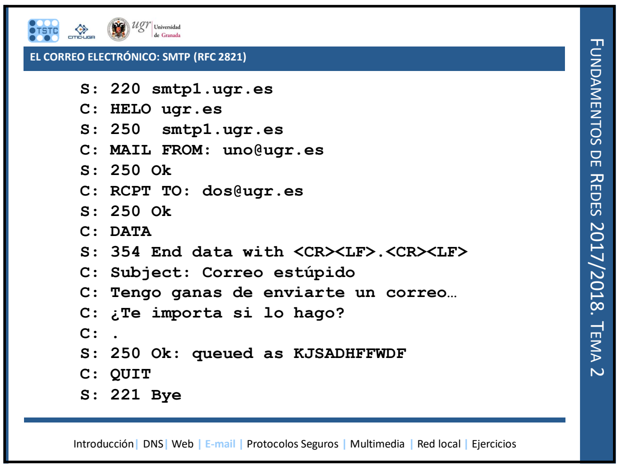
➢ Usa TCP

➢ 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

➢Los mensajes deben estar codificados en ASCII de 7 bits!! ➔ Extensiones MIME

Introducción| DNS| Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

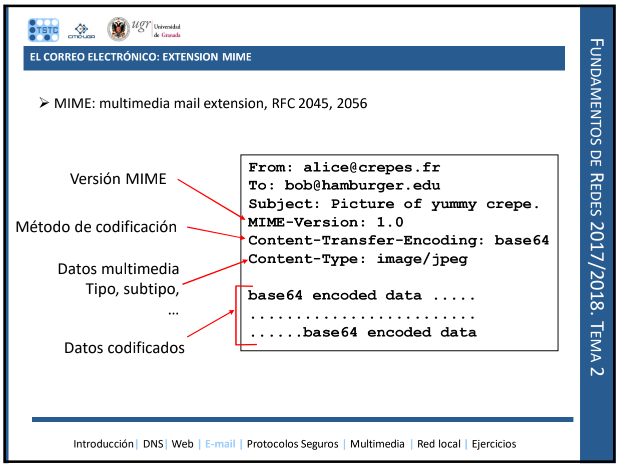


EL CORREO ELECTRÓNICO: SMTP (RFC 2821)

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

```
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
```

Introducción| DNS| Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



EL CORREO ELECTRÓNICO: EXTENSION MIME

- MIME: multimedia mail extension, RFC 2045, 2056

Versión MIME

Método de codificación

Datos multimedia
Tipo, subtipo,
...

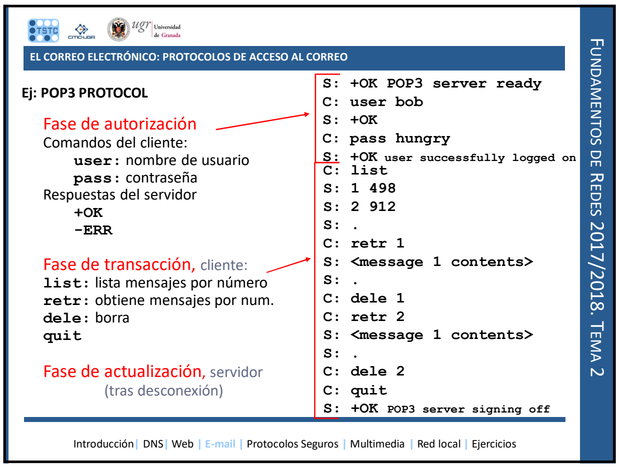
Datos codificados

```
From: alice@crepes.fr
To: bob@hamburger.edu
Subject: Picture of yummy crepe.
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Type: image/jpeg

base64 encoded data .....
.........................
......base64 encoded data
```

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

FUNDAMENTOS DE REDES 2017/2018. TEMA 2



EL CORREO ELECTRÓNICO: PROTOCOLOS DE ACCESO AL CORREO

Ej: POP3 PROTOCOL

Fase de autorización
Comandos del cliente:
user: nombre de usuario
pass: contraseña
Respuestas del servidor
+OK
-ERR

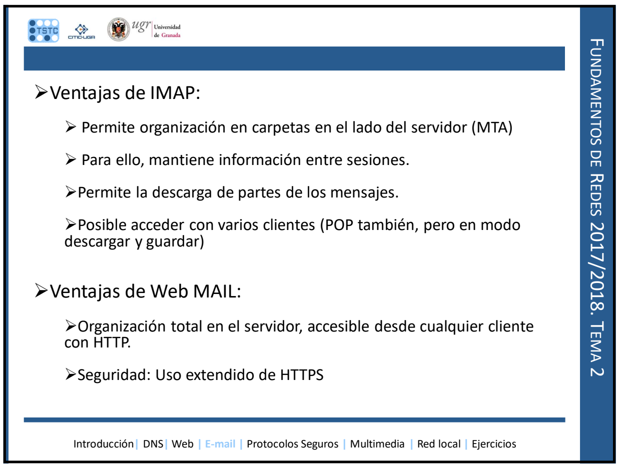
Fase de transacción, cliente:
list: lista mensajes por número
retr: obtiene mensajes por num.
dele: borra
quit

Fase de actualización, 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
```

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

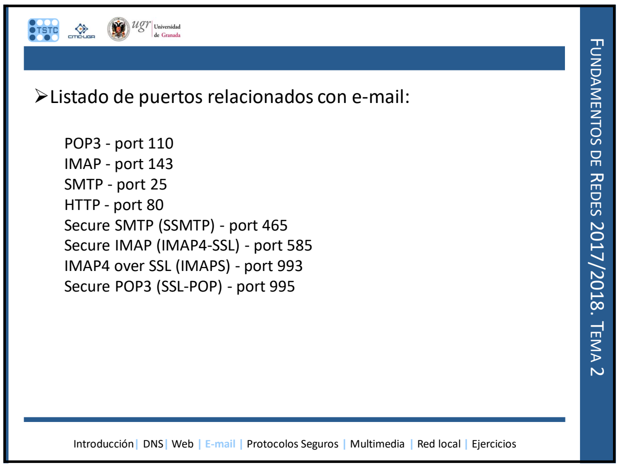
FUNDAMENTOS DE REDES 2017/2018. TEMA 2



- Ventajas de IMAP:
  - Permite organización en carpetas en el lado del servidor (MTA)
  - Para ello, mantiene información entre sesiones.
  - 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

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

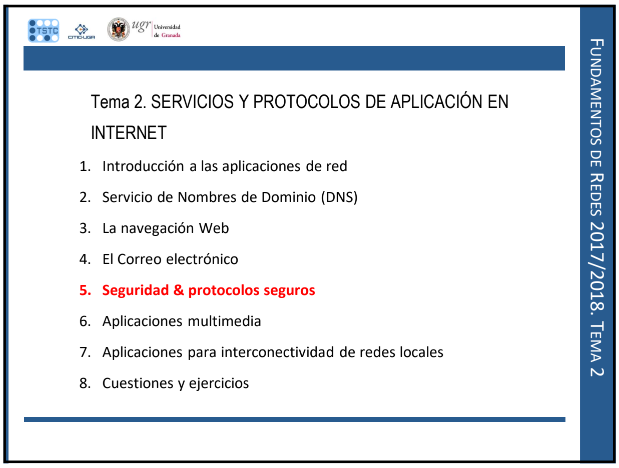


➢Listado de puertos relacionados con e-mail:

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

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

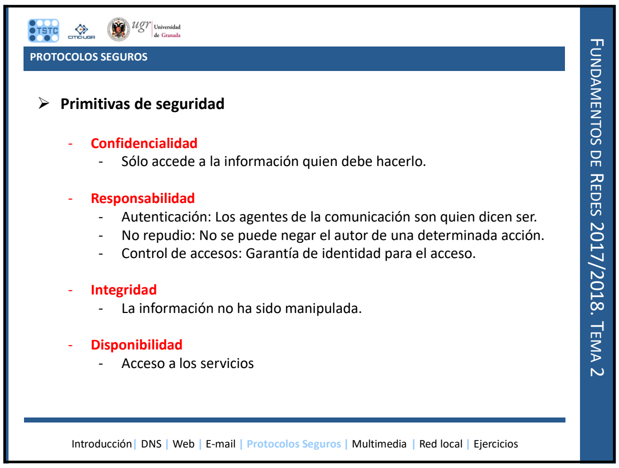
FUNDAMENTOS DE REDES 2017/2018. TEMA 2



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

FUNDAMENTOS DE REDES 2017/2018. TEMA 2



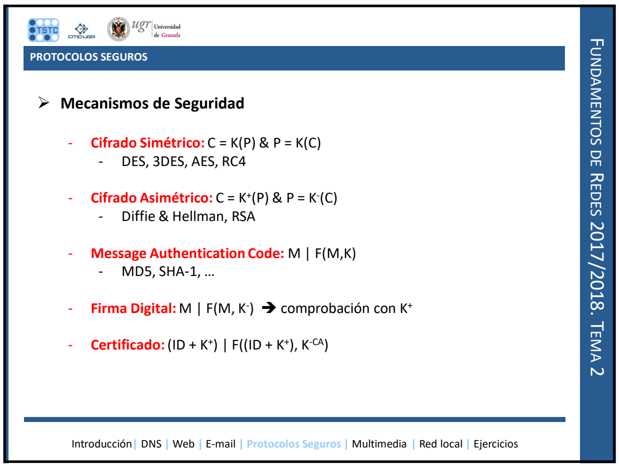
PROTOCOLOS SEGUROS

➢ **Primitivas de seguridad**

- **Confidencialidad**
  - Sólo accede a la información quien debe hacerlo.
- **Responsabilidad**
  - Autenticación: Los agentes de la comunicación 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**
  - La información no ha sido manipulada.
- **Disponibilidad**
  - Acceso a los servicios

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

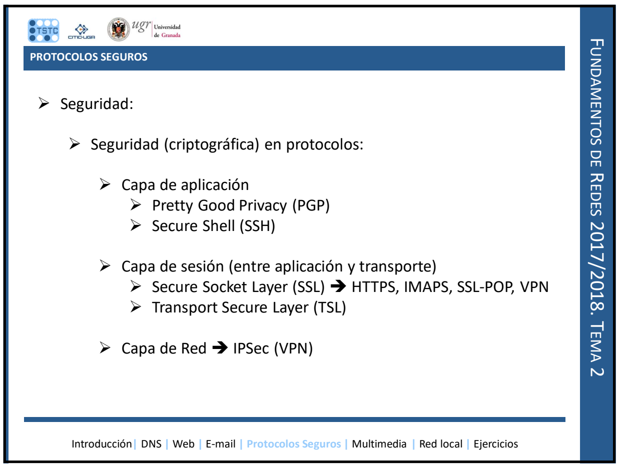


PROTOCOLOS SEGUROS

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

- **Mecanismos de Seguridad**
  - **Cifrado Simétrico:** C = K(P) & P = K(C)
    - DES, 3DES, AES, RC4
  - **Cifrado Asimétrico:** C = $K^+(P)$ & P = $K^-(C)$
    - Diffie & Hellman, RSA
  - **Message Authentication Code:** M | F(M,K)
    - MD5, SHA-1, …
  - **Firma Digital:** M | F(M, K^-) ➔ comprobación con K^+
  - **Certificado:** (ID + K^+) | F((ID + K^+), K^{-CA})

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

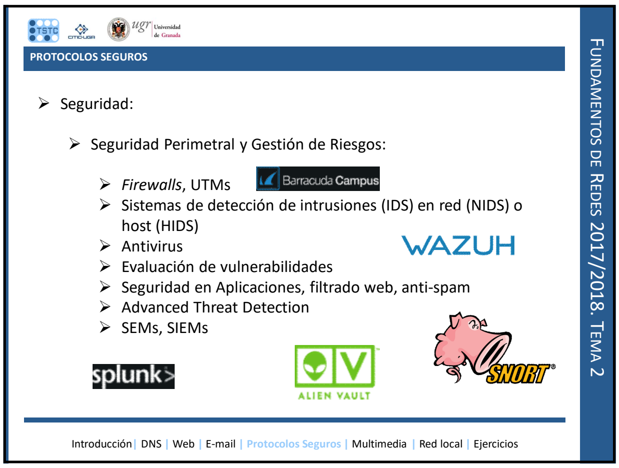


PROTOCOLOS SEGUROS

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

- Seguridad:
  - Seguridad (criptográfica) en protocolos:
    - Capa de aplicación
      - Pretty Good Privacy (PGP)
      - Secure Shell (SSH)
    - Capa de sesión (entre aplicación y transporte)
      - Secure Socket Layer (SSL) ➔ HTTPS, IMAPS, SSL-POP, VPN
      - Transport Secure Layer (TSL)
    - Capa de Red ➔ IPSec (VPN)

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios



PROTOCOLOS SEGUROS

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

- Seguridad:
  - Seguridad Perimetral y Gestión de Riesgos:
    - *Firewalls*, UTMs
    - Sistemas de detección de intrusiones (IDS) en red (NIDS) o host (HIDS)
    - Antivirus
    - Evaluación de vulnerabilidades
    - Seguridad en Aplicaciones, filtrado web, anti-spam
    - Advanced Threat Detection
    - SEMs, SIEMs

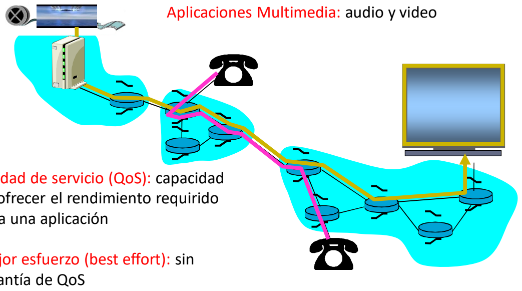
Barracuda Campus
WAZUH
SNORT
splunk>
ALIEN VAULT

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

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

- Conceptos

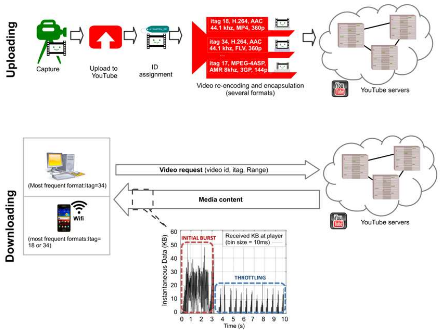


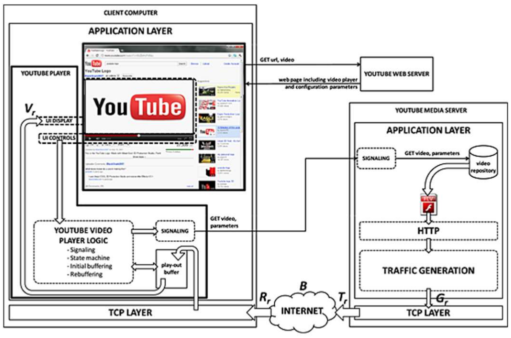
Aplicaciones Multimedia: audio y video

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

Mejor esfuerzo (best effort): sin garantía de QoS

- **Tipos de aplicaciones**
  - Flujo de audio y video (streaming) almacenado ➔ Ej YouTube
  - Flujo de audio y video en vivo ➔ Ej. emisoras de radio o IPTV
  - Audio y vídeo interactivo ➔ Ej. Skype
- **Características fundamentales**
  - Elevado ancho de banda
  - Tolerantes a la pérdida de datos
  - Delay acotado
  - Jitter acotado
  - Uso de multicast

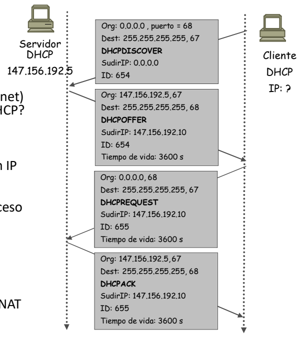

Uploading
Capture
Upload to YouTube
ID assignment
itag 18, H.264, AAC 44.1 khz, MP4, 360p
itag 34, H.264, AAC 44.1 khz, FLV, 360p
...
itag 17, MPEG-4ASP, AMR 8khz, 3GP, 144p
Video re-encoding and encapsulation (several formats)
YouTube servers
Downloading
(Most frequent format:Itag=34)
Wifi
(most frequent formats:Itag= 18 or 34)
Video request (video id, itag, Range)
Media content
YouTube servers
INITIAL BURST
Received KB at player (bin size = 10ms)
THROTTLING
Instantaneous Data (KB)
0
10
20
30
40
50
60
0 1 2 3 4 5 6 7 8 9 10
Time (s)



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

- DHCP
  - Configuración dinámica de direcciones IP
  - ¿Dónde (en qué parte de Internet) se suele utilizar un servidor DHCP?
- DynDNS, No-IP, …
  - Servicios en la red privada, con IP pública variable
  - Configuración en router de acceso necesaria
- UPnP
  - "Pervasive adhoc com."
  - Comunicación Dispositivo <-> NAT



Org: 0.0.0.0 , puerto = 68
Dest: 255.255.255.255, 67
DHCPDISCOVER
SudirIP: 0.0.0.0
ID: 654

Org: 147.156.192.5,67
Dest: 255.255.255.255, 68
DHCPOFFER
SudirIP: 147.156.192.10
ID: 654
Tiempo de vida: 3600 s

Org: 0.0.0.0, 68
Dest: 255.255.255.255, 67
DHCPREQUEST
SudirIP: 147.156.192.10
ID: 655
Tiempo de vida: 3600 s

Org: 147.156.192.5,67
Dest: 255.255.255.255, 68
DHCPACK
SudirIP: 147.156.192.10
ID: 655
Tiempo de vida: 3600 s

Introducción | DNS | Web | E-mail | Protocolos Seguros | Multimedia | Red local | Ejercicios

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

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**

FUNDAMENTOS DE REDES 2017/2018. TEMA 2

TEMA 2
SERVICIOS Y PROTOCOLOS DE APLICACIÓN EN INTERNET

Fundamentos de Redes
2017/2018

FUNDAMENTOS DE REDES 2017/2018. TEMA 2