

upna

Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

Redes de Nueva Generación
Área de Ingeniería Telemática

Nuevos protocolos

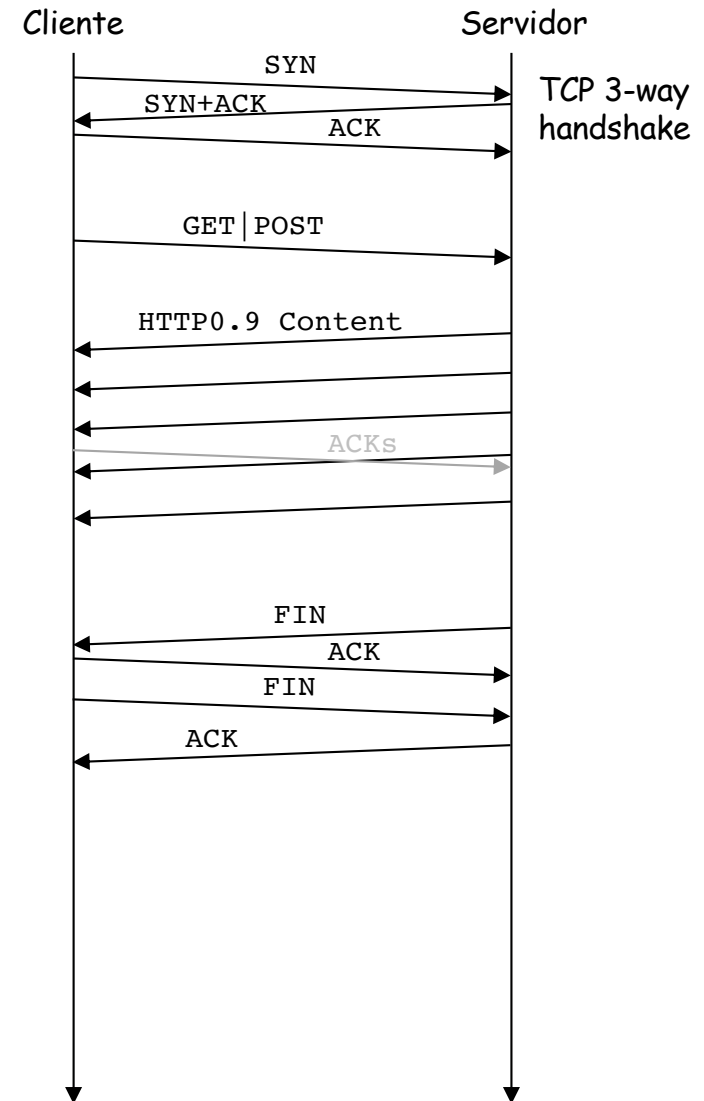
Factores en el rendimiento

- La infraestructura de red
 - Capacidad en el camino
 - Probabilidad de pérdidas
 - Desórdenes
 - Retardos
- El protocolo de transporte
 - Mecanismos de control de conexión
 - Reacción ante pérdidas
 - Adaptación ante congestión (y evitarla)
- El protocolo de aplicación

HTTP 1.1 – Conexiones persistentes y pipelining

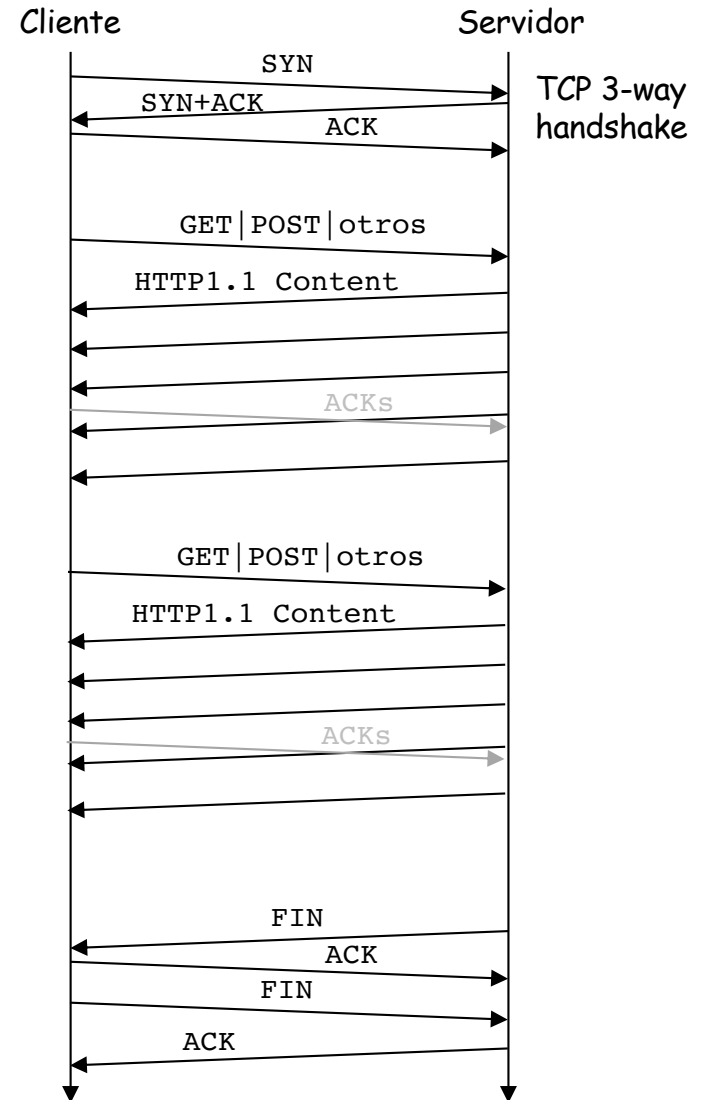
HTTP < 1.1

- Una petición por conexión
- Cierre marca el final de la respuesta



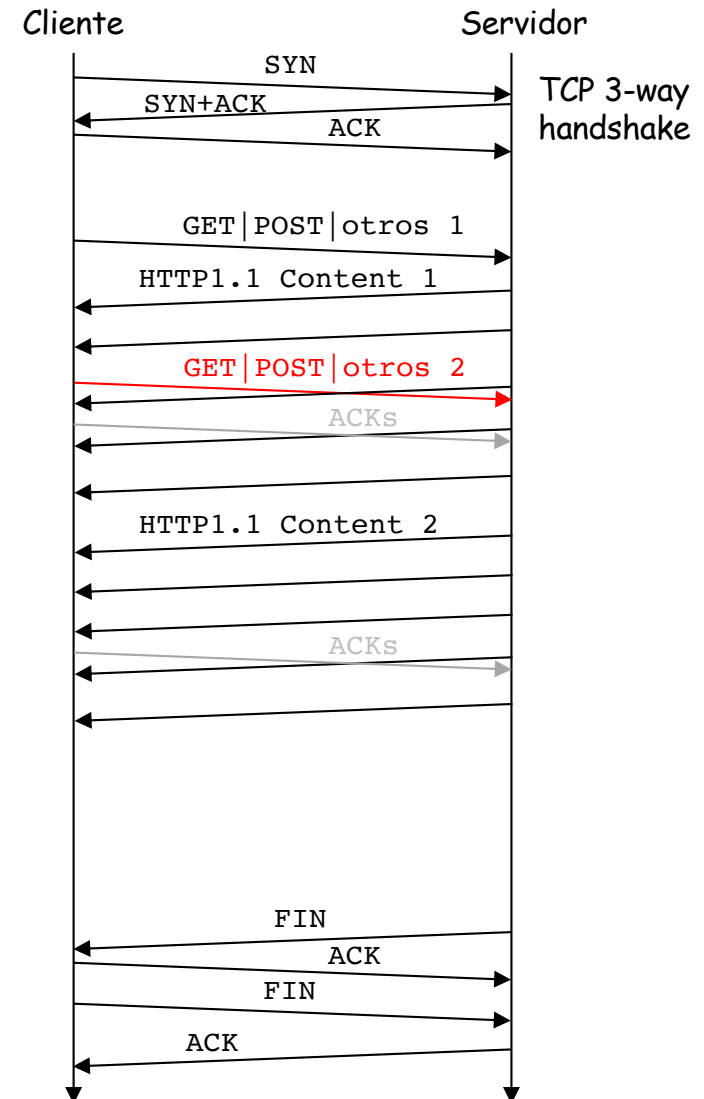
HTTP 1.1

- Conexiones persistentes



HTTP 1.1

- Conexiones persistentes
- Pipelining: respuestas en el mismo orden que las peticiones
- Posible entrega de rangos de bytes



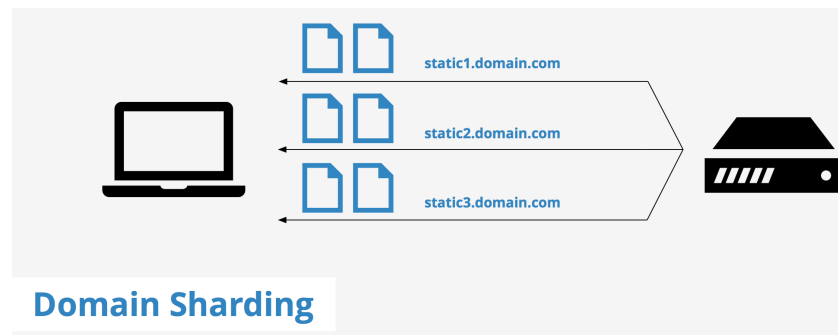
HTTP1.1

- Algunas mejoras en HTTP1.1
 - Conexiones persistentes
 - Pipelining
 - Entrega de rangos de bytes



HTTP1.1

- Y algunos “hacks” de navegadores y desarrolladores
 - Conexiones en paralelo (limitadas a 5-6 para un servidor)
 - *Domain sharding* (recursos en diferentes dominios)
 - Unión de ficheros pequeños (CSS, Javascript, imágenes)
 - Inline de ficheros con el HTML



```

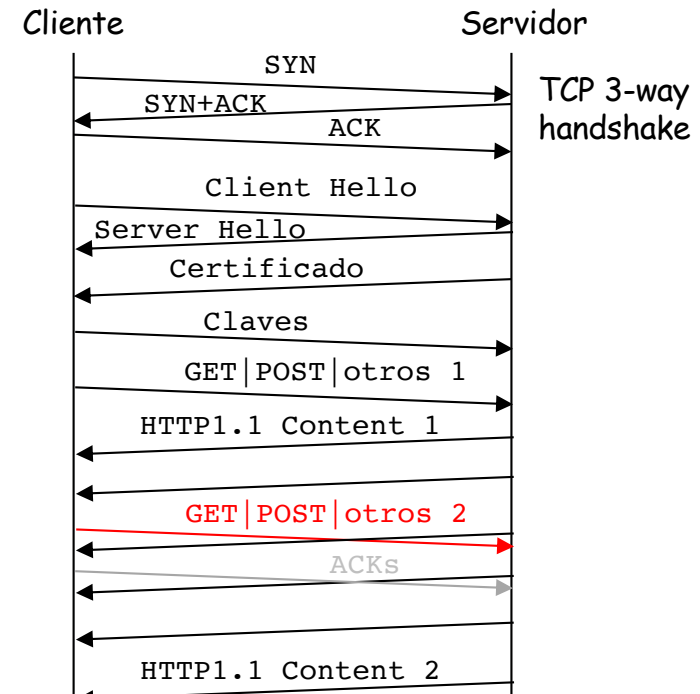
```


HTTP1.1 - Problemas

- Optimizado para grandes transferencias, pero una web contiene muchos recursos pequeños
- Pipelining no suele emplearse (problemas con proxies y algunos servidores)
- Aún con pipelining tiene **HOL blocking** (hasta completar respuesta grande no se atiende a otra del pipeline)
- Para mejorar el tiempo de carga hay que reducir el RTT (CDNs), pero esto tiene un límite (“c”)
- Reducir RTT reduciendo *chattiness*
- *TLS* añade aún más RTTs

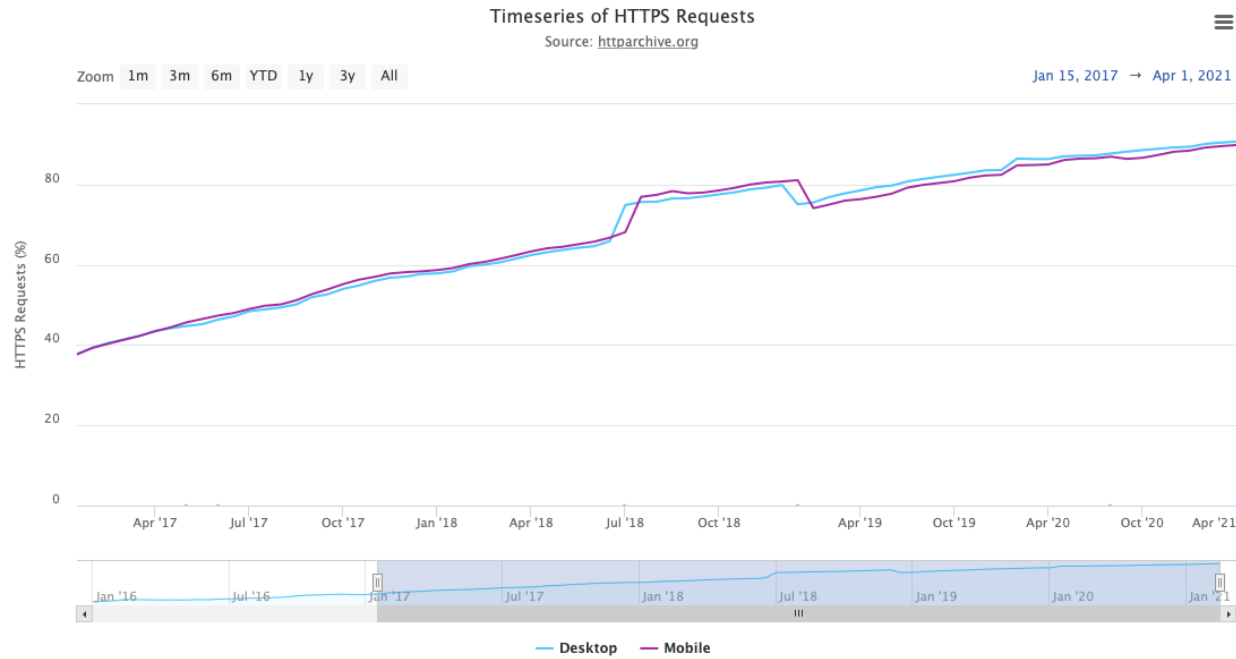
HTTP 1.1 + TLS

- Identificación de capacidades (ciphers, versiones)
- Intercambio de certificados
- Intercambio de información para la construcción de claves
- Al menos 1 RTT



	Time	Source	Destination	Total Length	Info
1	0.000000	10.6.4.40	108.174.11.37	60	45782 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2004512222 TSecr=0 WS=128
2	0.185023	108.174.11.37	10.6.4.40	60	443 → 45782 [SYN, ACK] Seq=0 Ack=1 Win=43440 Len=0 MSS=1460 SACK_PERM=1 TSval=1697854058 TSe
3	0.185106	10.6.4.40	108.174.11.37	52	45782 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2004512407 TSecr=1697854058
4	0.201494	10.6.4.40	108.174.11.37	569	Client Hello
5	0.386559	108.174.11.37	10.6.4.40	52	443 → 45782 [ACK] Seq=1 Ack=518 Win=45056 Len=0 TSval=1697854260 TSecr=2004512423
6	0.388269	108.174.11.37	10.6.4.40	1500	Server Hello
7	0.388341	10.6.4.40	108.174.11.37	52	45782 → 443 [ACK] Seq=518 Ack=1449 Win=64128 Len=0 TSval=2004512610 TSecr=1697854261
8	0.388394	108.174.11.37	10.6.4.40	1500	443 → 45782 [ACK] Seq=1449 Ack=518 Win=45056 Len=1448 TSval=1697854261 TSecr=2004512423 [TCP
9	0.388394	108.174.11.37	10.6.4.40	476	Certificate, Server Key Exchange, Server Hello Done
10	0.388452	10.6.4.40	108.174.11.37	52	45782 → 443 [ACK] Seq=518 Ack=3321 Win=63488 Len=0 TSval=2004512610 TSecr=1697854261
11	0.392660	10.6.4.40	108.174.11.37	145	Client Key Exchange, Change Cipher Spec, Finished
12	0.392847	10.6.4.40	108.174.11.37	151	Message SETTINGS [0] WINDOW_UPDATE [0]

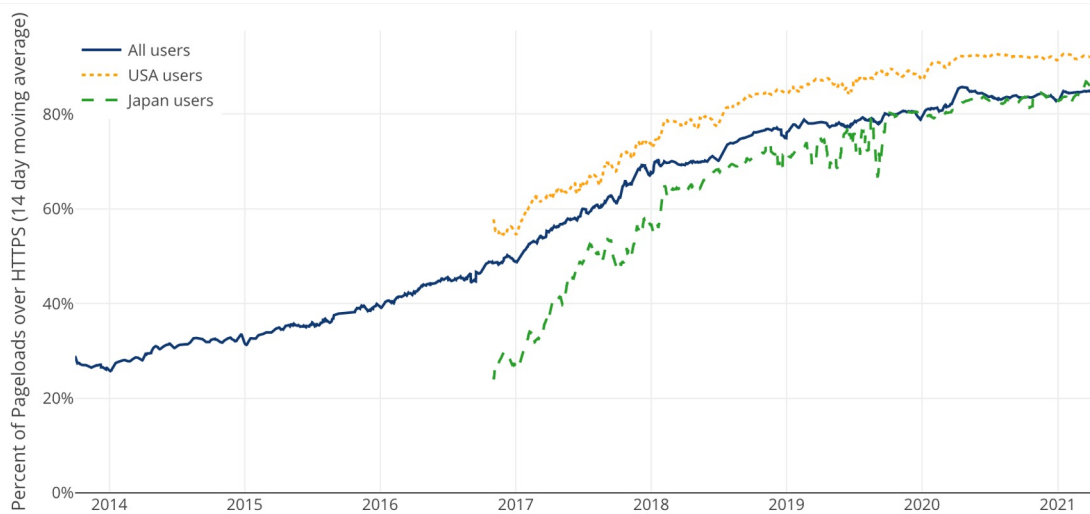
HTTP 1.1 + TLS



(Puede ser H2)

Percentage of Web Pages Loaded by Firefox Using HTTPS

(14-day moving average, source: Firefox Telemetry)



upna

Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

Redes de Nueva Generación
Área de Ingeniería Telemática

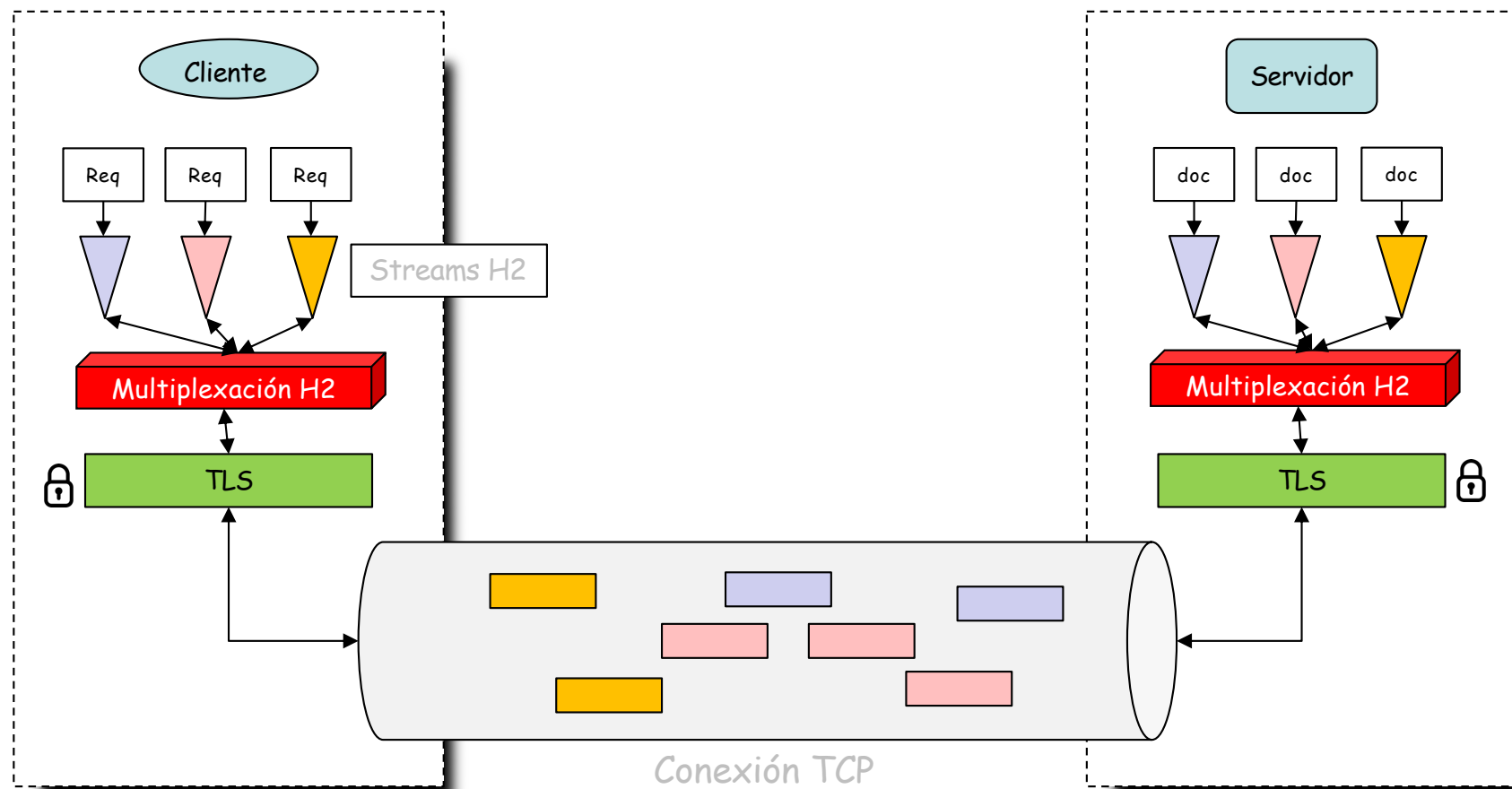
HTTP/2

HTTP/2 (H2)

- RFC 7540 “Hypertext Transfer Protocol Version 2 (HTTP/2)” (BitGo, Google, Mozilla, 2015)
- (Antes SPDY, de Google)
- Binario
 - Ya no es texto, más compacto, más eficiente al procesarlo
 - Se pueden comprimir las cabeceras (evita tener que enviarlas en cada petición o respuesta)
 - Permite multiplexación
- Multiplexación
 - Peticiones y respuestas pueden estar multiplexadas
 - Eso quiere decir por ejemplo que no es necesario completar una respuesta para empezar a enviar otra
 - Trabaja con *streams* dentro de una sola conexión
 - El navegador puede asignarles prioridades en las peticiones
 - Esto elimina el HOL blocking y la necesidad de conexiones en paralelo

Multiplexación en H2

- Frames de los diferentes streams HTTP/2 en mensajes *Application Data* de TLS enviados por la conexión TCP
- Frame HEADERS contienen la cabecera HTTP
- Frame DATA con el contenido de la respuesta (o del POST)



Ejemplo

No.	Time	Source	Destination	Info
61	0.411754	10.6.4.40	72.247.210.11	HEADERS[9]: GET /wp-content/themes/nobelprize/dist/css/style.0.4.2.min.css?ver=0.4.2
62	0.411803	10.6.4.40	72.247.210.11	HEADERS[11]: GET /wp-content/plugins/jetpack/css/jetpack.css?ver=9.2.1
63	0.411803	10.6.4.40	72.247.210.11	HEADERS[13]: GET /wp-content/themes/nobelprize/assets/js/frontend/lib/loadjs.js?ver=0.4.2
64	0.422646	72.247.210.11	10.6.4.40	443 → 60836 [ACK] Seq=29891 Ack=1635 Win=32256 Len=0 TSval=2231141594 TSecr=154066703
65	0.423735	10.6.4.40	72.247.210.11	HEADERS[15]: GET /wp-content/themes/nobelprize/assets/js/frontend/lib/clamp/clamp.min.js?ver=0.4.2
66	0.423785	10.6.4.40	72.247.210.11	HEADERS[17]: GET /wp-content/plugins/nobelprize/assets/js/admin/lib/flickity/flickity.pkgd.js?ver=0.2.0-3
67	0.423834	10.6.4.40	72.247.210.11	HEADERS[19]: GET /wp-content/themes/nobelprize/dist/js/frontend.0.4.2.min.js?ver=0.4.2
68	0.425261	72.247.210.11	10.6.4.40	443 → 60836 [ACK] Seq=29891 Ack=1746 Win=32256 Len=1448 TSval=2231141596 TSecr=154066703 [TCP segment of
69	0.425357	72.247.210.11	10.6.4.40	HEADERS[3]: 200 OK, DATA[3], DATA[3] (text/css)
70	0.425447	10.6.4.40	72.247.210.11	60836 → 443 [ACK] Seq=2092 Ack=32472 Win=63488 Len=0 TSval=154066717 TSecr=2231141596
71	0.426687	72.247.210.11	10.6.4.40	HEADERS[5]: 200 OK, DATA[5], DATA[5] (text/css)
72	0.427213	72.247.210.11	10.6.4.40	443 → 60836 [ACK] Seq=33326 Ack=1746 Win=32256 Len=1448 TSval=2231141598 TSecr=154066703 [TCP segment of
73	0.427279	10.6.4.40	72.247.210.11	60836 → 443 [ACK] Seq=2092 Ack=34774 Win=63488 Len=0 TSval=154066719 TSecr=2231141598
74	0.427335	72.247.210.11	10.6.4.40	443 → 60836 [ACK] Seq=34774 Ack=1746 Win=32256 Len=1448 TSval=2231141598 TSecr=154066703 [TCP segment of
75	0.427459	72.247.210.11	10.6.4.40	443 → 60836 [ACK] Seq=36222 Ack=1746 Win=32256 Len=1448 TSval=2231141598 TSecr=154066703 [TCP segment of

- ▶ Frame 69: 1199 bytes on wire (9592 bits), 1199 bytes captured (9592 bits)
- ▶ Ethernet II, Src: Cisco_dc:71:c4 (30:e4:db:dc:71:c4), Dst: Universa_2c:dc:6c (00:1e:37:2c:dc:6c)
- ▶ Internet Protocol Version 4, Src: 72.247.210.11, Dst: 10.6.4.40
- ▶ Transmission Control Protocol, Src Port: 443, Dst Port: 60836, Seq: 31339, Ack: 1746, Len: 1133
- ▶ [2 Reassembled TCP Segments (2581 bytes): #68(1448), #69(1133)]
- ▼ Transport Layer Security
 - ▼ TLSv1.3 Record Layer: Application Data Protocol: http2
 - Opaque Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 2576
 - [Content Type: Application Data (23)]
 - Encrypted Application Data: 77f9299f91c1e3032294907016a1b4ea3a5a541fe3dc618bc9b9c27bf0f6efba97b46755...
 - [Application Data Protocol: http2]
- ▼ HyperText Transfer Protocol 2
 - ▶ Stream: HEADERS, Stream ID: 3, Length 227, 200 OK
 - ▼ Stream: DATA, Stream ID: 3, Length 2305 (partial entity body)
 - Length: 2305
 - Type: DATA (0)
 - ▶ Flags: 0x00
 - 0... .. = Reserved: 0x0
 - .000 0000 0000 0000 0000 0000 0000 0011 = Stream Identifier: 3
 - [Pad Length: 0]
 - [Reassembled body in frame: 69](#)
 - Data: 1f8b080000000000cd5ae98ee336127e156f06013241d8b0bddd8389849d3ffb1883...
 - ▶ Stream: DATA, Stream ID: 3, Length 0

HTTP/2 (H2)

- RFC 7540 “Hypertext Transfer Protocol Version 2 (HTTP/2)” (BitGo, Google, Mozilla, 2015)
- (Antes SPDY, de Google)
- Binario
 - Ya no es texto, más compacto, más eficiente al procesarlo
 - Se pueden comprimir las cabeceras (evita tener que enviarlas en cada petición o respuesta)
 - Permite multiplexación
- Multiplexación
 - Peticiones y respuestas pueden estar multiplexadas
 - Eso quiere decir por ejemplo que no es necesario completar una respuesta para empezar a enviar otra
 - Trabaja con *streams* dentro de una sola conexión
 - El navegador puede asignarles prioridades en las peticiones
 - Esto elimina el HOL blocking y la necesidad de conexiones en paralelo
- Server Push
 - El servidor puede entregar recursos al cliente aunque no los haya pedido
 - Ahorra la petición (esto se estaba haciendo con el *inlining*)

HTTP/2

- Flow Control
 - Para cada *stream*
 - HTTP/2 no fuerza a un algoritmo para el control de flujo, solo lo soporta
- Negociación
 - Mediante mensajes se puede subir una conexión de HTTP1.1 a HTTP/2

```
GET /page HTTP/1.1
Host: server.example.com
Connection: Upgrade, HTTP2-Settings
Upgrade: HTTP/2.0
HTTP2-Settings: (SETTINGS payload)
```

```
HTTP/1.1 200 OK
Content-length: 243
Content-type: text/html
(... HTTP 1.1 response ...)
```

(or)

```
HTTP/1.1 101 Switching Protocols
Connection: Upgrade
Upgrade: HTTP/2.0
(... HTTP 2.0 response ...)
```

HTTP/2

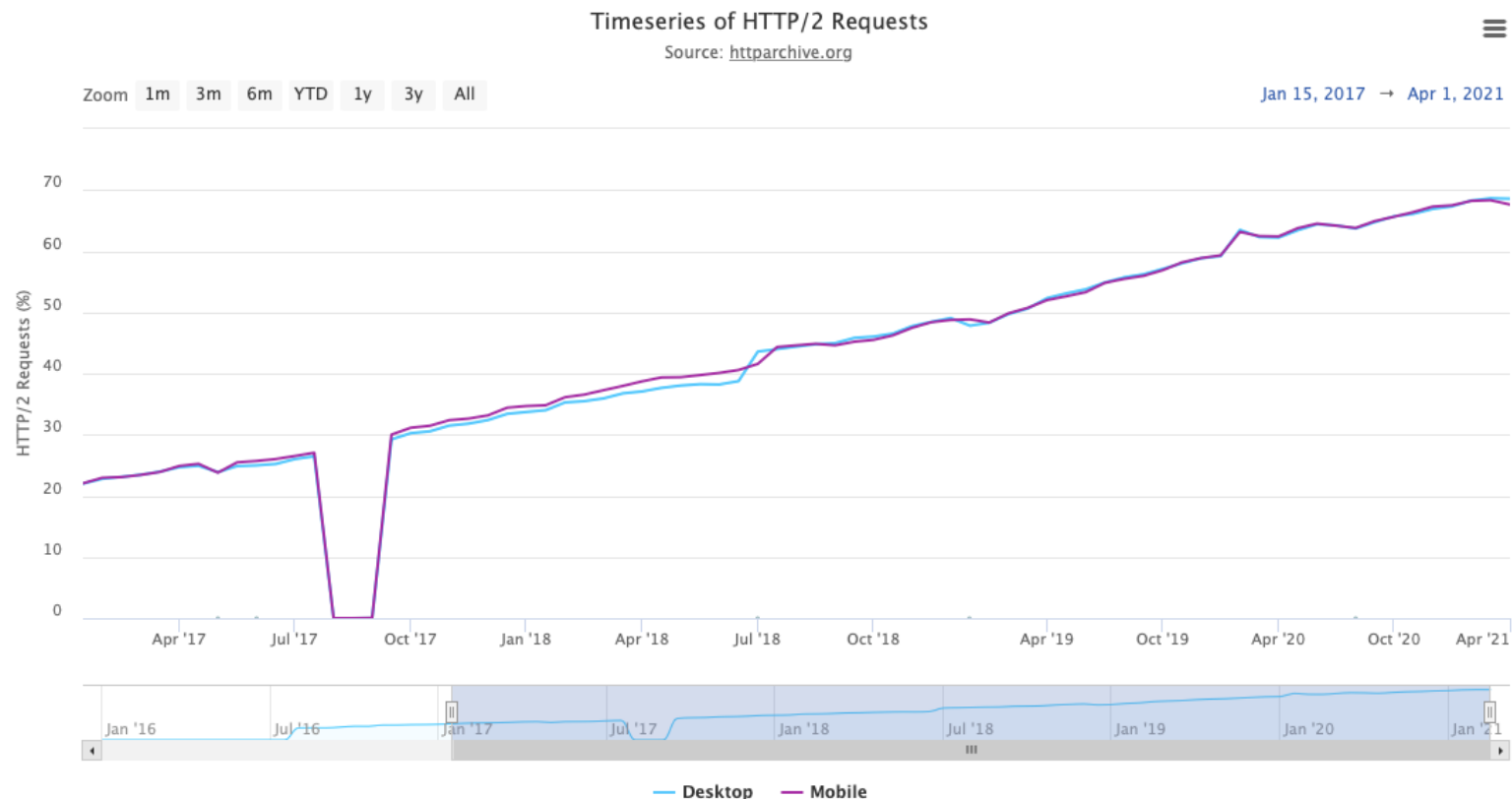
- Flow Control
 - Para cada *stream*
 - HTTP/2 no fuerza a un algoritmo para el control de flujo, solo lo soporta
- Negociación
 - Mediante mensajes se puede subir una conexión de HTTP1.1 a HTTP/2
 - Hoy en día solo sobre TLS
 - Mediante el ALPN

```
Transmission Control Protocol, Src Port: 45782, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
  Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 508
    Version: TLS 1.2 (0x0303)
    Random: 4232b9f46fd109bc090b941ecf727e14a3584d269a408fcf7514d8af2847d8
    Session ID Length: 32
    Session ID: fd8622edb4e61e53991a279dfd553827984a4b1941ea0eef9d18d62e75a1cbcd
    Cipher Suites Length: 32
    Cipher Suites (16 suites)
    Compression Methods Length: 1
    Compression Methods (1 method)
    Extensions Length: 403
    Extension: Reserved (GREASE) (len=0)
    Extension: server_name (len=24)
    Extension: extended_master_secret (len=0)
    Extension: renegotiation_info (len=1)
    Extension: supported_groups (len=10)
    Extension: ec_point_formats (len=2)
    Extension: session_ticket (len=0)
    Extension: application_layer_protocol_negotiation (len=14)
      Type: application_layer_protocol_negotiation (16)
      Length: 14
      ALPN Extension Length: 12
    ALPN Protocol
      ALPN string length: 2
      ALPN Next Protocol: h2
      ALPN string length: 8
      ALPN Next Protocol: http/1.1
    Extension: status_request (len=5)
    Extension: signature_algorithms (len=18)
```

```
Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
Ethernet II, Src: Cisco_dc:71:c4 (30:e4:db:dc:71:c4), Dst: Universa_2c:dc:6c (00:1e:37
Internet Protocol Version 4, Src: 108.174.11.37, Dst: 10.6.4.40
Transmission Control Protocol, Src Port: 443, Dst Port: 45782, Seq: 1, Ack: 518, Len:
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 106
  Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 102
    Version: TLS 1.2 (0x0303)
    Random: 331342a38cec5db5f136683375f91bf62cc515ff2d5eeb65fe820e9d03c4281b
    Session ID Length: 32
    Session ID: 714f39799dd6b7b43998b1c41d9e1209a6fe7514f7de012408ed9472cbf179e3
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Compression Method: null (0)
    Extensions Length: 30
    Extension: renegotiation_info (len=1)
    Extension: server_name (len=0)
    Extension: ec_point_formats (len=4)
    Extension: application_layer_protocol_negotiation (len=5)
      Type: application_layer_protocol_negotiation (16)
      Length: 5
      ALPN Extension Length: 3
    ALPN Protocol
      ALPN string length: 2
      ALPN Next Protocol: h2
    Extension: extended_master_secret (len=0)
```

HTTP/2: Status

- RFC aprobada
- Múltiples implementaciones, en navegadores y servidores
- Soportado en IE11, Firefox51, Chrome49, Safari10, Opera43, etc
- Soportado ya por muchas CDNs y hostings (ej: Akamai, Azure CDN, MaxCDN, KeyCDN, CacheFly, CloudFlare, Hawk host, etc)
- Estimaciones de que es empleado en el 46.4% de websites¹



<http://isthewebhttp2yet.com/measurements/adoption.html#time>

¹ <https://w3techs.com/technologies/details/ce-http2/all/all> (Mayo 2021)