

HTTP

Redes de Ordenadores para Robots y Máquinas Inteligentes

GSyC

Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Febrero de 2023



©2023 Grupo de Sistemas y Comunicaciones.
Algunos derechos reservados.
Este trabajo se distribuye bajo la licencia
Creative Commons Attribution Share-Alike 4.0
disponible en <http://creativecommons.org/licenses/by-sa/4.0/deed.es>

Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP
- 4 Caché de contenidos en HTTP
- 5 Cookies
- 6 HTTPS
- 7 HTTP 2.0 y 3.0
- 8 Referencias

Contenidos

- 1 **Introducción**
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP
- 4 Caché de contenidos en HTTP
- 5 Cookies
- 6 HTTPS
- 7 HTTP 2.0 y 3.0
- 8 Referencias

Definiciones

URL (*Universal Resource Locator*)

Interfaz común para acceder a diferentes tipos de servicios/documentos en Internet a través de un sistema de nombres.

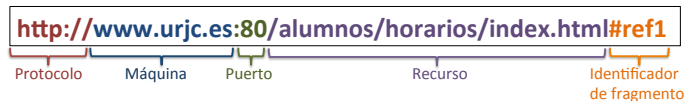
HTML (*HyperText Markup Language*)

Lenguaje de marcado para la elaboración de contenidos integrados por texto, gráficos, etc, que permite incluir en un documento referencias a otros recursos mediante URLs

HTTP (*HyperText Transfer Protocol*)

Protocolo entre navegadores y servidores WWW para transferir recursos hipermedia (texto, gráficos, audio, vídeo).

URL



- **Protocolo**: Protocolo por el que se accede al recurso. Por defecto el predeterminado para la aplicación que usa la URL.
- **Máquina**: Máquina en la que reside el recurso. Por defecto la máquina local.
- **Puerto**: Puerto de la máquina a través del que se pide el recurso. Por defecto el predeterminado para el protocolo (`http=80`)
- **Recurso**: Identificación del recurso dentro de la máquina, incluyendo (a veces) un *path*. Por defecto el recurso predeterminado para la máquina.
- **Identificador de fragmento**: Opcionalmente, se utiliza para identificar un fragmento del recurso.


HTML

```
<!DOCTYPE html>
<html>
<head>
<title>Mi primera página HTML</title> </head>
<body>
<h1>Primer Título</h1>
<p>
<a href="http://www.w3schools.com">Esto es un enlace</a> </p>
<h2>Primer Subtítulo</h2>
<p>
<!-- Esto es un comentario -->
Una imagen:
 </p>
<p>
<!-- Imagen con URL completa por si viene de otro directorio y/o servidor -->
 </p>
<p>
Si en una URL no se especifica servidor, se entiende que es el mismo. Idem para el directorio</p>
</body>
</html>
```

Primer Título

[Esto es un enlace](#)

Primer Subtítulo

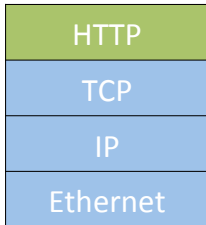
Una imagen: 



Si en una URL no se especifica servidor, se entiende que es el mismo. Idem para el directorio

HTTP

- Protocolo de nivel de aplicación utilizado para transferir recursos hipermedia entre ordenadores.
- Sigue el **modelo Cliente-Servidor**:
 - **Cliente HTTP**: navegador web que pide páginas y, al recibirlas, las muestra al usuario. Ej: Firefox, Explorer, Chrome, Safari...
 - **Servidor HTTP**: servidor web en el que están alojadas páginas que piden los clientes. Ej: Apache, IIS...
- Funciona sobre TCP como protocolo de transporte
- Por defecto un servidor HTTP escucha en el puerto 80, pero puede usar cualquier otro puerto.
- HTTP puede servir tanto **contenido estático** (ficheros) como **contenido dinámico** (el resultado de ejecutar programas en el servidor).



Versiones de HTTP

- **0.9**: Primera versión documentada, no tiene número de versión oficial, pero es referida como versión 0.9 (1991)
- **1.0**: Primera versión oficial (RFC 1945, año 1996)
- **1.1**: Versión “clásica” (RFC 2068, año 1997 y RFC 2616, año 1999)
- **2.0**: Versión “nueva” (RFC 7540, junio 2015)
 - Soportado en las versiones actuales de todos los navegadores
 - Utilizado en el 39 % de los sitios web (según W³Tech).
- **3.0**: Versión en proceso de estandarización, RFC 9114.
Utilizado hoy en día en un 25 % de los sitios web.

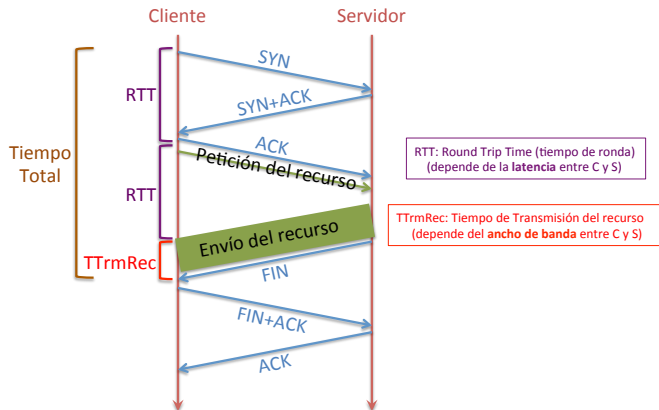
Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP
- 4 Caché de contenidos en HTTP
- 5 Cookies
- 6 HTTPS
- 7 HTTP 2.0 y 3.0
- 8 Referencias

Páginas web

- Una **página web** se compone de uno o más **recursos**.
- Cada recurso suele ser un archivo, y hay recursos de distinto tipo (archivos HTML, imágenes PNG, vídeos AVI, applets Java, etc)
- A un recurso se hace referencia a través de su URL.
- La mayoría de las páginas web están formadas por **un recurso principal y varios recursos referenciados en él** como contenido que forma parte de la misma página.
 - Ej: Una página web puede estar compuesta por 6 recursos: 1 fichero HTML y 5 imágenes PNG.

Petición de una página web de un solo recurso



- El tiempo total mide lo que se tarda en tener el recurso en el cliente (para mostrarlo), por lo que el tiempo de cerrar la conexión no cuenta.

Páginas web con varios recursos

- Normalmente una página web está compuesta por varios recursos alojados en diferentes servidores.
- Tras obtenerse el recurso principal, de él se extrae la relación de recursos adicionales que forman parte de la misma página:
 - Para cada nuevo servidor, se abrirá una conexión TCP nueva para pedirle sus recursos.
 - Si hay varios recursos en un mismo servidor, suelen solicitarse todos ellos a través de la misma conexión TCP.

Valores típicos en una aplicación web hoy

Carga de la página principal de una aplicación web:

- 90 solicitudes de HTTP, obtenidas de 15 servidores, 1300 KB transferidos, 3 segundos:
 - HTML: 10 solicitudes, 52 KB
 - Imágenes: 55 solicitudes, 812 KB
 - JavaScript: 15 solicitudes, 216 KB
 - CSS: 5 solicitudes, 36 KB
 - Otros: 5 solicitudes, 195 KB

Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP**
- 4 Caché de contenidos en HTTP
- 5 Cookies
- 6 HTTPS
- 7 HTTP 2.0 y 3.0
- 8 Referencias

- ### Línea inicial

[illegible]

Líneas de cabecera

Línea en blanco

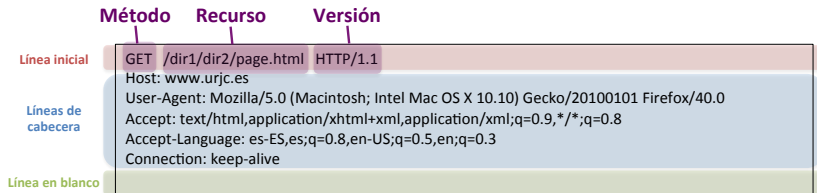
[illegible]

Cuerpo
(opcional)

Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP**
 - Petición HTTP
 - Respuesta HTTP
 - Líneas de cabecera en petición/respuesta HTTP
 - GET y POST para envío de datos al servidor
- 4 Caché de contenidos en HTTP
 - Cache-Control y ETag en HTTP/1.1
 - Uso de Cache-Control en una petición
- 5 Cookies
- 6 HTTPS
- 7 HTTP 2.0 y 3.0
- 8 Referencias

Formato peticiones



- La especificación del recurso incluye la ruta (*path*), pero no el nombre de máquina.
- La versión del protocolo indica la versión de HTTP bajo la que se hace la petición.
- Las peticiones normalmente no llevan cuerpo (aunque, a veces, sí).

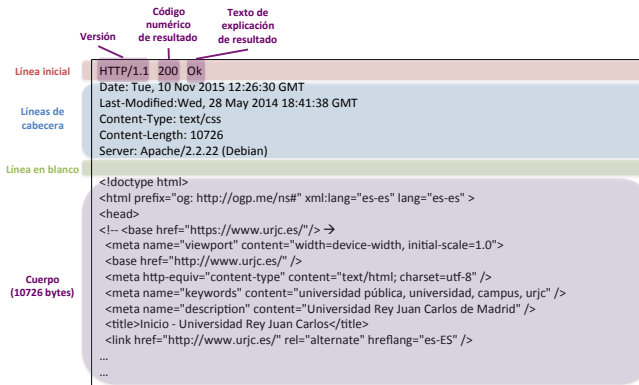
Métodos de las peticiones

- **GET:**
 - Solicita un recurso, la petición no lleva cuerpo. El recurso solicitado se indica en la línea inicial.
 - Ejemplo: solicitar una página web.
- **POST:**
 - Envía datos a un recurso del servidor. El recurso se indica en la línea inicial y los datos van en el cuerpo de la petición.
 - Ejemplo: enviar los datos que rellena el usuario a través de un formulario web.
- **PUT:**
 - Actualiza un recurso existente en el servidor (“actualiza” una página web).
 - Hoy no se usa para este fin, pues las páginas WWW se colocan en los servidores por mecanismos externos a HTTP.
- **DELETE:**
 - Elimina en el servidor el recurso especificado.
 - También en desuso para este fin.
- ...

Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP**
 - Petición HTTP
 - **Respuesta HTTP**
 - Líneas de cabecera en petición/respuesta HTTP
 - GET y POST para envío de datos al servidor
- 4 Caché de contenidos en HTTP
 - Cache-Control y ETag en HTTP/1.1
 - Uso de Cache-Control en una petición
- 5 Cookies
- 6 HTTPS
- 7 HTTP 2.0 y 3.0
- 8 Referencias

Formato respuestas



- La versión del protocolo indica la mayor versión que entiende el servidor, pero siempre se responde atendiendo a la versión de la petición recibida.
- Las respuestas normalmente sí llevan cuerpo: el recurso solicitado. Las cabeceras **Content-Length** y **Content-Type** son necesarias en este caso.

Respuestas: Resultado

- Códigos de estado del resultado en los mensajes de respuesta:
 - 1xx: Mensaje informativo
 - 2xx: Resultado con éxito
 - 200 OK
 - 3xx: Redirección del cliente a otra URL
 - 301 Moved permanently
 - 304 Not Modified
 - 4xx: Error en el lado del cliente
 - 404 Not Found
 - 5xx: Error en el lado del servidor
 - 500 Internal Server Error

Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP**
 - Petición HTTP
 - Respuesta HTTP
 - **Líneas de cabecera en petición/respuesta HTTP**
 - GET y POST para envío de datos al servidor
- 4 Caché de contenidos en HTTP
 - Cache-Control y ETag en HTTP/1.1
 - Uso de Cache-Control en una petición
- 5 Cookies
- 6 HTTPS
- 7 HTTP 2.0 y 3.0
- 8 Referencias

Líneas de cabecera

- Mismo formato que las cabeceras del formato de los correos electrónicos (RFC 822, sección 3).
- En HTTP/1.0 se definen 16 cabeceras, ninguna obligatoria.
- En HTTP/1.1 se definen 46 cabeceras, **siendo obligatoria en las peticiones la cabecera Host**: nombre del servidor del recurso

Host: www.urjc.es

- Se recomienda incluir en las peticiones al menos:

- **User-Agent**: tipo de navegador

User-Agent: Mozilla/5.0

- Se recomienda incluir en las respuestas al menos:

- **Server**: tipo de servidor

Server: Apache/1.3

- **Last-Modified**: fecha de última modificación del recurso

Last-Modified: Wed, 28 May 2014 18:41:38 GMT

- Si un mensaje tiene cuerpo, es obligatorio que se incluyan las cabeceras:

- **Content-Type**: tipo MIME de lo que va en el cuerpo

Content-Type: text/html

- **Content-Length**: tamaño en bytes del cuerpo

Content-Length: 10726

Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP**
 - Petición HTTP
 - Respuesta HTTP
 - Líneas de cabecera en petición/respuesta HTTP
 - **GET y POST para envío de datos al servidor**
- 4 Caché de contenidos en HTTP
 - Cache-Control y ETag en HTTP/1.1
 - Uso de Cache-Control en una petición
- 5 Cookies
- 6 HTTPS
- 7 HTTP 2.0 y 3.0
- 8 Referencias

Uso de GET y POST para envío de datos al servidor

- Los formularios se utilizan para enviar datos desde el navegador al servidor:

Nombre:

Edad:

- **POST:**

- Envía datos al servidor, normalmente los introducidos por el usuario en un formulario.
- **Los datos van en el cuerpo.**
- El *path* de la línea inicial (URL) se refiere normalmente al programa que tratará los datos que se envían.

- **GET:**

- GET también permite enviar los datos de un formulario. En este caso, **los datos van en el path de la línea inicial (URL), y no hay cuerpo.**
- El tamaño de los datos subidos con GET está limitado por el tamaño máximo de una URL (255 caracteres), por lo que NO se utiliza GET para subir datos de formularios grandes.

Ejemplo de formularios HTML

- Código HTML de un formulario que enviará los datos mediante GET:

```
<FORM action="http://pc2.emp2.net/form.php" method=GET>
  <P>
    Nombre: <INPUT type="text" name="nombre"><BR>
    Edad: <INPUT type="text" name="edad"><BR>
    <INPUT type="submit" value="Enviar"><INPUT type="reset">
  </P>
</FORM>
```

- Código HTML de un formulario que enviará los datos mediante POST:

```
<FORM action="http://pc2.emp2.net/form.php" method=POST>
  <P>
    Nombre: <INPUT type="text" name="nombre"><BR>
    Edad: <INPUT type="text" name="edad"><BR>
    <INPUT type="submit" value="Enviar"><INPUT type="reset">
  </P>
</FORM>
```

Ejemplo de envío de datos con GET y POST

- Cuando el usuario rellene los datos y pulse sobre el botón "Enviar", el navegador mandará un mensaje con los datos al servidor.

```
GET /form.php?nombre=Fulano+Mengano&edad=24 HTTP/1.0
Host: pc2.emp2.net
User-Agent: Mozilla/4.5 [en]
Accept: image/jpeg, image/gif, text/html
Accept-language: en
Accept-Charset: iso-8859-1
```

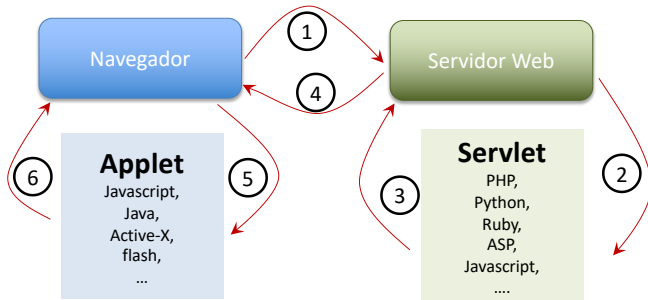
```
POST /form.php HTTP/1.0
Host: pc2.emp2.net
User-Agent: Mozilla/4.5 [en]
Accept: image/jpeg, image/gif, text/html
Accept-language: en
Accept-Charset: iso-8859-1
Content-Type: application/x-www-form-urlencoded
Content-Length: 26

nombre=Perico+Palotes&edad=24
```

- ?: separación entre el recurso y los parámetros
- =: separación entre nombre del campo del formulario y su valor
- &: separación entre parámetros
- +: espacio en blanco

Páginas web dinámicas. Aplicaciones web

- El protocolo HTTP se diseña pensando (básicamente) en transmitir ficheros (estáticos)
- El término **Aplicación Web** empieza a utilizarse cuando la petición de un recurso vía HTTP involucra la ejecución de uno o más programas, bien en el cliente o bien en el servidor



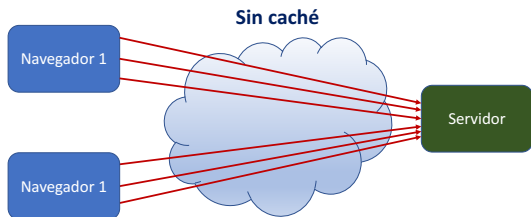
Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP
- 4 Caché de contenidos en HTTP**
- 5 Cookies
- 6 HTTPS
- 7 HTTP 2.0 y 3.0
- 8 Referencias

Cachés en HTTP

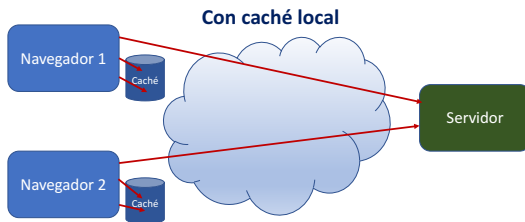
Objetivo

Minimizar las transferencias vía HTTP de recursos que no han cambiado.



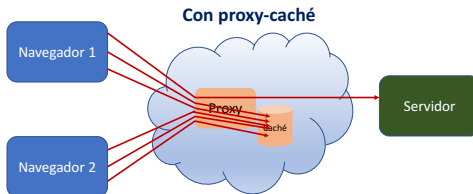
- Cuando no se utilizan cachés:
 - si un mismo cliente pide varias veces un mismo recurso que no ha cambiado, todas las veces se transfiere su contenido.
 - si varios clientes piden el mismo recurso que no ha cambiado, todas las veces se transfiere su contenido.

Caché local (privada)



- Cada navegador mantiene una **caché local (privada)**, para cada usuario):
 - la primera vez que se pide un recurso, se almacena en la caché
 - las siguientes veces el recurso puede obtenerse de la caché sin volver a transferirlo desde el servidor.

Caché global: Proxy-caché



- Los navegadores pueden estar configurados para realizar las peticiones HTTP a través de una máquina intermedia, el **proxy-caché**. Los clientes no se comunican directamente con los servidores que tienen los recursos, es el proxy-caché el que hace de intermediario y se comunica por una parte con los clientes y por otra con los servidores finales.
- Las peticiones a un proxy se distinguen porque incluyen la URL completa en la primera línea del mensaje de petición. Ejemplo:

```
GET http://gsyc.escet.urjc.es/index.html HTTP/1.0
```
- Las peticiones y respuestas que envía un proxy incluyen la línea de cabecera **Via**. Ejemplo:

```
Via: 1.0 myproxy.com
```
- Un proxy HTTP casi siempre tiene asociada una **caché global** (llamada **pública** pues se comparte entre distintos usuarios):
 - la primera vez que un cliente pide al Proxy un recurso, se almacena en la caché
 - las siguientes veces el recurso puede obtenerse de la caché sin volver a transferirlo desde el servidor.

Funcionamiento general de las cachés

- Un servidor puede controlar si se puede o no almacenar cada recurso que envía, y durante cuánto tiempo, para según qué **tipo de caché** (privada o pública).
- Un recurso cacheado tiene un **tiempo de vigencia**, durante el cuál el recurso es servido directamente de la caché sin consultar al servidor que originalmente lo envió.
- Un recurso **caducado** provoca que quien lo tiene intente **revalidarlo**, es decir, comprobar si su contenido ha cambiado en el servidor original:
 - si NO hubiera cambiado, NO se vuelve a transferir, se sirve desde la caché, y se define un nuevo tiempo de vigencia
 - si SÍ hubiera cambiado, SÍ se vuelve a transferir, y si el nuevo contenido puede volver a cachearse, se definirá un nuevo tiempo de vigencia.
- Bajo determinadas circunstancias (ej: desconexión de la red), se puede servir contenidos caducados desde una caché, es decir, sin revalidar.

Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP
 - Petición HTTP
 - Respuesta HTTP
 - Líneas de cabecera en petición/respuesta HTTP
 - GET y POST para envío de datos al servidor
- 4 Caché de contenidos en HTTP**
 - **Cache-Control y ETag en HTTP/1.1**
 - Uso de Cache-Control en una petición
- 5 Cookies
- 6 HTTPS
- 7 HTTP 2.0 y 3.0
- 8 Referencias

Cabecera **Cache-Control** en respuestas

- Introducida en HTTP 1.1.
- Enviada por los servidores en las respuestas para controlar si un recurso puede cachearse o no, cómo y cuánto tiempo.
- Principales valores (pueden concatenarse varios):
 - **no-store**: el recurso no puede almacenarse
 - **no-cache**: si el recurso se almacenara, no podría servirse desde la caché sin revalidarlo previamente
 - **must-revalidate**: cuando el recurso caduque, es obligatorio revalidarlo (es decir, no puede servirse caducado en ninguna circunstancia)
 - **public**: el recurso puede ser almacenado en cachés de cualquier tipo
 - **private**: el recurso sólo puede ser almacenado en cachés privadas
 - **max-age=X**: número X de segundos que el recurso tiene de vigencia
- Ejemplos:

```
Cache-Control: no-cache, must-revalidate
```

```
Cache-Control: max-age=86400
```

```
Cache-Control: private, max-age=600
```

Cabecera ETag

- Introducida en HTTP 1.1.
- Identifica de manera única un recurso para su posterior validación.
- Lo genera el servidor cuando envía la respuesta con el recurso solicitado. No se especifica la forma de generar estos identificadores, pero típicamente serán un *hash* del recurso.

ETag: "33a64df551425fcc55d9f25f89d4"

- **El ETag se utilizará para revalidar un recurso caducado.** El cliente solicitará el recurso y usará la cabecera **If-None-Match** cuyo valor contendrá el ETag de dicho recurso (que recibió previamente y desea saber si se ha modificado):

If-None-Match: "33a64df551425fcc55d9f25f89d4"

- En el servidor se comprobará el valor recibido en la cabecera If-None-Match:
 - Si el recurso ha cambiado tendrá un valor diferente ETag y por tanto no coincidirá con el enviado en la cabecera If-None-Match. El servidor enviará de nuevo el recurso.
 - Si el recurso no ha cambiado, el ETag enviado para revalidar será el mismo que el almacenado en el servidor y por tanto, el servidor no necesita enviar de nuevo el recurso.
- La validación con ETag se consiera **validación fuerte**.

Ejemplo

- Respuesta de un servidor a un recurso:

```
HTTP/1.1 200 OK
Date: Mon, 3 Apr 2017 13:19:41 GMT
Server: Apache/1.3.3 (Unix)
Cache-Control: max-age=3600, must-revalidate
ETag: "3e86-410-3596fbbc"
Content-Length: 1040
Content-Type: text/html
```

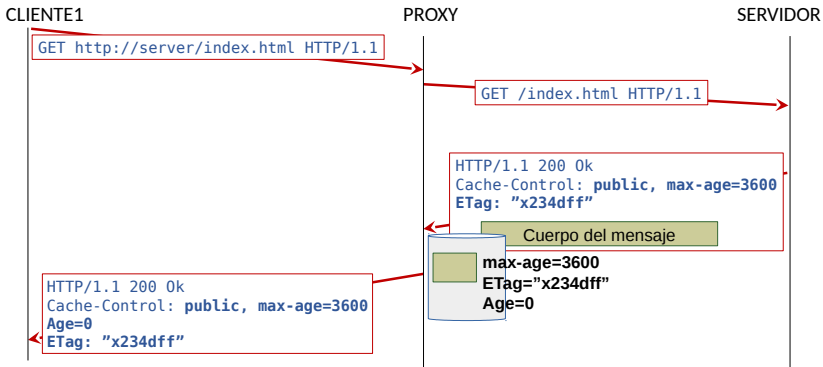
- Significado:
 - **Cache-Control**: puede cachearse, vigencia de 1 hora, no puede devolverse sin revalidar (cuando caduque).
 - **ETag** para validación
- Mientras no caduque (durante 1 hora), se servirá de la caché.
- El valor por defecto para Cache-Control es **private**, por tanto, solo puede ser almacenada en una caché privada.
- Tras caducar, el cliente tendrá que revalidar el recurso utilizando la cabecera If-None-Match.

Respuestas servidas por un Proxy desde su caché

- La respuesta incluye la cabecera `Age`, que indica el tiempo en segundos de vigencia ya consumido por el recurso desde que está en la caché (o ha sido revalidado):
`Age: 20`
- Si tiene valor 0 indica que el recurso está recién obtenido.

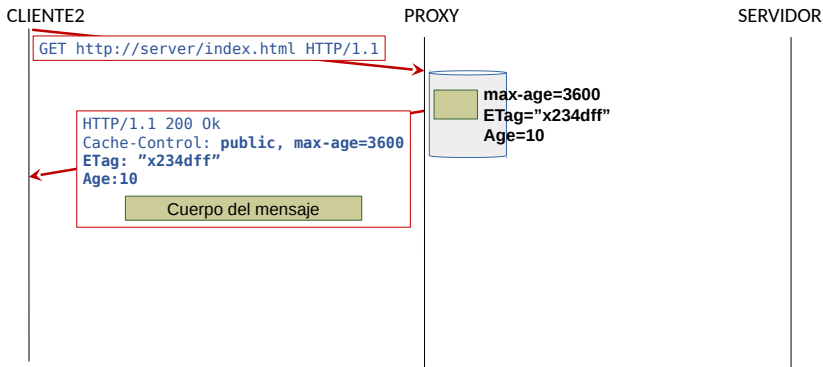
Caché pública: cabeceras Cache-Control y ETag (I)

- El cliente1 solicita recurso a un servidor a través de un proxy que no lo tiene en su caché.



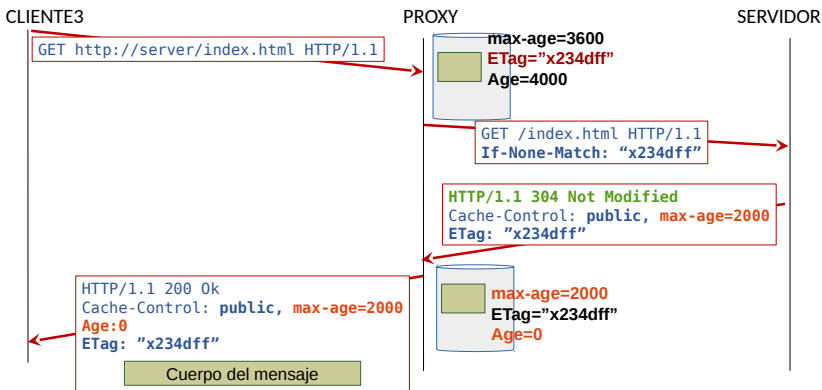
Caché pública: cabeceras Cache-Control y ETag (II)

- El cliente2 solicita recurso a un servidor a través de un proxy que lo tiene vigente en su caché.



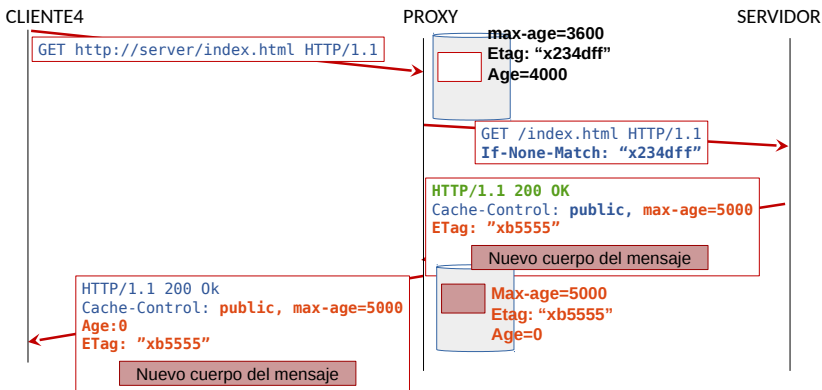
Caché pública: cabeceras Cache-Control y ETag (III)

- El cliente3 solicita recurso a un servidor a través de un proxy que lo tiene caducado en su caché y tiene que revalidarlo. El recurso no ha cambiado.



Caché pública: cabeceras Cache-Control y ETag (IV)

- El cliente4 solicita recurso a un servidor a través de un proxy que lo tiene caducado en su caché y tiene que revalidarlo. **El recurso ha cambiado.**



Caché privada: cabeceras Cache-Control y ETag (IV)

- Los ejemplos de caché pública y cabeceras Cache-Control y Etag pueden aplicarse también a las cachés privadas.
- Con las cachés privadas es el propio navegador (cliente) el que almacena los recursos y comprueba su tiempo de vigencia para solicitar la revalidación al servidor.
- En entornos reales se producen situaciones que combinan tanto la caché privada del navegador como cachés públicas (pueden encadenarse proxys HTTP).

Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP
 - Petición HTTP
 - Respuesta HTTP
 - Líneas de cabecera en petición/respuesta HTTP
 - GET y POST para envío de datos al servidor
- 4 Caché de contenidos en HTTP**
 - Cache-Control y ETag en HTTP/1.1
 - **Uso de Cache-Control en una petición**
- 5 Cookies
- 6 HTTPS
- 7 HTTP 2.0 y 3.0
- 8 Referencias

Cabecera `Cache-Control` en las peticiones

- La cabecera `Cache-Control` puede incluirse en las peticiones.
- Principales valores (pueden concatenarse varios):
 - `no-cache`: el recurso no puede provenir de una caché sin haber sido revalidado
 - `no-store`: quien reciba la petición no puede almacenar la respuesta
 - `max-age=X`: el cliente sólo quiere una respuesta cacheada si su `Age` es menor o igual que X segundos.

Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP
- 4 Caché de contenidos en HTTP
- 5 Cookies**
- 6 HTTPS
- 7 HTTP 2.0 y 3.0
- 8 Referencias

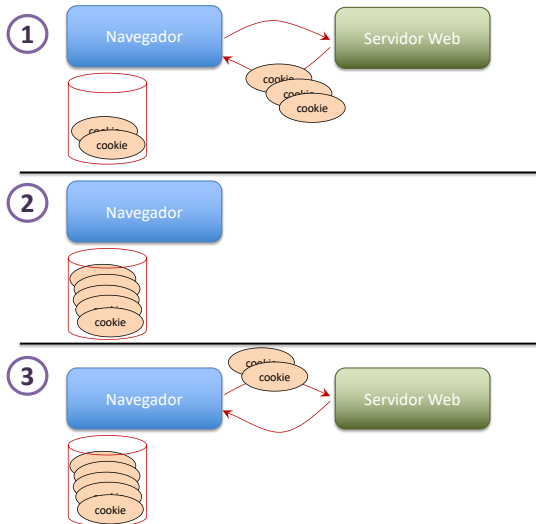
Persistencia de estado en HTTP

- HTTP se diseña de forma que **un servidor no almacena estado por cada petición**. Es decir: cada petición es completamente independiente de otras peticiones que haya hecho antes el mismo cliente.
- Sin embargo, es muy frecuente que aplicaciones web necesiten de mantener un estado persistente entre distintas operaciones de un mismo cliente con un mismo servidor
 - Ejemplo: datos asociados a un usuario (carro de la compra, login de usuario...)
- Soluciones:
 - 1 El estado es mantenido por el servidor de forma externa a HTTP (basándose en la IP del cliente, o en otros datos)
 - 2 Se utiliza HTTP para que el estado se mantenga en los clientes:
 - Mediante URLs incluidas en las páginas que va devolviendo el servidor: se incrusta el estado como parte de la URL
 - En campos (ocultos) de formularios que envía el servidor con el formulario para que posteriormente viajen como parámetros (con GET o POST) al mandar el formulario relleno el cliente al servidor.
 - **Mediante cookies** (RFCs 2109 y 2965).
 - 3 Combinaciones de las dos anteriores: se guardan datos de forma externa (en una base de datos) referenciados por una cookies.

Cookies

- Las **cookies** son datos asociados a identificadores.
- Funcionamiento:
 - 1 el servidor genera una *cookie* para representar un estado asociado a un cliente que ha hecho una petición
 - 2 el servidor envía la *cookie* al cliente
 - 3 el cliente almacena la *cookie*
 - 4 el cliente reenvía la *cookie* al servidor en las futuras peticiones que le realice
- Especificación original de Netscape, luego propuesto como RFC 2109, ampliada en RFC 2965.

Cookies



Cabecera Set-Cookie

- Cabecera con la que un servidor que ha creado una *cookie* se la envía a un cliente.
- El formato incluye:
 - Nombre de la cabecera: `Set-Cookie`
 - Nombre de la *cookie* y valor: `<nombre>=<valor>`
 - Fecha de caducidad: `expires=<fecha>`
 - Dominio (servidor) y trayecto (*path*) para el que es válida: El cliente la reenviará a ese servidor para todas las peticiones de recursos que **empiecen exactamente por ese path**:
`domain=<dominio>; path=<trayecto>`
 - Si debe ser transmitida sólo sobre canales seguros (HTTPS):
`secure`

Ejemplo de cabecera Set-Cookie

```
Set-Cookie: login=pepe; expires=Mon, 30-Jan-2029 12:35:23 GMT;  
domain=www.myserver.com; path=/dir
```

- El servidor ha enviado esta cookie al cliente que la almacenará.
- En peticiones futuras desde ese cliente se enviará esa cookie si se cumplen todas las siguientes condiciones simultáneamente:
 - El cliente se comunica con el servidor `www.myserver.com`.
 - La petición se realiza antes de que expire: 30-Jan-2029 12:35:23 GMT
 - Se accede a un recurso que empiece exactamente por `/dir`.
Por ejemplo si se accede a:
 - `http://www.myserver.com/dir/index.html`: la *cookie* se envía.
 - `http://www.myserver.com/dir/compras/index.html`: la *cookie* se envía.
 - `http://www.myserver.com/compras/dir/index.html`: la *cookie* NO se envía.

Cabecera Cookie

- Cuando un cliente pide una URL a un servidor, buscará en su lista de *cookies* almacenadas de peticiones anteriores, las que cumplen **simultáneamente** las siguientes condiciones:
 - 1 Aún no han expirado
 - 2 Son del mismo *domain* (servidor) al que va se va a hacer la nueva petición
 - 3 La URL que se va a pedir **empieza** por el *path* para el que es válida
- El cliente enviará todas las *cookies* que cumplen las condiciones, en una o más cabeceras **Cookie**.
- Dentro de esta cabecera, las *cookies* se ordenarán de más a menos específicas (según su *path*).
- Las *cookies* con caducidad en el pasado se eliminarán periódicamente para liberar espacio en el cliente.
- Ejemplo de envío de 2 *cookies* que cumplen las condiciones:

```
Cookie: login=pepe; theme=basic
```

Ejemplo (I): el servidor envía Cookie a cliente

- Un cliente solicita un recurso a un servidor y éste guarda información de esta petición asociándole la *cookie* `session-id=11111`.
- El cliente almacenará dicha *cookie*.



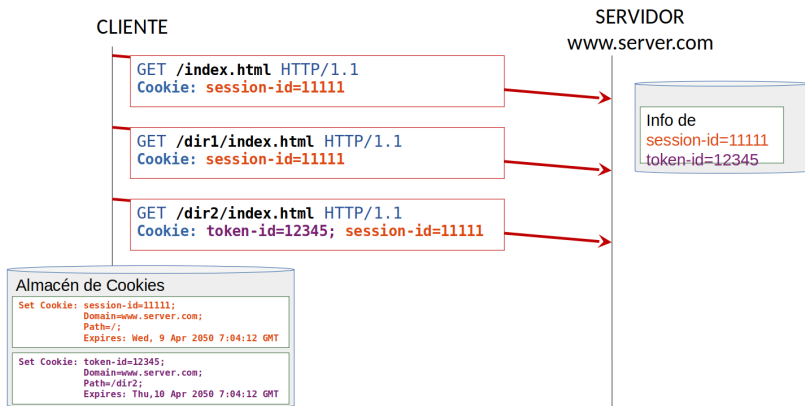
Ejemplo (II): el cliente envía Cookie al servidor

- El cliente tiene almacenada la *cookie* `session-id=11111` y enviará la *cookie* en posteriores accesos si se cumplen las condiciones: Expires, Domain, Path.



Ejemplo: el cliente envía Cookie al servidor

- El cliente tiene almacenadas la *cookies* `session-id=11111` y `token-id=12345` y enviará la cookie en posteriores accesos si se cumplen las condiciones: Expires, Domain, Path.
- Primero se envían las cookies más específicas.



Futuro de las Cookies

- Las cookies se han hecho muy grandes y los mensajes de petición han aumentado alarmantemente de tamaño: El 50 % de las cookies tiene un tamaño mayor de 500 bytes (!!!)
- Se trabaja en alternativas más razonables:

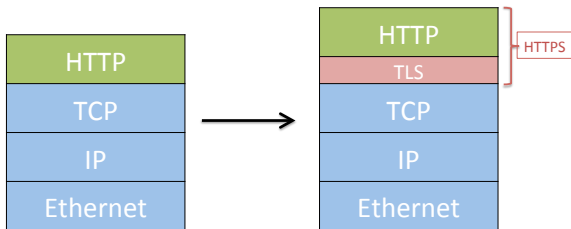
HTTP State Tokens

`https://mikewest.github.io/http-state-tokens/
draft-west-http-state-tokens.html`

Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP
- 4 Caché de contenidos en HTTP
- 5 Cookies
- 6 HTTPS**
- 7 HTTP 2.0 y 3.0
- 8 Referencias

HTTPS



- El término **HTTPS** se refiere a colocar HTTP sobre **TLS** (*Transport Layer Security*).
- TLS aporta características de seguridad a las conexiones TCP. Antiguamente se llamaba SSL (*Secure Sockets Layer*)
- Permite confidencialidad en la conexión (mediante cifrado), autenticación de los extremos e integridad del contenido.
- Las URLs comienzan por **https://**
- El puerto por defecto pasa a ser el **443**.

Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP
- 4 Caché de contenidos en HTTP
- 5 Cookies
- 6 HTTPS
- 7 HTTP 2.0 y 3.0**
- 8 Referencias

HTTP/2

- **HTTP/2** (versión 2.0) es la nueva versión de HTTP. Muy influido por protocolo SPDY desarrollado por Google desde 2009.
- Principales características:
 - Se mantiene la semántica de HTTP/1.1 en cuanto a métodos, códigos de respuesta, URLs, cabeceras...
 - Se especifica cómo será la interacción entre clientes 1.1 y servidores 2.0 o viceversa
 - Una sola conexión para transmitir todos los recursos del mismo servidor, cada petición/respuesta de un recurso será un flujo (*stream*) dentro de la conexión
 - Cabeceras binarias (no de texto), mediante compresión (tamaño medio de cabeceras en 1.1: 800 bytes !!!).
 - Paquetes de datos y paquetes de control
 - Prioridades en los flujos para evitar tener que esperar a completar los recursos previos para que llegue un recurso imprescindible para empezar a mostrar el principio del contenido.
 - **Obligatoriamente sobre TLS.**
 - Extensible para poder cubrir futuras necesidades.

HTTP/3

- Desde los tiempos de HTTP 1.0, ya se pensaba que TCP no era un protocolo de transporte adecuado para HTTP.
- Desde entonces ha habido muchas propuestas de protocolos de transporte alternativos a TCP, pensados para que HTTP resulte eficiente sobre ellos.
- En 2012 Google empieza a trabajar en QUIC, un protocolo de transporte en espacio de usuario (implementado sobre UDP), especialmente pensado para que SPDY fuera encima de QUIC. Desde 2015 está en proceso de estandarización.
- Desde Octubre de 2018, el término **HTTP/3** se refiere oficialmente a los trabajos antes denominados HTTP/2-over-QUIC.
- Actualmente HTTP/2-over-QUIC está soportado en el navegador Chrome y Opera, y en los servidores de Google y en el servidor comercial LiteSpeed.
 - LiteSpeed es el cuarto servidor en implantación (4 %), tras Apache (44 %), Nginx (42 %) y Microsoft IIS (8 %).

Contenidos

- 1 Introducción
- 2 Relación entre HTTP y conexiones TCP
- 3 Formato de mensajes HTTP
- 4 Caché de contenidos en HTTP
- 5 Cookies
- 6 HTTPS
- 7 HTTP 2.0 y 3.0
- 8 Referencias**

Referencias

- J.J. Kurose y K.W. Ross, **Redes de Computadores: un enfoque descendente basado en Internet**, Pearson Educación, 2ª edición.
- W. Richard Stevens, **TCP/IP Illustrated, vol 3**, Addison Wesley.
- James Marshall, **HTTP Made Really Easy. A Practical Guide to Writing Clients and Servers**,
<http://www.jmarshall.com/easy/http/>
- RFC 1945, **HTTP 1.0**,
<http://www.faqs.org/rfcs/rfc1945.html>
- RFC 2068, **HTTP 1.1**,
<http://www.faqs.org/rfcs/rfc2068.html>
- RFC 7540, **HTTP 2.0**,
<http://www.faqs.org/rfcs/rfc7540.html>
- RFC 2964, **Use of HTTP State Management**,
<http://www.faqs.org/rfcs/rfc2964.html>
- RFC 2965, **HTTP State Management Mechanism**,
<http://www.faqs.org/rfcs/rfc2965.html>