Universidad Nacional de Luján

Proxy Adaptativo Para Protocolos Web Avanzados

Trabajo Final presentado por Pablo Maximiliano Lulic
para obtener el grado de Licenciado en Sistemas de Información

Director: Mg. Gabriel Tolosa
Co-Director: Lic. Marcelo Fernández

2014

Agradecimientos

Agradezco a mi familia, por su apoyo en todos estos años de carrera y porque sin ustedes esto no hubiera sido posible.

A Euge, por estar junto a mi y acompañarme todos estos años, por tu comprensión y por alentarme en cada momento.

A Gabriel, por su gran apoyo y paciencia, por impulsar el desarrollo de este trabajo y por sobre todo, por ser una gran persona. De igual manera a Marcelo, por estar siempre dispuesto a ayudar y ser mi soporte técnico.

A mis compañeros de trabajo, por brindarme el espacio necesario para poder dedicarle tiempo a este trabajo.

Índice general

Capítulo 1

Introducción

El principal protocolo utilizado en la Web es HTTP[1] [15], tuvo su primera versión en mayo de 1996, culminando en 1999 con el estándar actual que es HTTP 1.1. Es un protocolo sin estado, lo que conlleva a que sea necesario realizar una conexión nueva por cada recurso que se necesite en un sitio. Por ejemplo, si una página posee 5 imágenes y un archivo de Javascript[2], se van a realizar 7 conexiones para obtener toda la página completa, la primera para obtener la página, y una vez que el navegador lee el contenido de la misma, realiza el resto de las peticiones para obtener todos los elementos.

Los sitios web de la actualidad difieren de las páginas de hace más de 10 años, tanto en tamaño como en cantidad de recursos. Este fenómeno, hace que el protocolo ya no tenga el mismo rendimiento que en épocas anteriores. A pesar del avance de la tecnología en cuanto a mejoras en las velocidades de los enlaces de red, poseer gran ancho de banda no es el único factor que interviene en la performance de la carga de las páginas. Google propuso un protocolo llamado SPDY[3] como solución a los problemas actuales, busca mejorar la performance de HTTP siendo transparente su implementación. Se verá en los capítulos siguientes, los problemas que presentan los protocolos, y bajo qué circunstancias se ven beneficiados o perjudicados en cuanto a su performance.

[1] Hypertext Transfer Protocol.

[2] Lenguaje de programación interpretado que se utiliza principalmente del lado del cliente en el navegador.

[3] SPeeDY.

1.1. Motivación

La IETF[4] es una organización internacional que regula las propuestas y los estándares de Internet, conocidos como RFC[5]. Un grupo de trabajo que pertenece a la IETF llamado *HTTPbis*[6] se encuentra desarrollando el nuevo protocolo HTTP 2.0 [10] que es la evolución de HTTP. Este protocolo, toma como punto de partida a SPDY y se continúan realizando cambios y mejoras. Por esto, es importante estudiar el rendimiento de los protocolos, en especial el de SPDY que es la base de la evolución del protocolo más utilizado en Internet.

1.2. Objetivos

En este trabajo, se presenta la problemática, se propone, y desarrolla un servidor proxy con un algoritmo adaptativo que determina según el perfil de cada sitio que método (HTTP, HTTPS ó SPDY) elegir para mejorar la performance, es decir, que decisión sería la óptima.

1.3. Organización del trabajo

En el Capítulo 2 se conoce el desarrollo que tuvo la web a lo largo de estos años, se observa el crecimiento de Internet y de los sitios

En el Capítulo 3, se avanza sobre diversos conceptos de los protocolos que se utilizan actualmente, así también como sus debilidades.

En el Capítulo 4, se estudian las problemáticas asociadas a la web y ciertas técnicas de optimización.

En el Capítulo 5, se ve el concepto de proxy, necesario para comprender el desarrollo en sí, también se introducen ciertas cuestiones de caché web en el Capítulo 6. Ya con toda la información necesaria, en el Capítulo 7, se ve el desarrollo del proxy propuesto, con sus características y funcionalidades.

[4]Internet Engineering Task Force - http://www.ietf.org
[5]Request For Comments
[6]Hypertext Transfer Protocol Bis.

Hacia el final, en el Capítulo 8, con el fin de evaluar las prestaciones del proxy en un ambiente real, se realiza un experimento y se comentan sus resultados. En el último Capítulo se exponen las conclusiones finales y los trabajos futuros.

El glosario, la bibliografía y los anexos se encuentran al final de este trabajo.

No existe un capítulo dedicado a trabajos relacionados como tal, pero estos pueden encontrarse a lo largo de los capítulos, especialmente en el capítulo del desarrolo de la web (Capítulo 2) y de la problemática de la misma (Capítulo 4).

Capítulo 2

Desarrollo de la Web

2.1. Introducción

Internet es una red de interconexión global de redes individuales alrededor del mundo. Originalmente fué utilizada para interconectar laboratorios dedicados a la investigación gubernamental. Desde 1994 se expandió para millones de usuarios de todo el mundo que la utilizan con múltiples propósitos. A medida que fué creciendo, cambió la forma de hacer negocios y de comunicarse hasta llegar a ser una fuente de información universal para millones de personas [11].

2.2. El crecimiento de Internet

Internet es un medio que sigue creciendo de manera exponencial. Hacia 1995 la cantidad de usuarios promedio era de 16 millones, 1 año después, la cifra ascendió a más del doble. Para el año 2000 se incrementó 10 veces la cantidad de usuarios. Esta información puede verse en el Cuadro 2.1.

Fecha	Usuarios(mill)	% Población Mundial
Diciembre, 1995	16	0.4
Diciembre, 1996	36	0.9
Diciembre, 1997	70	1.7
Diciembre, 1998	147	3.6
Diciembre, 1999	248	4.1
Diciembre, 2000	361	5.8
Agosto, 2001	513	8.6
Septiembre, 2002	587	9.4
Diciembre, 2003	719	11.1
Diciembre, 2004	817	12.7
Diciembre, 2005	1018	15.7
Diciembre, 2006	1093	16.7
Diciembre, 2007	1319	20.0
Diciembre, 2008	1574	23.5
Junio, 2009	1669	24.7
Septiembre, 2009	1734	25.6
Junio, 2010	1966	28.7
Septiembre, 2010	1971	28.8
Marzo, 2011	2095	30.2
Junio, 2011	2110	30.4
Septiembre, 2011	2180	31.5
Diciembre, 2011	2267	32.7
Marzo, 2012	2336	33.3
Junio, 2012	2405	34.3
Septiembre, 2012	2439	34.8
Diciembre, 2012	2497	35.7
Marzo, 2013	2749	38.8

Cuadro 2.1: Crecimiento de la cantidad de usuarios de Internet, información extraída de [11]

También puede observarse en el Gráfico 2.1 el crecimiento exponencial que tuvo la cantidad de usuarios de Internet, y es clara la tendencia de seguir creciendo.

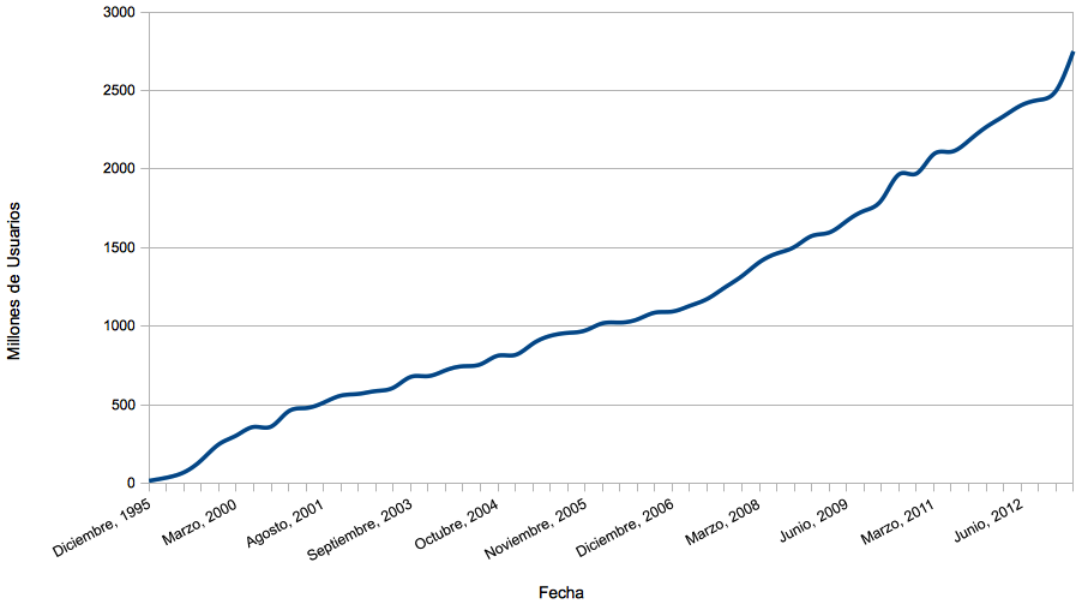

Figura 2.1: Crecimiento de la cantidad de usuarios de Internet, información extraída de [11]

Además de la cantidad de usuarios, en paralelo iba creciendo la cantidad de dominios[1]. En sus inicios, la cantidad de dominios era de 19.732 (medición realizada en Agosto de 1995), la medición más actual (Febrero 2014) realizada por Netcraft[2] da un total aproximado de sitios de 920.102.079 [6] (58 millones más que el mes anterior). Esto se puede ver en el Gráfico 2.2.

[1]Nombre que identifica un sitio web, se asocia a una dirección IP (ver 3.3) única.
[2]NetCraft - http://news.netcraft.com/

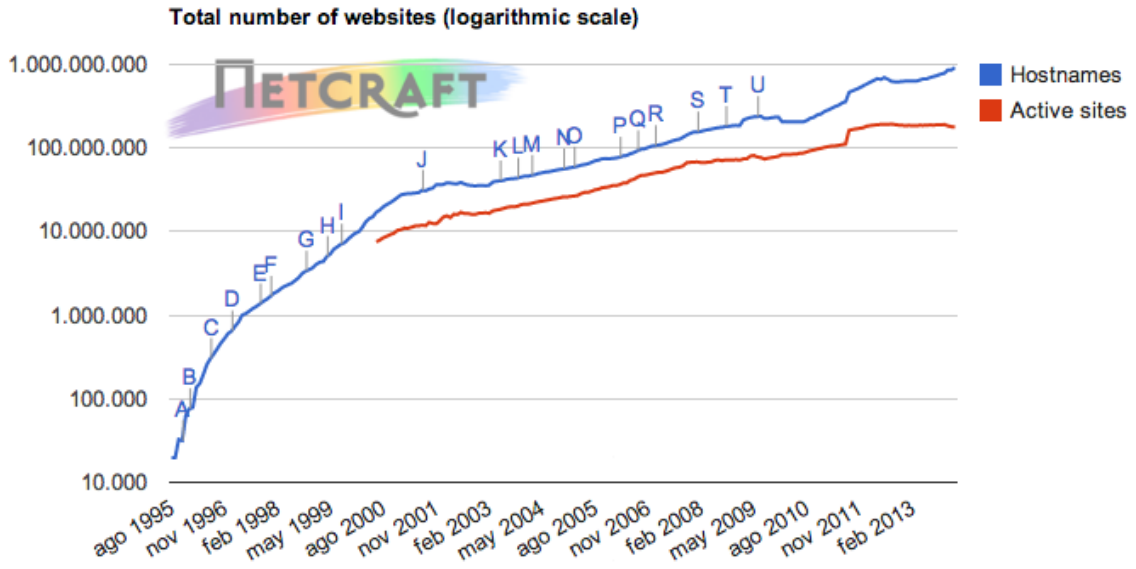

Figura 2.2: Crecimiento de la cantidad de sitios en Internet, extraído de [6]

2.3. El crecimiento de los sitios

Se define sitio como el conjunto de páginas relacionadas, que se encuentran en un servidor web, bajo un mismo dominio en Internet. El aumento del tamaño promedio de los sitios así también como la cantidad de recursos que poseen los mismos, es otra variable que entra en juego.

En el año 1997, el tamaño promedio de un sitio era de 60Kb [48], prácticamente era todo texto, pocas imágenes y poca interactividad. Esto fué cambiando con el tiempo, con el avance de la tecnología y de los recursos que se podían compartir en la red. El crecimiento a lo largo del tiempo puede verse en el Gráfico 2.3.

Hoy en día, el contenido de los sitios es mucho más variado e interactivo. Se componen de diversos tipos de recursos: scripts, hojas de estilo, variados tipos de imágenes, video, contenido Flash[3], etc. Esto produce un aumento en el tiempo de carga de las páginas y la necesidad de poseer un dispositivo con la capacidad necesaria para procesarla y renderizarla[4].

[3] http://www.adobe.com/
[4] El navegador "dibuja"la página según el código HTML y el estilo.

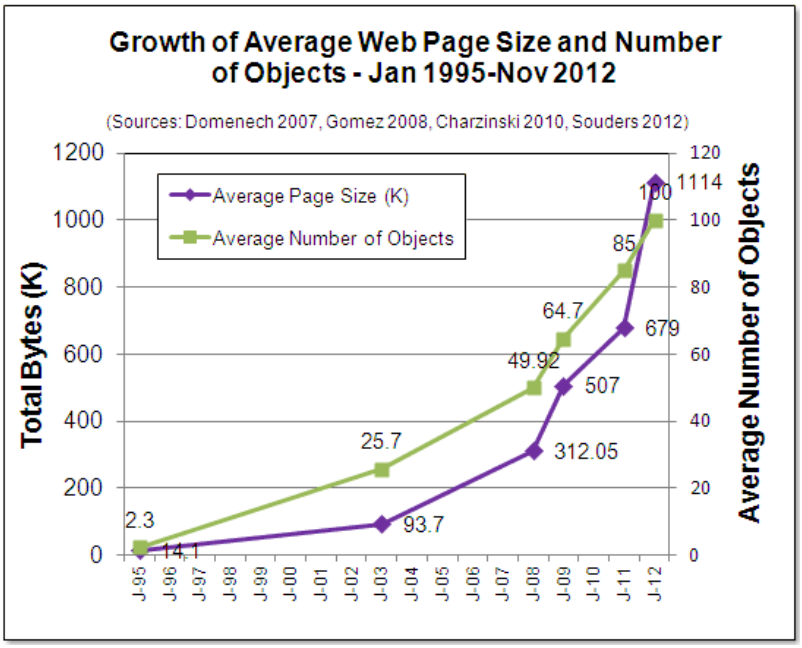

Figura 2.3: Crecimiento del tamaño de los sitios en Internet (1995 a 2012), extraído de [40]

Comparando 2 medidas realizadas por HTTP Archive [9] con casi 4 años de diferencia, se observa que, en la primera medición el promedio es de 702Kb[5], el promedio detallado por contenido de los sitios se puede ver en el Gráfico 2.4. En la segunda medición realizada en Junio de 2014, se observa que el promedio es de 1808Kb, es decir, que hubo un aumento de un 157 %.

[5]Medición extraída de [9] el 15 de Noviembre de 2010.

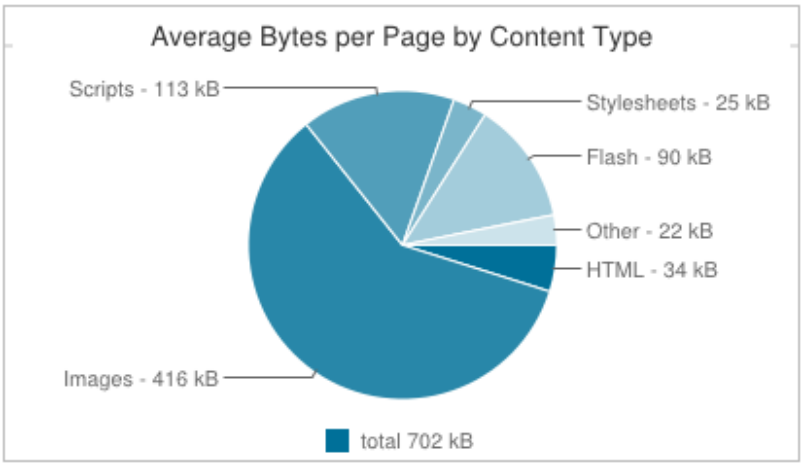

Figura 2.4: Tamaño promedio de los sitios en Internet (Noviembre 2010), detallado por contenido, extraído de [9]

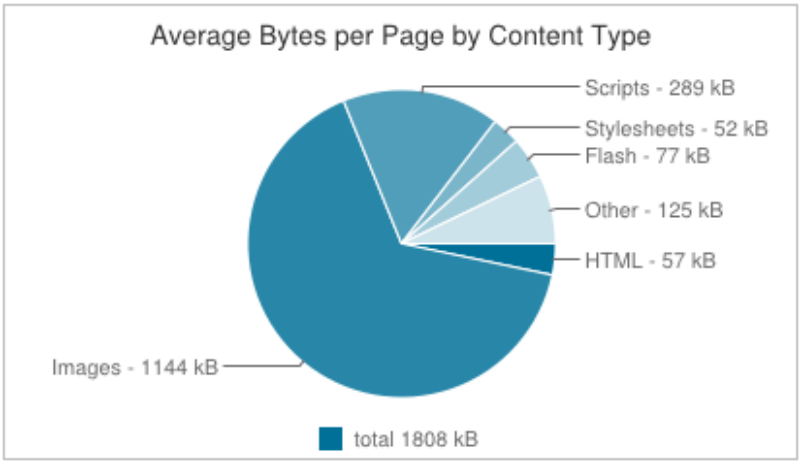

Figura 2.5: Tamaño promedio de los sitios en Internet (Junio 2014), detallado por contenido, extraído de [9]

Otra cuestión es el aumento de la utilización de HTTPS[6], la versión segura de HTTP (ver Capítulo 3), como se verá más adelante, este protocolo añade tiempo en la negociación previa a recuperar la página.

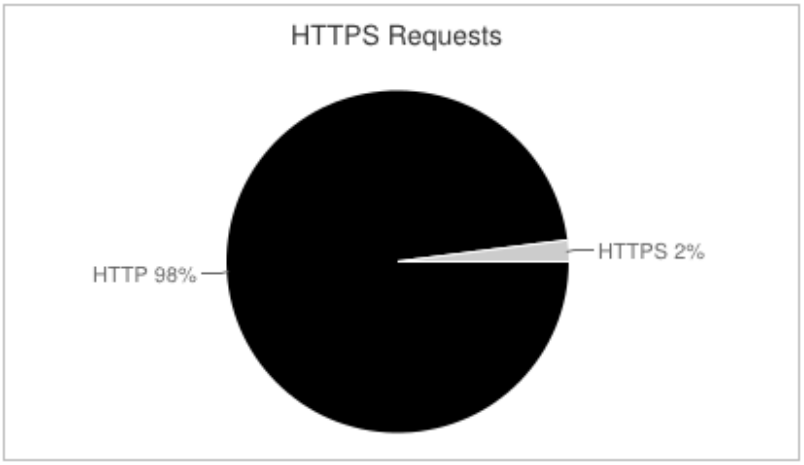

Figura 2.6: Porcentaje de utilización de HTTP/HTTPS (Noviembre 2010), extraído de [9]

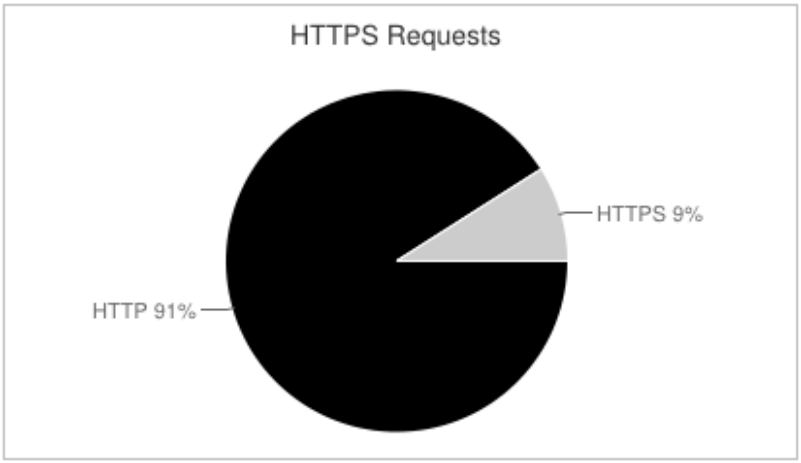

Figura 2.7: Porcentaje de utilización de HTTP/HTTPS (Junio 2014), extraído de [9]

[6]Hypertext Transfer Protocol Secure.

El aumento de complejidad de los sitios, hace que el protocolo HTTP, que originalmente fué diseñado para páginas "simples", baje su performance, aumentando el tiempo de carga de las páginas. No fué especialmente diseñado para latencia, la demanda actual de la web no se pudo haber previsto cuando se desarrolló. Esto motiva a repensar el protocolo, y revisar cuestiones como: petición individual por conexión, peticiones iniciadas exclusivamente por los clientes, headers de petición y respuesta sin compresión, headers redundantes, compresión opcional. Estas características y otras se verán en el Capítulo siguiente.

Capítulo 3

Conceptos sobre Protocolos

3.1. Definición

Un protocolo de comunicación es un conjunto de reglas y normas de transmisión, que permite a dos o más entidades, comunicarse entre sí.

> *"Un protocolo define el formato y el orden de los mensajes intercambiados entre dos o más entidades que se comunican, así como las acciones que se toman en la transmisión y/o recepción de un mensaje u otro evento [34]."*

Es necesario que, antes de establecer una comunicación entre partes, se definan ciertos protocolos para poder asegurar la interoperabilidad y hacer posible la comunicación entre el emisor y receptor.

Las reglas definen la forma en la que debe efectuarse la comunicación, incluyendo cuestiones como la temporización, secuencia, revisión y corrección de errores. Define una *sintaxis* (formato de los mensajes), una *semántica* (significado de los mensajes) y *sincronización* (secuenciamiento y temporización en la comunicación).

Las tareas a realizar se dividen en niveles (capas), luego, los protocolos de cada capa son los que resuelven las tareas. Definir los modelos en capas brinda las siguientes ventajas:

1. Dividir la comunicación en partes más pequeñas y sencillas
2. Normalizar los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
3. Permitir la interoperabilidad de diferentes tipos de hardware y software de red para comunicarse entre sí.
4. Impedir que los cambios en una capa puedan afectar a las otras capas. Facilita la actualización del protocolo pudiendo modificar un módulo a reemplazarlo todo por completo.

3.2. Modelo OSI

En los inicios de Internet, hubo un gran crecimiento tanto en cantidad como en tamao de las redes. Debido a esto, muchas de las redes eran incompatibles entre sí, y era extremadamente complicada la comunicación entre ellas. Para solucionar este problema, la ISO[1], realizó ciertas investigaciones acerca de los esquemas de red. En 1980 [53], creó un modelo de red para ayudar a los diseadores de redes a poder implementar redes que puedan comunicarse entre sí y trabajar en conjunto. Este es el modelo de referencia OSI, definida en la ISO/IEC 7498-1 [32]. Este modelo se agrupa en capas, cada capa agrupa una función determinada. Están organizadas jerárquicamente, cada capa ofrece un servicio a la capa superior. Es un modelo teórico, toma la experiencia de la pila de protocolos TCP/IP (ver 3.3), modelo que soporta Internet.

[1]International Standard Organization

El modelo tiene 7 capas:

7. Aplicación
6. Presentación
5. Sesión
4. Transporte
3. Red
2. Enlace
1. Físico

Se puede ver su distribución en la Figura 3.1

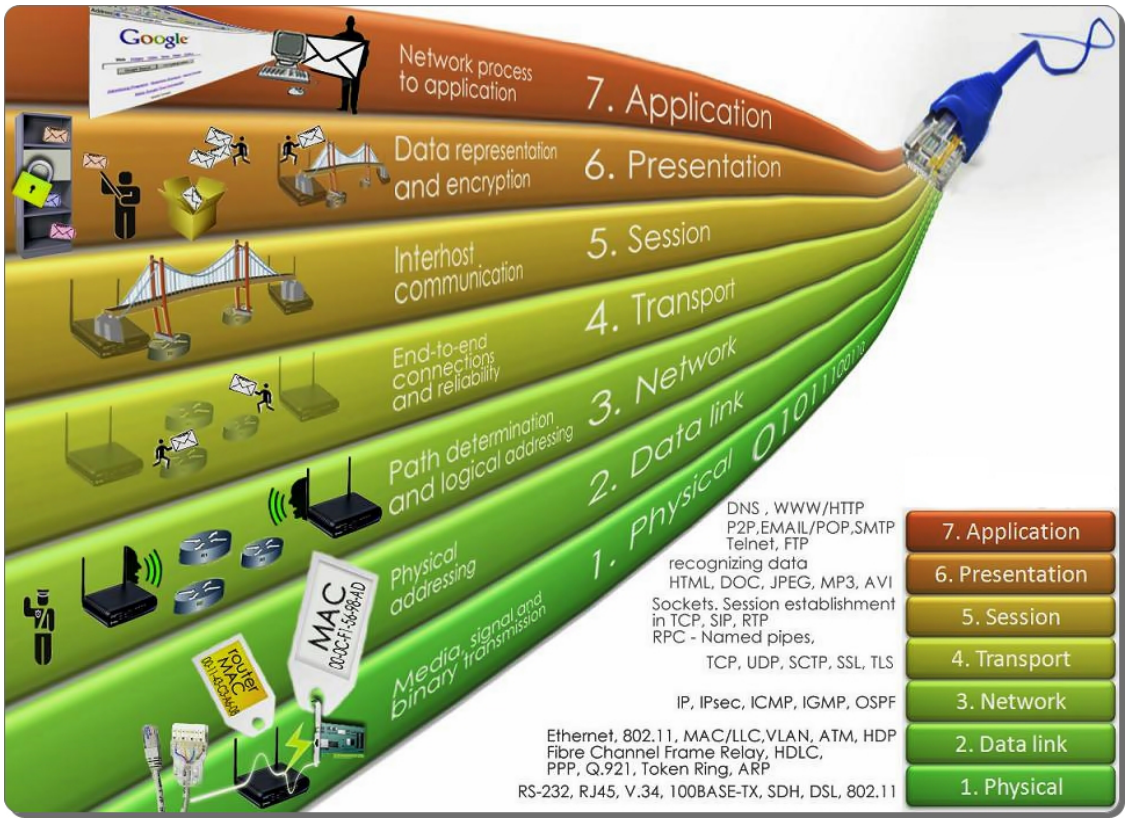

Figura 3.1: Capas OSI, extraído de http://www.gargasz.info/

3.2.1. Capa de Aplicación

Proporciona servicios de red a las aplicaciones del usuario, es la única capa que no provee servicios a otra capa. Si bien es la interfaz hacia el usuario, este no interactúa directamente con esta capa, sino que lo hace a través de una aplicación que si tiene acceso directo a esta capa.

3.2.2. Capa de Presentación

Define el formato de los datos que se van a intercambiar entre las aplicaciones y ofrece a los programas de aplicación un conjunto de servicios de transformación de datos. Esta capa es la encargada de manejar las estructuras de datos abstractas y realizar las conversiones de representación de datos necesarias para la correcta interpretación de los mismos.

3.2.3. Capa de Sesión

Esta capa establece, administra y finaliza las sesiones entre las partes intervinientes en la comunicación, a esto se le llama servicio de administración de la sesión. También realiza el control del intercambio de datos y sincroniza el diálogo entre las partes, a esto se le llama servicio de administración del diálogo.

3.2.4. Capa de Transporte

Esta capa provee un servicio de transporte universal. Ofrece transparencia en el intercambio de datos entre los hosts involucrados (extremo a extremo) y aísla a las capas superiores de los detalles de implementación del transporte. Asegura que los datos enviados lleguen en el mismo orden en el que han sido enviados y sin errores, brindando calidad de servicio y confiabilidad en la comunicación.

3.2.5. Capa de Red

Se encarga de la conexión de hosts que pueden encontrarse en redes diferentes, define un esquema de direccionamiento, enrutamiento y selección de rutas. Permite que los datos viajen de un extremo a otro a través de redes interconectadas. Se

utilizan los paquetes como unidad de información, estos paquetes son los que se rutean a través de la red para llegar del origen al destino.

3.2.6. Capa de Enlace

Proporciona una comunicación confiable entre equipos adyacentes. Se ocupa del direccionamiento físico, la topología de la red y el acceso a la misma. Se utilizan tramas como unidad de información, aquí se realizan los controles de flujo, controles de secuencia, y notificación de errores.

3.2.7. Capa Física

Esta capa provee las características procedurales, funcionales, eléctricas y mecánicas para establecer, mantener y cerrar conexiones físicas. Define como se transmiten los datos al medio, recibe mensajes y los transforma en bits para su posterior envío a través de señales. Ciertas características tales como los conectores físicos, niveles de voltaje, duración de un bit, velocidad de los datos físicos, temporización y otros datos similares son definidos por las especificaciones de esta capa.

3.2.8. Funciones de los Protocolos

Entre las funciones de los protocolos se encuentran:

1. Encapsulamiento:

   Cada capa define lo que se conoce como PDU (Unidad de Datos del Protocolo), que es el resultado de la capa anterior con información propia. A medida que los datos van bajando a través de las capas se agregan encabezados y eventualmente una cola a los datos con información correspondiente a cada capa. Estos agregados contienen información de control para asegurar la entrega de los datos y la correcta interpretación de los mismos en el receptor. Una vez que se reúna la información de todas las capas, se convierten en bits y son enviadas por el medio físico. En la Figura 3.2 puede verse como se van acoplando las PDUs a medida que se avanza hacia abajo en el Modelo OSI.

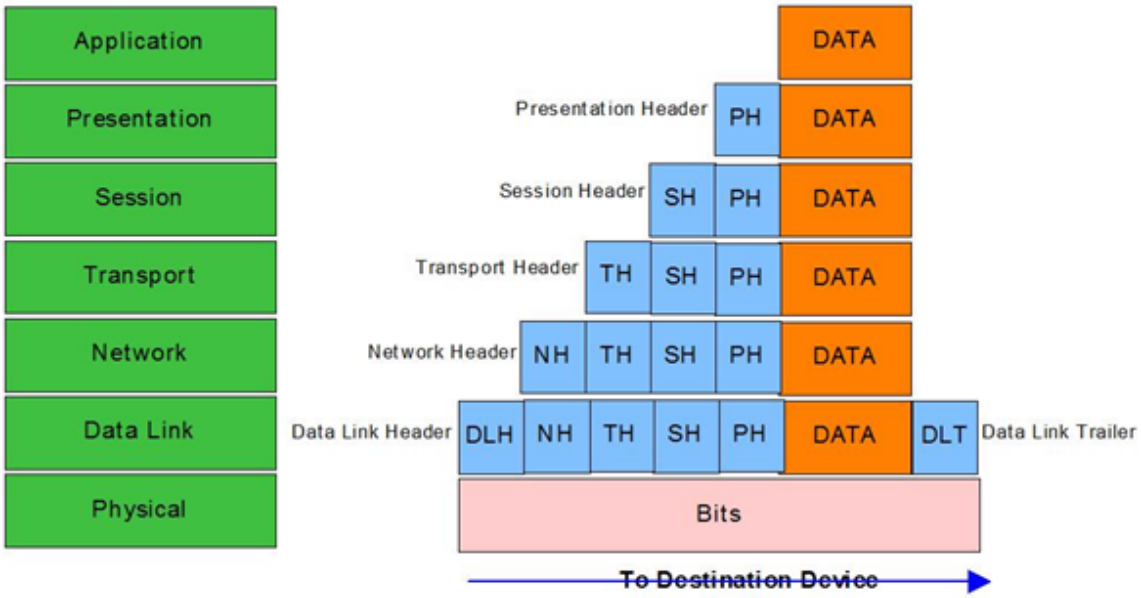

Figura 3.2: Encapsulamiento en el Modelo OSI, extraída de [12]

2. Establecimiento, control y cierre de la conexión.

3. Control de Flujo: Asegurar que la velocidad de los datos no sature las posibilidades particulares de cada capa.

4. Control de Errores: Detección y corrección de errores.

5. Multiplexación: Posibilidad de compartir el canal entre varias conexiones.

6. Encriptación y compresión.

3.3. TCP/IP

El conjunto de protocolos TCP/IP permite que computadoras de distintos tamaños, marcas, y diferentes sistemas operativos puedan lograr una comunicación entre sí [47]. Su desarrollo comenzó hacia los años 60', y en los 90' se convirtieron en los protocolos más utilizados en las redes. Conforma la base de Internet, la WAN[2] que conecta millones de dispositivos en todo el planeta.

[2]Wide Area Network, Red de Área Amplia

Tiene un diseño en capas similar al del Modelo OSI (ver Sección 3.2), en donde cada capa provee una funcionalidad diferente para la comunicación. El modelo posee 4 capas, aplicación, transporte, red y enlace, como puede verse en la Figura 3.3.

Figura 3.3: TCP/IP

3.3.1. Las Capas

1. Aplicación

   En esta capa se manejan los detalles de una aplicación particular. Aquí se encuentran protocolos muy conocidos tales como HTTP (Hipertext Transfer Protocol), HTTPS (Hipertext Transfer Protocol Secure), FTP (File Transfer Protocol), POP (Post Office Protocol), SMTP (Simple Mail Transfer Protocol), SNMP (Simple Network Management Protocol), Telnet (para login remoto), DNS (Domain Name System) [34].

2. Transporte

   Provee el servicio de envío de flujo de datos entre dos hosts. En esta capa se encuentran 2 protocolos muy importantes:

   TCP (Transfer Control Protocol):

   Permite crear conexiones entre hosts para el envío de flujos de datos. Se ocupa de dividir los datos que vienen de la capa de aplicación en paquetes de un tamaño adecuado para realizar el envío en las capas inferiores. También se encarga del control de la recepción de los paquetes enviados, así también como el establecimiento de los tiempos de espera para asegurarse que el otro extremo reconoce los paquetes enviados. Realiza la multiplexación de la conexión, es decir, que permite compartir el canal entre varias conexiones.

   Para establecer la conexión entre los 2 extremos, el servidor debe dejar en "escucha" una dirección en un puerto determinado. El cliente, envía un mensaje SYN[3] inicial al servidor para iniciar la negociación, el servidor contesta con un paquete SYN-ACK[4] que es contestado por el cliente por un ACK. Una vez intercambiados estos 3 mensajes, el cliente puede empezar a realizar las peticiones al servidor. Esto se llama ThreeWay Handshake (Negociación de 3 vías), y puede verse en la Figura 3.4.

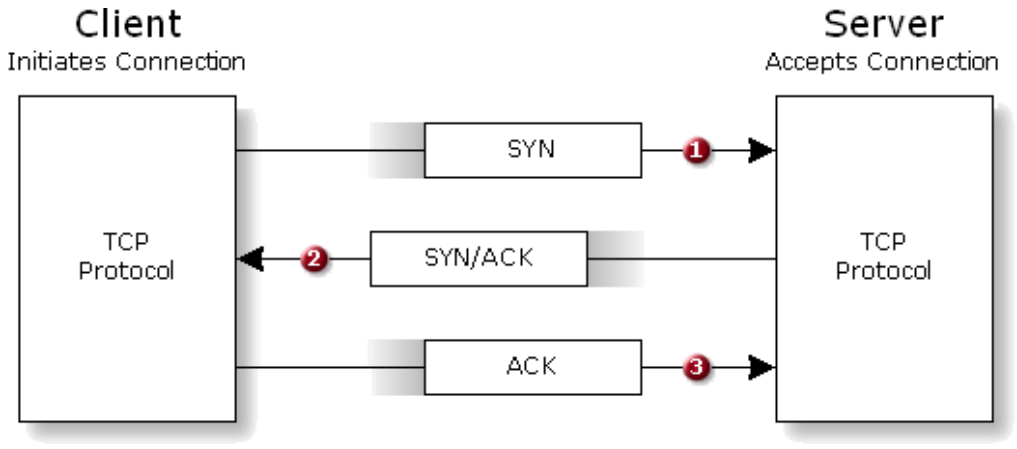

Figura 3.4: ThreeWay Handshake, extraído de https://www.grc.com/

[3] SYNchronize.
[4] ACKnowledgement.

UDP (User Datagram Protocol):

Se ocupa de enviar paquetes de datos llamados datagramas de un extremo a otro, sin realizar una conexión previa, el mismo datagrama posee suficiente información para llegar a destino. No brinda ninguna garantía de que el paquete llegue a su destino y tampoco hace control de flujo.

3. Red

   Esta capa, a veces llamada capa de Internet, maneja el movimiento de los paquetes a través de la red. El enrutamiento y encaminamiento de los paquetes tiene lugar en esta capa. El protocolo principal de esta capa es IP (Internet Protocol), define el direccionamiento de la capa de red, los campos del datagrama, y las acciones tomadas por los routers y los sistemas finales sobre el datagrama basándose en los valores de dichos campos [34]. Otros protocolos de esta capa son: ICMP (Internet Control Message Protocol) e IGMP (Internet Group Management Protocol).

4. Enlace

   Esta capa, a veces llamada capa de enlace de datos o capa de interfaz de red, incluye el driver[5] del sistema operativo y la correspondiente placa de red del dispositivo. Juntos se encargan de todos los detalles del hardware y de la interconexión física con el medio (Cable, WiFi, Fibra Óptica, etc.).

3.3.2. TCP/IP y el Modelo OSI

Similitudes

1. Ambos se dividen en capas.
2. Ambos tienen Capa de Aplicación, pero ofrecen servicios diferentes.
3. La capa de transporte y la de red son similares.
4. La conmutación es por paquetes[6] (no por circuitos).

[5] Controlador de Dispositivo

[6] Método de envío de datos, cada paquete posee datos e información de control que indica la ruta a destino.

Diferencias:

1. En la capa de aplicación de TCP/IP se combinan las capas de presentación y de sesión del Modelo OSI.
2. En la capa de enlace de TCP/IP se combinan las capas de enlace y de física del Modelo OSI.
3. Al tener menos capas, TCP/IP es más simple.
4. TCP/IP es el estándar de Internet, las redes no se desarrollan a partir del Modelo OSI, se utiliza como guía.

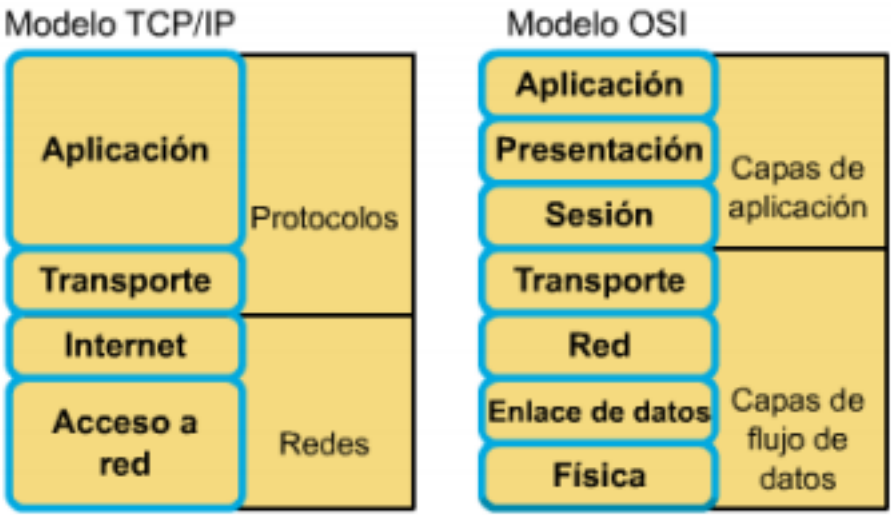

Figura 3.5: Comparación entre TCP/IP y OSI

3.4. HTTP

Las siglas de este protocolo son por HyperText Transfer Protocol (Protocolo de Transferencia de Hipertexto). Es un protocolo de capa de aplicación (ver Sección 3.2) que sirve para distribuir información. Fué utilizado en la web desde el año 1990 en su primera versión (0.9), en la que simplemente se podía transferir texto plano. Su evolución fue el estándar 1.0 en el que se mejoró el protocolo permitiendo que los mensajes usen el formato MIME - Multipurpose Internet Mail Extensions, se incorporaron metadatos acerca de la información transferida y modificadores en la semántica de petición/respuesta. La revisión del protocolo que se usa actualmente es la 1.1, definida en la RFC 2616 [15]. Contiene nuevos métodos, headers y otras características. Las principales diferencias de esta última definición se pueden ver en [33].

El contenido web reside en servidores, estos son los que se comunican utilizando este protocolo entre otros. Sirven RECURSOS, estos recursos pueden ser páginas HTML, imágenes, PDF's, video, etc, tanto contenido estático como dinámico (generado a demanda). Debido a la gran diversidad de contenido que provee un servidor, es necesario identificar el tipo de recurso que se está enviando. Esto se hace utilizando una etiqueta llamada MIME-Type, que define el tipo de contenido a transferir.

Cada recurso del servidor tiene un nombre, para que los clientes puedan apuntar directamente al recurso deseado. Se nombra con una URL, que tiene el siguiente formato:

PROTOCOLO://SERVIDOR/PATH_AL_RECURSO/RECURSO

El funcionamiento básico es, el cliente envía una petición al servidor (al puerto 80 por defecto) y este le responde. Esta comunicación se realiza a través de mensajes HTTP. Existen diferentes métodos que se pueden utilizar cuando se envía una petición al servidor, tales como

1. GET - El cliente solicita un recurso específico del servidor.
2. POST - El cliente envía datos que van a ser utilizados por el servidor.
3. HEAD - El cliente solicita sólo los headers (se detallarán más adelante).

Estos son algunos de los métodos, hay otros tales como PUT, DELETE, etc. Según el método, el servidor opera de manera diferente. En la petición se envía el método, el recurso solicitado, la versión del protocolo utilizado, el host, el user-agent[7], entre otros. El servidor, responde a la petición con una respuesta, que contiene un código de estado de 3 dígitos que le dice al cliente que la petición fue exitosa u otras, por ejemplo 200 (OK) o 404 (Documento no encontrado) de los más comunes.

Los mensajes de HTTP consisten en peticiones y respuestas, sus formatos son similares. Consisten en 3 partes:

1. Linea Inicial - Se indica que hacer en la petición o que fue lo que pasó en la respuesta.

2. Headers - Acá se pueden definir diferentes parámetros por cáda línea con la sintaxis "nombre:valor".

3. Cuerpo - Esta parte contiene los datos enviados, ya sea del cliente al servidor o viceversa.

El formato de una petición es el siguiente:

<método> <url del recurso> <versión>

<headers>

<cuerpo>

El formato de la respuesta es el siguiente:

<versión> <estado> <descripción del estado>

<headers>

<cuerpo>

[7]Quién está generando la petición, por ejemplo Mozilla, Safari, Squid (browser, proxy, etc.).

3.4.1. HEADERS

Los headers, añaden información adicional a las peticiones y respuestas. El protocolo define varios headers, pero se pueden inventar también, los servidores y clientes son libres de hacerlo. Hay diferentes tipos de headers, entre los que se encuentran:

1. Headers generales

   Pueden aparecer en peticiones y respuestas.

2. Headers de peticiones.

   Proveen más información acerca de las peticiones.

3. Headers de respuesta.

   Proveen información acerca del recurso del mensaje.

4. Headers de extensión

   Permite agregar nuevos headers que no estén dentro de la especificación estándar [15].

La definición completa de los headers se encuentra en la Sección 14 de [15].

3.5. HTTPS

Los usuarios de Internet, utilizan la web para hacer transacciones que requieren que el nivel de seguridad sea fuerte. Operaciones como realizar transacciones bancarias o hacer compras online, no se realizarían si los datos que el usuario envía al servidor viajan desprotegidos. Ante esta necesidad, se combina el protocolo HTTP con la tecnología de encriptación digital. HTTPS es la versión "segura" de HTTP, añade a este protocolo, una capa de cifrado utilizando SSL [8] (el predecesor de TLS[9]) sobre TCP, como se puede ver en la Figura 3.6. Se define en la RFC 2818 [8]. Se distingue el tráfico seguro del inseguro por la utilización de un número de puerto diferente.

[8]Secure Sockets Layer.
[9]Transport Layer Security.

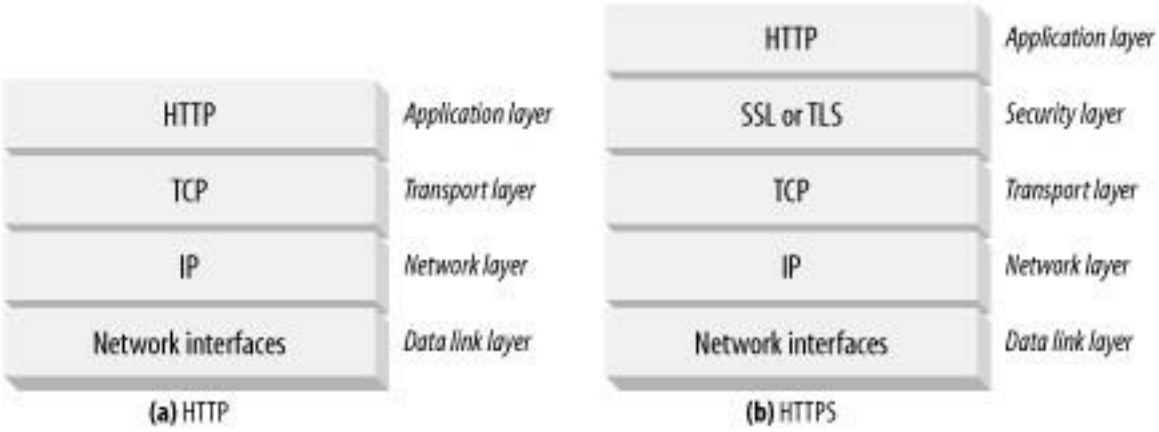

Figura 3.6: Comparación entre HTTP y HTTPS, extraído de [29]

Permite que los datos que viajan entre cliente y servidor vayan encriptados, esto se hace antes de enviar los datos por la red. Se distingue fácilmente porque el formato de la URL empieza con https:// y la conexión por defecto se establece con el puerto 443. Es decir, si el browser hace una petición a un servidor, en la cual, el esquema es https, se inicia la negociación para establecer la conexión segura con el mismo.

La conexión se hace con otro puerto diferente al de HTTP ya que SSL es un protocolo binario, completamente diferente. Si ambos llegaran al mismo puerto, los servidores interpretarían SSL como HTTP erróneo y cerrarían la conexión.

3.5.1. Criptografía

La criptografía es el arte y la ciencia de codificar y decodificar mensajes, alterando la representación linguística de mensajes, buscando la confidencialidad y para prevenir la manipulación de los mismos. También se utiliza para probar quien fue el autor del mensaje o una transacción (no repudio).

Se basa en algoritmos de cifrado (Ciphers) que tienen un método para codificar el mensaje y otro para decodificarlo posteriormente. Comenzaron siendo algoritmos simples hasta que se empezaron a construir máquinas[10] para reforzar la seguridad de la encriptación haciendo operaciones más complejas. A causa de que estos algoritmos y máquinas podían llegar a manos no apropiadas, se incluyeron diversos métodos

[10]Ver Máquina Enigma Alemana, http://www.bbc.co.uk/history/topics/enigma

(llaves metálicas, diales de configuración), que actúan como entrada para que el algoritmo o máquina pudiera funcionar. De esta manera, aún teniendo el algoritmo o dispositivo, sin la clave no se puede decodificar.

En la era digital, los métodos (clave) para la entrada de los algoritmos de encriptación son simplemente números. Estos algoritmos son funciones que toman una porción de datos y la codifican/decodifican basados en el algoritmo de encriptación y la clave proporcionada.

Criptografía Simétrica

La criptografía puede ser simétrica, es decir, que la clave para encriptar y desencriptar el mensaje es la misma. De esta manera, tanto el emisor como el receptor deben intercambiarse previamente la clave, antes de comenzar la comunicación.

El algoritmo más conocido de criptografía simétrica es el DES (Data Encryption Standard) [46]. Se trata de un algoritmo que utiliza claves de 56 bits para cifrar/descifrar bloques de datos de 64 bits. El uso de múltiples claves conduce al algoritmo Triple-DES, en el que DES se aplica 3 veces, consiste en 3 claves de 56 bits que se utilizan sucesivamente en los datos a cifrar/descifrar como puede verse en la Figura 3.7.

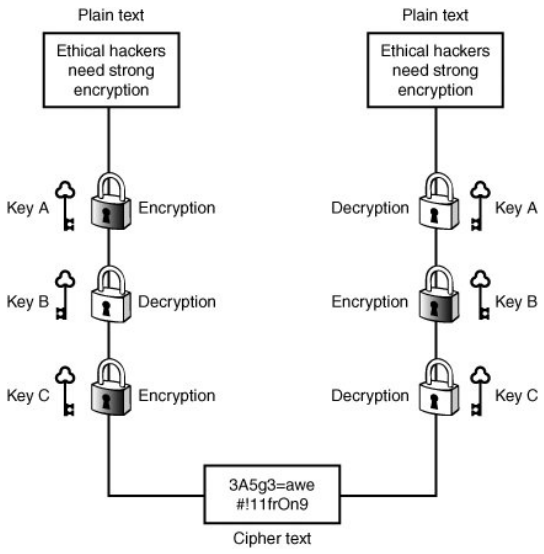

Figura 3.7: Algoritmo Triple-DES, extraído de http://flylib.com/

Criptografía Asímetrica

En la criptografía de clave pública (ver Figura 3.8), las claves son asimétricas, es decir, que la clave para encriptar difiere de la clave para desencriptar el mensaje. En este tipo de criptografía, la clave para encriptar el mensaje es pública, cualquiera que quiera establecer una conexión con seguridad, puede obtener la clave[11] para iniciar la comunicación. Por otro lado, la clave para desencriptar los mensajes es privada, pertenece al servidor que es el único que puede decodificar los mensajes recibidos por el cliente.

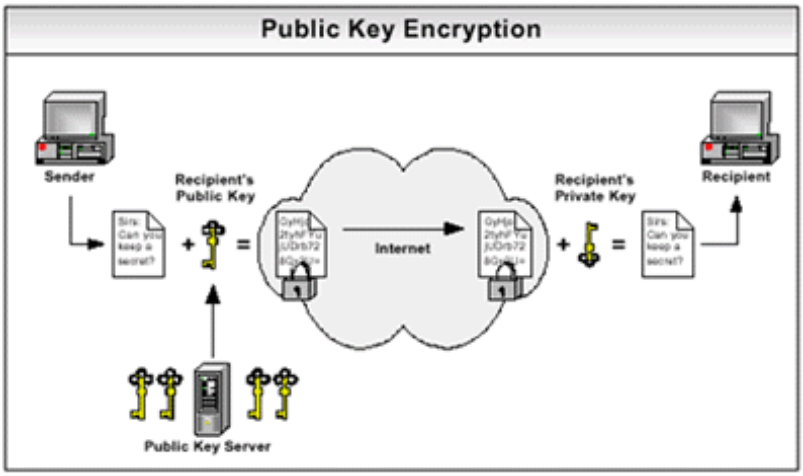

Figura 3.8: Criptografía de Clave Pública, extraído de http://www.novell.com/

RSA (Rivest, Shamir y Adleman) [43] es un algoritmo asimétrico que se utiliza en firma digital[12]. La clave utilizada para cifrar es diferente (pero relacionada) a la que se utiliza para descifrar. El algoritmo consta de los siguientes pasos:

1. Se seleccionan 2 números primos p y q.

2. Se calcula el producto de ambos números $n = p * q$, este número se llama *módulo*.

3. Se elige un número entero e tal que $1 < e < (p-1)*(q-1)$.

[11] Almacenada en servidores de acceso público.

[12] Mecanismo criptográfico que permite al receptor del mensaje poder determinar la entidad del emisor y confirmar que el mensaje no ha sido alterado desde que fue firmado.

4. Se calcula $d = e^{-1}$ *mod[(p-1)*(q-1)]*.

La clave pública es el par de números (n,e) y la clave privada es el par de números (n,d).

Para encriptar un mensaje m se calcula:

$$c \equiv m^e \pmod{n}$$

Para desencriptar un mensaje c se calcula:

$$\equiv c^d \pmod{n}$$

3.5.2. Conexión

Una conexión es una sesión de intercambio entre dos procesos en la cual ambos ha acordado y coordinado acciones para dicho intercambio. Esto incluye una etapa de establecimiento o apertura de la conexión, una de transferencia y finalmente, una de cierre.

El procedimiento para iniciar una comunicación HTTPS es el siguiente: El cliente abre una conexión con el puerto 443 al servidor. Una vez que la conexión TCP está establecida, el cliente y el servidor inicializan la capa SSL negociando algunos parámetros criptográficos e intercambiando llaves. Una vez concluida esta negociación, ya pueden empezar a intercambiar mensajes encriptados. Se puede ver en detalle en la Figura 3.9.

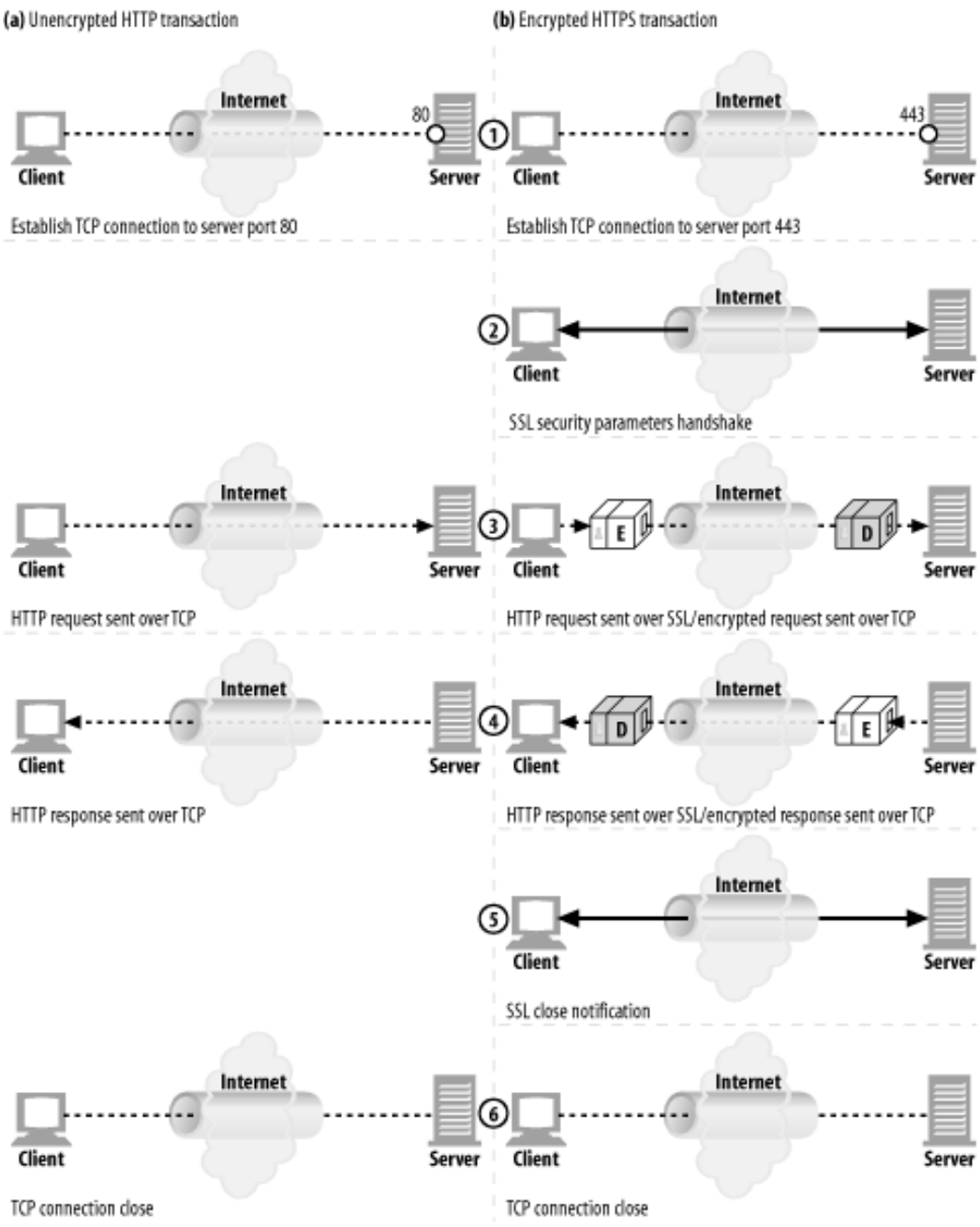

Figura 3.9: Establecimiento de Conexiones HTTP y HTTPS, extraído de [29]

Capítulo 4

Problemáticas asociadas a la Web

4.1. Introducción

Debido al crecimiento de Internet visto en el Cápitulo 2 y a los problemas que presenta el protocolo HTTP en su implementación (visto en el Cápitulo 3), mejorar los tiempos de carga de los sitios web es clave. Un estudio realizado por Akamai[1] [24], concluye:

1. El 47 % de las personas esperan que una página tarde 2 segundos o menos en cargarse. Ver Figura 4.1.

2. El 40 % de las personas, abandonan el sitio si este tarda más de 3 segundos en cargar. Ver Figura 4.2.

3. El 52 % de los compradores online, afirman que una carga rápida del sitio es importante para la lealtad con el mismo.

4. El 14 % va a comenzar a hacer compras en un sitio diferente si la carga de las páginas es lenta, el 23 % dejará de comprar.

5. De los compradores insatisfechos con el sitio, el 64 % visitará otro sitio la próxima vez.

[1] http://www.akamai.com/

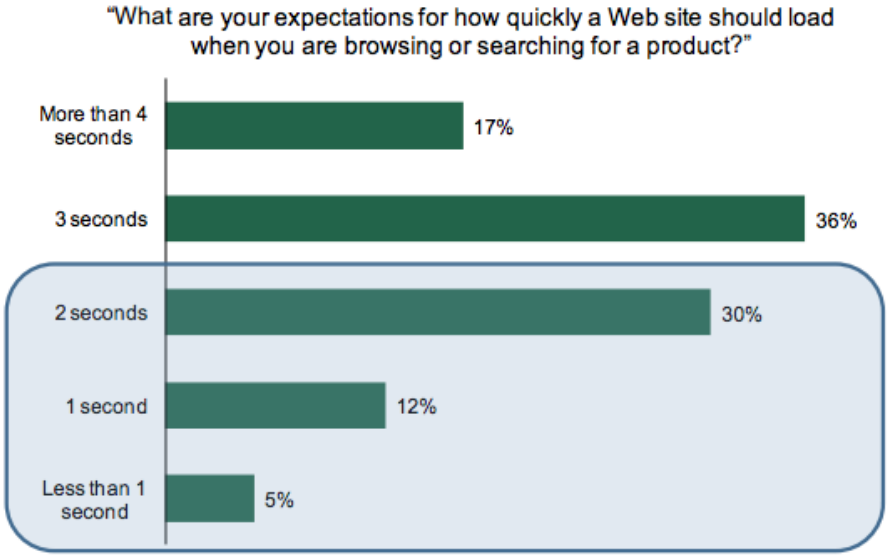

Figura 4.1: Expectativa del tiempo de carga de un sitio, extraído de [24]

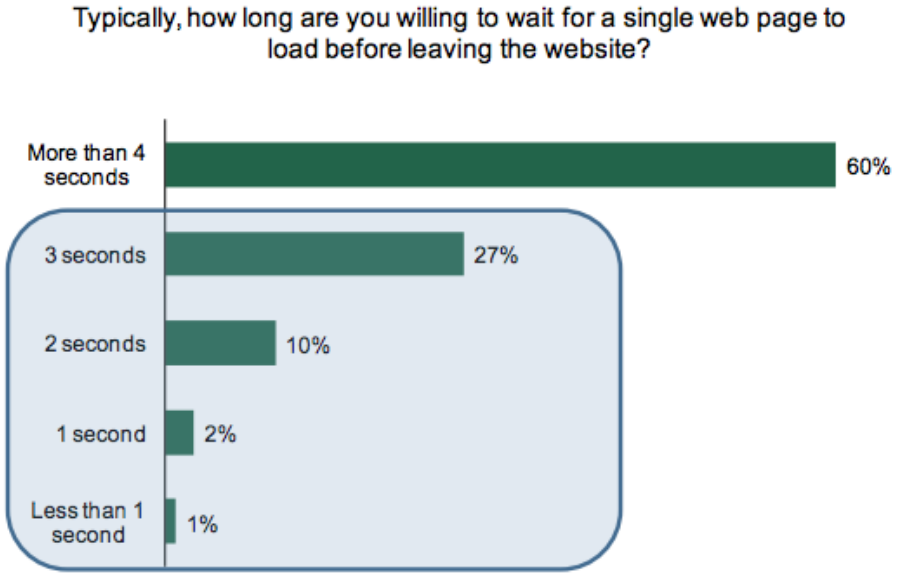

Figura 4.2: Tiempo máximo de espera antes de abandonar el sitio, extraído de [24]

4.2. Performance

Cada aplicación se desarrolla con los requerimientos del modelo de negocio, el contexto, las expectativas de los usuarios y la complejidad de la tarea. A causa de esto, hay que planificar y diseñar, centrándose en el usuario, y su percepción del tiempo de procesamiento [31]. Los tiempos de reacción de las personas son constantes, independientemente del tipo de aplicación o dispositivo utilizado, puede verse en la tabla siguiente:

Retardo	Percepción del Usuario
0-100ms	Instantánea
100-300ms	Retraso pequeño perceptible
300-1000ms	La máquina se encuentra procesando
1,000+ ms	Distracción en lo que se está realizando
10,000+ ms	La tarea es abandonada

Percepción del usuario ante los retardos, extraído de [31].

Para que la experiencia del usuario sea positiva, el sitio debe renderizarse, o al menos tener una respuesta visual de que el sitio se está cargando, en al menos 250 milisegundos.

En agosto del 2010, Mike Belsche[2] publicó un estudio [22] acerca de 2 factores importantes en el tiempo de carga de los sitios, ancho de banda y RTT. El RTT[3] es el tiempo que demora un paquete en ir del emisor al receptor y volver al emisor nuevamente. Realizó 2 experimentos, el primero variando el ancho de banda y el segundo variando el RTT.

En el Gráfico 4.3 puede observarse el resultado del primer experimento, al aumentar el ancho de banda hay mejoras en el tiempo de respuesta en los valores más bajos, pero, a partir de cierto ancho de banda, el aumento no produce mejoras en el rendimiento.

[2]Ingeniero de Software, fué uno de los desarrolladores del protocolo SPDY (ver Sección 4.8) - https://www.belshe.com

[3]Round Trip Time

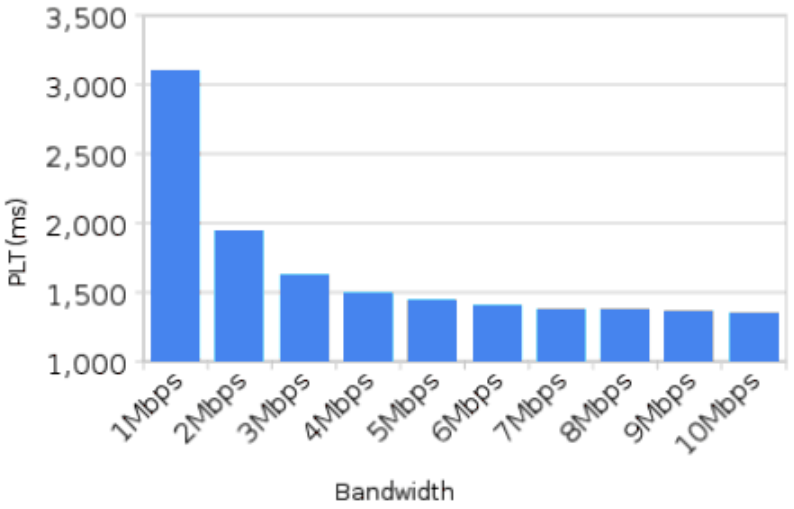

Figura 4.3: Latencia por ancho de banda, extraído de [22]

En cambio, en el Gráfico 4.4, se ve claramente que a medida que el RTT se va reduciendo, también lo hace el tiempo de carga del sitio, incluso cuando ya el RTT es bajo.

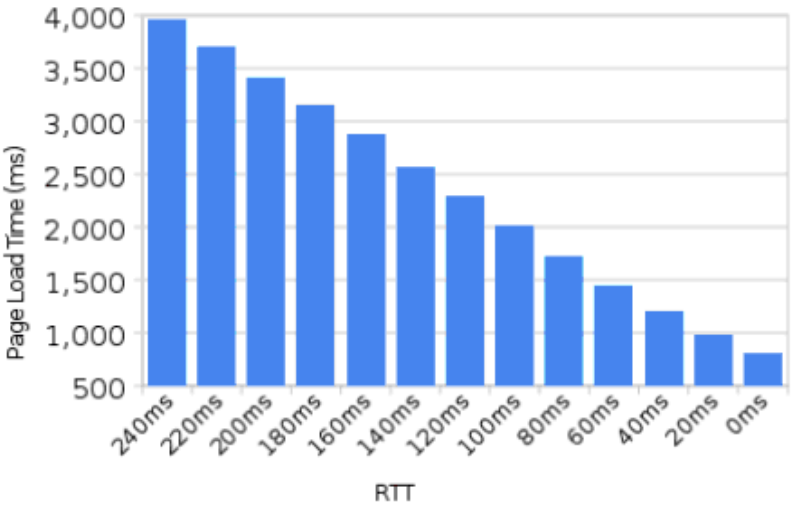

Figura 4.4: Tiempo de Carga de un sitio a medida que el RTT se decrementa, extraído de [22]

La conclusión del estudio de Belshe es que, si se duplica su ancho de banda sin reducir el RTT significantemente, sólo se obtiene una mejora mínima en la navegación. Disminuir el RTT, sin importar el ancho de banda utilizado, siempre supone una mejora en la velocidad. Para acelerar Internet, o bien hay que ocuparse de reducir el RTT, o reducir la cantidad de RTT's requeridos para cargar un sitio.

Es importante también conocer, dónde es que el usuario pasa el tiempo esperando en la carga de un sitio web. Según el estudio de Steve Souders en su libro [45], el cliente tarda menos del 20 % para obtener el documento HTML, y el tiempo restante para recibir el resto de los componentes del sitio. Es importante enfocarse en el 80 %, 90 % restante, ya que el tiempo no se desperdicia en descargar el documento HTML ni en el procesamiento que realiza el servidor antes de enviarnos la petición. Esto se resume en la "Regla de oro de la performance" de dicho libro:

> *"Solo el 10-20 % del tiempo de respuesta del usuario es consumido descargando el documento HTML. El otro 80-90 % se consume descargando todos los componentes de la página."*

4.3. Técnicas de optimización

Souders [45], plantea 14 reglas para la optimización de los sitios que se describen a continuación.

1. **Minimizar la cantidad de peticiones.**

   La idea básica es eliminar las peticiones al servidor, esto se hace utilizando varias técnicas enumeradas a continuación.

   a) Mapa de Imágenes - Permite asociar múltiples áreas en una imagen para que se puedan cliquear y realizar cierta acción (el ejemplo más básico es el de navegar un hipervínculo). En vez de utilizar múltiples imágenes para realizar un menú por ejemplo, se utilizaría una sola mapeada. De esta manera se ahorran las peticiones de las imágenes por 1 sola petición.

b) CSS Sprites - Permite combinar várias imágenes en una sola, luego en el sitio, se define que parte de la imagen combinada desea mostrarse. Por ejemplo, en el sitio de Google cuando se realiza una búsqueda, se utiliza el sprite que se ve en la Figura 4.5.

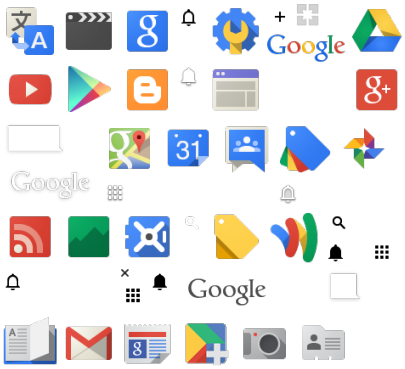

Figura 4.5: Sprite del sitio www.google.com

A simple vista se ven 44 imágenes combinadas. La utilización de este sprite reduciría todas estas peticiones a 1 sola.

c) Imágenes Inline - Se pueden incluir imágenes en un sitio web sin necesidad de realizar una petición al servidor definiéndolas con el esquema *data:* [1] dentro del código HTML de la página.

d) Combinar Scripts y Hojas de Estilo - Como la mayoría de los sitios actuales utilizan Javascript y CSS[4], es preferible que los scripts se combinen en uno solo al igual que las hojas de estilo. En el caso de tener varios archivos, el navegador va a generar una petición por cada uno de ellos de no tenerlo almacenado en una copia local.

2. **Utilizar un CDN**[5]

La proximidad del cliente al servidor web tiene un impacto en el tiempo de respuesta de las peticiones. No es lo mismo solicitar un recurso localizado en China estando en Argentina que uno ubicado dentro del mismo país. Por ende,

[4]Cascade Style Sheets.
[5]Content Delivery Networks.

si los contenidos están cerca[6] el tiempo de respuesta es menor. Debido a que solo el 10-20 % del tiempo de respuesta se dedica al HTML (visto al inicio de este capítulo), si el resto de los recursos del sitio se encuentran cerca del cliente, se mejorarían los tiempos de respuesta. Para esto es necesario dispersar estos recursos geográficamente.

Un CDN es una red de distribución de contenidos. Son servidores dispersados geográficamente que ofrecen réplicas de los recursos de un sitio particular para brindarlos al cliente desde el más cercano a su locación.

Utilizar el servicio que brinda un CDN mejora los tiempos de respuesta de los usuarios.

3. **Añadir Headers para Cachés**

   Cuando un usuario visita el sitio por primera vez, realiza tantas peticiones HTTP como recursos tenga la página. Utilizando headers Expires o Cache-Control[7] (Capítulo 3, Sección 3.4.1) se puede hacer que los recursos puedan ser almacenados en cachés (Capítulo 6.). Esto disminuye la cantidad de peticiones en una posterior visita a la página del mismo usuario.

   La performance del tiempo de respuesta del sitio mejora según la cantidad de "hits"[8] que el usuario tenga de los componentes del sitio.

4. **Comprimir los componentes (Gzip)**

   Se puede reducir el tiempo de respuesta, disminuyendo el tamaño de la respuesta HTTP. Esto se puede realizar comprimiendo el recurso que se está solicitando. La reducción del tiempo es mayor en ambientes en donde el ancho de banda es bajo. El formato *Gzip*[9] [7] es el más popular y el más efectivo, el otro formato que se usa con menos frecuencia es *deflate* [2].

   El usuario tiene que enviar en la petición un header *Accept-Encoding* indicando los métodos aceptados. Cuando el servidor recibe este header, puede comprimir el recurso utilizando alguno de los métodos indicados por el usuario. Este

[6] En términos de distancia física.
[7] Desde HTTP 1.1
[8] Necesidad de solicitar un recurso que ya tengo almacenado en la caché.
[9] http://www.gzip.org/

devuelve la respuesta con un header *Content-Encoding* indicando el tipo de compresión utilizado en el recurso que se está enviando.

Los tipos de archivos que se deberían comprimir son aquellos de texto, tales como HTML, scripts, CSS, etc. Aquellos formatos que ya se encuentran comprimidos como las imágenes o los archivos PDF[10] no deberían comprimirse ya que se desperdicia tiempo de CPU del servidor[11] y además puede incluso incrementar el tamaño del archivo.

5. **CSS en la parte superior del HTML**

   Las hojas de estilo deben incluirse en la parte superior del HTML. De esta manera, los navegadores pueden ir renderizando la página a medida que van llegando las respuestas de las peticiones. Esto es importante en términos de usabilidad, para brindarle un medio visual [12] al usuario que está esperando el sitio.

6. **Scripts en la parte inferior del HTML**

   Cuando se realizan las peticiones al servidor, las descargas pueden hacerse en paralelo con ciertos límites[13], eso claramente es beneficioso, ya que al paralelizar las descargas, el tiempo es menor comparado con descargas secuenciales. En el caso de los scripts, esta característica se deshabilita por 2 motivos, uno es que si es script altera contenido de la página, el navegador debe esperar a recibirlo para mostrar el contenido correctamente. El otro motivo es que el navegador debe respetar el orden de ejecución de los scripts, si estos vinieran en paralelo, no se puede asegurar que su ejecución tenga el mismo orden en el que se solicitaron.

[10] Portable Document Format.
[11] Para realizar la compresión.
[12] Carga progresiva del sitio.
[13] 2 según la especificación HTTP 1.1, hasta 6 según el navegador.

7. **Evitar expresiones en CSS**

   Las expresiones en CSS se encuentran obsoletas[14] en los navegadores modernos. Afectaban directamente a la performance de la renderización del sitio una vez que todos los componentes eran recibidos.

8. **Utilizar JavaScript y CSS de manera externa (no embebido en el HTML)**

   Al embeber los scripts y el estilo en el HTML, se minimiza la cantidad de peticiones al servidor, pero se aumenta el tamaño del archivo HTML. Incluir archivos externos al HTML, permite a los navegadores y proxies que puedan almacenar en su caché el objeto. Esto es útil ya que si en todas las páginas del sitio se utilizan el mismo Javascript y CSS, al ir navegando las diferentes páginas del sitio, estos recursos ya están almacenados en el navegador. También disminuye el tiempo de respuesta en visitas posteriores.

9. **Reducir las búsquedas de DNS**[15]

   Cada servidor tiene una dirección IP asignada, esta dirección se encuentra asociada a un nombre de dominio, esto se almacena en los DNS. Cuando se ingresa un nombre de un sitio en el navegador, este necesita la dirección IP asociada a ese dominio. Para ello necesita solicitar esa asociación a un DNS Resolver, antes de empezar a solicitar los recursos debe esperar la respuesta del DNS. Esto al igual que los recursos se almacenan en una caché local del navegador. A raíz de esta cuestión, tener menos dominios en las URL's de los componentes de una página, requiere menos peticiones (DNS lookups) a los servidores que almacenan los dominios para solicitar las direcciones IP que corresponden a esos dominios.

10. **Minificar el JavaScript**

    La minificación, es la práctica de remover caracteres innecesarios del código para reducir el tamaño del archivo. Se quitan los comentarios, los espacios en blanco (tabulaciones, espacios, saltos de línea). Una optimización alternativa

[14] http://blogs.msdn.com/b/ie/archive/2008/10/16/ending-expressions.aspx
[15] Domain Name System.

tiene el nombre de ofuscación, además de lo que hace la minificación, renombra las variables del código por cadenas de texto más pequeñas. Este método disminuye aún más el tamaño de los archivos, que el método visto anteriormente. Con esta optimización se mejora el tiempo de respuesta ya que los recursos tienen menor tamaño.

11. **Evitar redirecciones**

    Una redirección es utilizada para enrutar a los usuarios de una URL a otra. Generalmente se utilizan para documentos HTML, pero, ocasionalmente, también cuando se peticionan componentes de la página. Los retrasos ocasionados por una redirección retrasan directamente el documento HTML completo. Insertar una redirección entre el usuario y el HTML retrasa todo en el sitio.

12. **Remover scripts duplicados**

    Incluir archivos Javascript más de una vez en un sitio, afecta directamente la performance por 2 factores, peticiones innecesarias y tiempo de procesamiento innecesario del script.

13. **Configurar Etags**

    Los Etags son cadenas de texto únicas que identifican una versión específica de un componente (ver Capítulo 6, Sección 6.4) . Provee un mecanismo para poder realizar una petición condicional al servidor, comparando el Etag de la copia local con el del servidor. En el caso de que el valor coincida con el del servidor, la respuesta devuelve un código (ver 3.4) que indica que el recurso está fresco (ver 6), de esta manera, se reduce notablemente el tamaño de la respuesta y el tiempo ya que viaja por la red solamente los headers.

    Hay ciertas cuestiones referidas a la utilización de los Etags. Por un lado, en el caso de un cluster de servidores, los Etags generados por los mismos, no son iguales entre ellos. En este caso, si se realiza una petición condicional, a pesar de que el componente es igual, al no coincidir los Etags, el recurso es devuelto al usuario. Otra cuestión es que la petición condicional *If-None-Match* toma precedencia ante *If-Modified-Since*, según la especificación del protocolo HTTP 1.1 si ambos headers se encuentran en la petición, ambas condiciones

se tienen que cumplir para devolver un código 304. Por todas estas cuestiones, se recomienda, o bien configurar los Etags de manera que las peticiones sean precisas, o quitarlos.

4.4. SPDY

4.4.1. Introducción

SPDY es un protocolo experimental desarrollado por Google a mediados del 2009, cuya meta principal es reducir los tiempos de carga de los sitios enfocándose en las limitaciones de HTTP (ver 3.4). Específicamente se busca lo siguiente [31]:

1. Reducir el Tiempo de Carga de los Sitios.

2. Evitar la necesidad de que los desarrolladores tengan que realizar cambios a los sitios actuales.

3. Evitar cambios en la infraestructura de las redes y minificar la complejidad de implementación.

4. Liberar el desarrollo a la comunidad de código abierto.

5. Recopilar datos reales de rendimiento para validar o invalidar el protocolo experimental.

Desde el año 2012 el protocolo es soportado por los navegadores Chrome[16], Mozilla Firefox[17], y Opera[18]. Existen varias opciones de servidores que soportan el protocolo tales como Apache[19], Jetty[20] y NodeJS[21]. Varios sitios populares (Google, Facebook, Twitter) ya ofrecen un cliente para la utilización del protocolo.

[16] http://www.google.com/intl/es_AR/chrome/browser/
[17] http://www.mozilla.org/es-AR/firefox/new/
[18] http://www.opera.com/
[19] http://code.google.com/p/mod-spdy/
[20] http://wiki.eclipse.org/Jetty/Feature/SPDY
[21] https://github.com/indutny/node-spdy

4.4.2. Detalles del Protocolo

Es un protocolo que añade una capa de sesión que funciona sobre SSL (ver Figura 4.6) que permite la transmisión de múltiples streams[22] sobre una conexión TCP. Especifica un nuevo formato de trama para codificar y transmitir datos. Su especificación se puede ver en [16] y su draft se puede encontrar en [17].

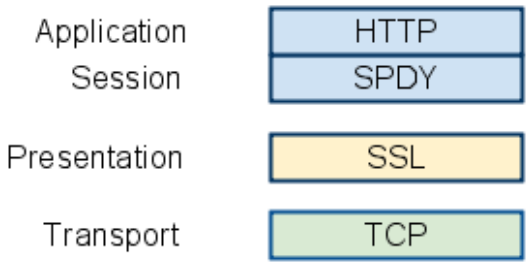

Figura 4.6: Protocolo de aplicación SPDY, extraído de [16]

El protocolo HTTP no tiene estado, y, por cada recurso que requiera existe la necesidad de abrir una conexión nueva y cerrarla. Esto trae varios problemas:

1. Por cada conexión nueva que se hace, se necesitan varios mensajes para establecer la conexión TCP, lo que trae varios RTT (Round Trip Time) adicionales a la comunicación. El RTT es el tiempo estimado para enviar y recibir un mensaje por parte del interlocutor [47], puede verse en la Figura 4.7.

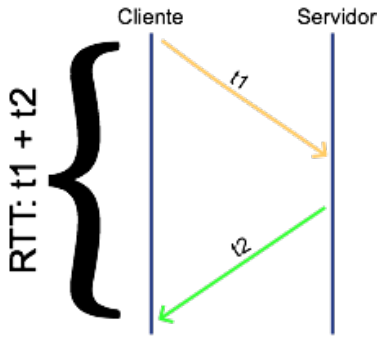

Figura 4.7: RTT

[22]Flujo de Datos.

2. Retrasos debido al "Slow Start" de TCP. Se comienza enviando un volumen de datos pequeño hasta alcanzar cierto valor llamado Umbral de Congestión.

3. Clientes que evitan realizar múltiples conexiones con el mismo servidor (hasta 6 actualmente).

4. A su vez, los servidores crean varios subdominios para almacenar el contenido para que los clientes puedan realizar las peticiones sin tener que evitar las múltiples conexiones a un mismo dominio.

El funcionamiento básico de SPDY puede verse en la Figura 4.8. Inicia la conexión con el servidor realizando el ThreeWay Handshake de TCP (ver 2), se establece una conexión segura entre ambos extremos, y luego se pueden empezar a pedir los recursos a través de la misma conexión y en paralelo.

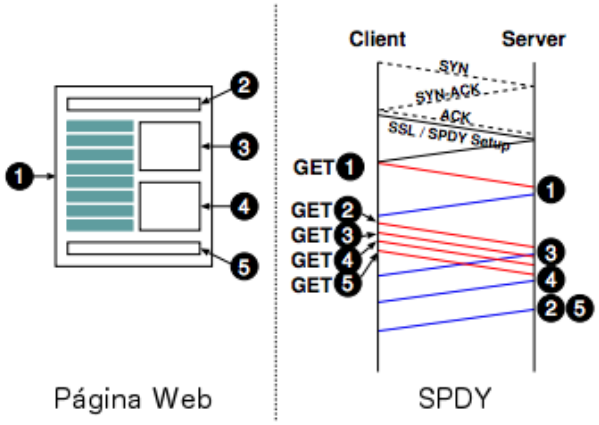

Figura 4.8: Funcionamiento de SPDY, extraído de [27]

SPDY ofrece por sobre HTTP las siguientes mejoras:

1. Peticiones Multiplexadas. No existen límites de peticiones que se pueden realizar en una sesión de SPDY. A causa de que las peticiones son multiplexadas aumenta la eficiencia del protocolo TCP.

2. Priorización de Peticiones. Los clientes pueden solicitar al servidor cuáles recursos quiere obtener antes que otros. Esto evita la congestión de recursos que no son críticos cuando todavía está pendiente el envío de algún recurso que tiene una prioridad mayor.

3. Compresión de Headers. A causa de que hoy en día los clientes envían mucha información redundante en forma de headers, como la cantidad de peticiones para obtener un sitio promedio va desde 50 a 100, esta cantidad de información es relevante. Comprimir los headers reduce el ancho de banda utilizado.

4. Server Push. Al permitir la comunicación bi-direccional a través de streams, cualquiera de los 2 (cliente o servidor) puede iniciar un stream hacia el otro. El servidor puede enviar un recurso al cliente antes de que este lo pida[23], esto reduce el tiempo de carga del sitio y disminuye la cantidad de peticiones del cliente.

5. Server Hint. El servidor puede "sugerirle" al cliente que pida un recurso en particular, ya que lo va a necesitar. De todas maneras, el servidor espera a que el cliente peticione el recurso en cuestión antes de enviarlo. Esto reduce el tiempo que tarda el cliente en descubrir cuales son los recursos que tiene que pedirle al servidor.

SPDY se enfoca en la manera en la que se transmiten los datos por la red, preserva toda la semántica del protocolo HTTP. De esta manera, para las aplicaciones se implementa de manera transparente, ya que reside entre la capa de aplicación y la de transporte. Esta sesión es similar al par petición-respuesta de HTTP. Es obligatoria la compresión del mensaje.

4.4.3. Alternativas Propuestas

Existen varias alternativas que se propusieron para mejorar la performance de Internet,

SCTP (Stream Control Transmission Protocol)

Es una alternativa al Protocolo TCP, definido en la RFC 2960 [18], provee confiabilidad, control de flujo y secuenciación, opcionalmente permite el envío de mensajes sin un orden preestablecido. Permite Multihoming, que es la capacidad de que los extremos conectados puedan tener más de una dirección IP.

[23]El servidor conoce de antemano que el cliente va a necesitar el recurso en cuestión.

HTTP sobre SCTP

Es una propuesta de utilizar HTTP sobre SCTP definida en el draft "draft-natarajan-http-over-sctp-00" [20]. El servicio de múltiples streams de SCTP es la característica que beneficia la combinación de protocolos. Las transacciones HTTP independientes cuando se transmiten sobre diferentes streams de SCTP mejoran significativamente los tiempos de respuesta.

Structured Stream Transport (SST)

Es un protocolo de transporte experimental [28] diseñado para las aplicaciones que requieren de muchas conexiones asíncronas en paralelo, tales como la descarga de las diferentes partes que componen un sitio web y reproducir simultáneamente múltiples flujos de audio y video a la vez. No realiza el ThreeWay Handshake en el inicio como TCP. Multiplexa flujos de datos de aplicaciones en una sola conexión de red. Soporta mensajes/datagramas de cualquier tamaño, no hay necesidad de limitar el tamaño de los envíos. Priorización de flujos de datos.

MUX y SMUX

MUX[24] y SMUX[25] son protocolos de capa intermedia (entre la capa de transporte y la capa de aplicación) que proporcionan la multiplexación de flujos de datos. Se propusieron al mismo tiempo que HTTP/1.1.

4.4.4. Estudios Relacionados

Se han realizado diversos estudios acerca de la performance de SPDY, que arrojan diferentes resultados. Estos resultados ayudan a ver en qué condiciones la utilización de SPDY realmente mejora la performance de la carga de un sitio.

Jitendra Padhye y Henrik Frystyk Nielsen, en su paper "A comparison of SPDY and HTTP performance" [42], realizaron una comparación de ambos protocolos en un ambiente controlado. Con un sitio de prueba[26], variando el RTT y el ancho de

[24] http://www.w3.org/Protocols/MUX/
[25] http://www.w3.org/TR/WD-mux
[26] index.html + 20 imágenes + 3 hojas de estilo

banda, obtuvieron los resultados que se ven en los Gráficos 4.9 y 4.10.

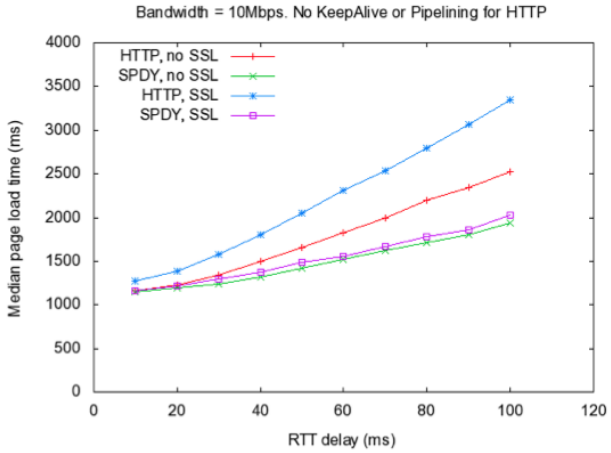

Figura 4.9: SPDY vs HTTP - 10Mbps, extraído de [42]

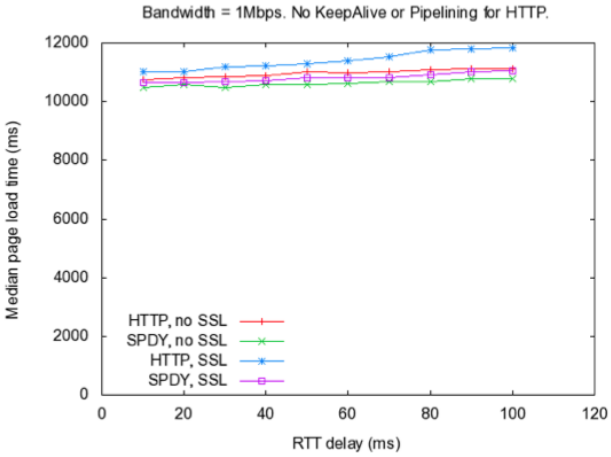

Figura 4.10: SPDY vs HTTP - 1Mbps, extraído de [42]

Claramente se observa que, con anchos de banda más limitados, el incremento de performance de SPDY es bajo (del 3 % al 8 %) frente a un ancho de banda de 10mb en el cual el incremento es de hasta 39 %. Lo cual es un indicador de que, en un ambiente en el cual la velocidad del enlace sea pobre (por ejemplo una red 3G), que causa que esté sujeto a una mayor probabilidad de pérdidas de paquetes, SPDY no funciona como lo esperado. Posiblemente a causa del alto costo de retransmisión

del flujo de datos, ya que si el Stream se pierde, se debe retransmitir todo completo ya que usa una sola conexión entre los extremos para comunicarse.

Otro estudio interesante, relacionado con los resultados del estudio anterior, es "Towards a SPDYier Mobile Web?" [27]. En este paper se estudió el rendimiento de SPDY vs HTTP en redes de celulares. También concluyen que no hay una diferencia significativa entre los protocolos estudiados en ese ambiente en particular.

En "The Effect of Network and Infrastructural Variables on SPDY?s Performance" [26] también se realiza una experimentación en diferentes ambientes, en donde se observa que con valores de RTT bajos, los beneficios de SPDY sobre HTTPS son marginales, en cambio, a medida que el valor del RTT va aumentando, los beneficios van creciendo. Este beneficio se da por la multiplexación de streams que realiza SPDY, es muy costoso para HTTPS establecer conexiones separadas para cada recurso. Otra cuestión es la pérdida de paquetes, el costo de retransmisión de SPDY es muy costoso ya que debe enviar el stream completo nuevamente, resultado similar al de [42].

En el paper "How Speedy is SPDY?" [51], se realiza una comparación de la performance de HTTP vs SPDY. Desarrollaron una herramienta para emular la carga de diferentes páginas. Utilizaron un árbol de decisión para identificar las situaciones en las que SPDY se comporta mejor que HTTP y viceversa. En conclusión, SPDY mejora de manera significativa el tiempo de caga de las páginas en ciertos escenarios en los que se ve beneficiado por la utilización de una sola conexión TCP. Pero empeora la performance en situaciones con alta pérdida de paquetes para objetos de mayor tamaño.

Capítulo 5

Proxy

5.1. Definición

Los servidores proxy son intermediarios entre el cliente y el servidor. Actúan enviando los mensajes del cliente al servidor y viceversa. En una comunicación normal, le cliente se comunica directamente con el servidor, en el caso de que en la red haya un proxy presente, el cliente se comunica con el proxy y este es el que se comunica con el servidor.

El proxy HTTP es un web server y también es cliente. Para recibir los pedidos de los clientes, tiene que actuar como un servidor y manejar correctamente las peticiones, conexiones y respuestas. A su vez, para poder conectarse a los destinos finales y recuperar los recursos que le son pedidos por el usuario del proxy, tiene que actuar como un cliente, enviando peticiones y recibiendo las respuestas. Se puede ver el funcionamiento básico de un proxy en la Figura 5.1.

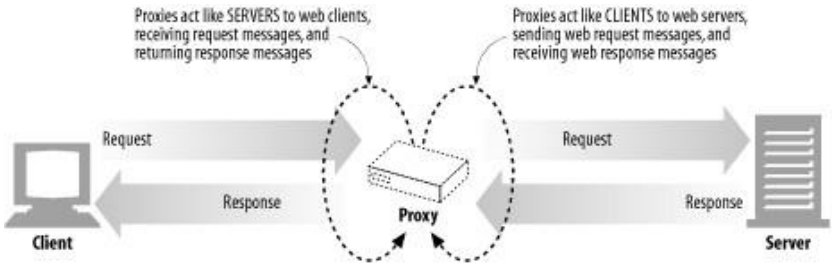

Figura 5.1: Esquema del funcionamiento de un proxy, extraído de [29]

El esquema de la Figura 5.1 muestra una conexión utilizando HTTP, las peticiones viajan directamente al proxy y de ahí al servidor final. En el caso de HTTPS se hace de manera diferente. Primero el cliente envía una petición con el método CONNECT que incluye la dirección y el puerto del destino final. El proxy autentica la conexión, completa la negociación con el destino y responde al cliente con un mensaje que contiene el código 200 que indica que la conexión fué establecida. Luego, el proxy se convierte en un túnel que solo reenvía los paquetes del cliente hacia el servidor y viceversa (todo el tráfico se encuentra encriptado). Esto puede ilustrarse en la Figura 5.2. Los browsers actuales no soportan proxies HTTP Seguros, es decir, que se establezca una sesión SSL del cliente al proxy y otra del proxy al servidor final como puede verse en la Figura 5.3. Este último punto está en discusión, se propuso un borrador [5] al respecto.

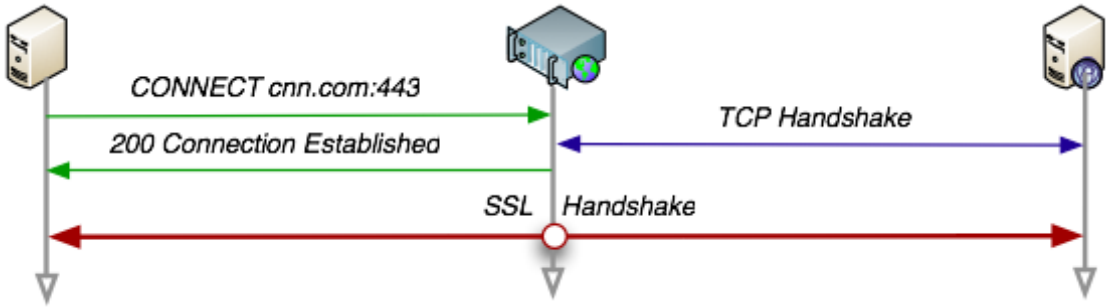

Figura 5.2: Túnel HTTPS sobre un proxy, extraído de [30]

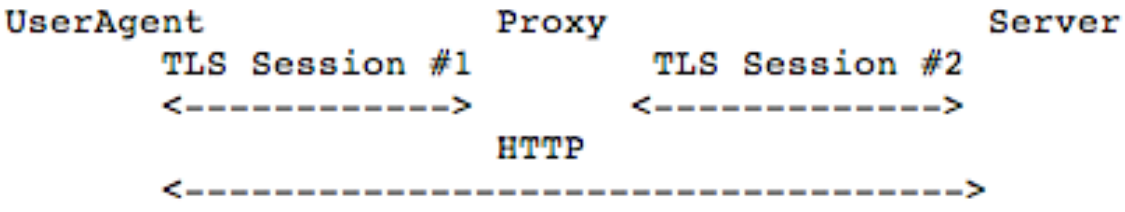

Figura 5.3: Túnel HTTPS sobre un proxy, extraído de [5]

5.2. Usos de un Proxy

Hay diversas utilizaciones de los servidores proxy, entre ellas se destacan:

1. Proxy NAT[1] / Enmascaramiento

   El enmascaramiento IP o también llamado traducción de direcciones de red, es el proceso por el cual las direcciones IP del origen/destino son reescritas, se sustituyen por otras. Es útil cuando se dispone de una única dirección pública que se comparte entre varios usuarios. El proxy se encarga de enmascarar las direcciones privadas de los clientes, traduciendolá a la dirección pública, para realizar las peticiones al exterior. Cuando recibe la respuesta de los servidores exteriores, se encarga de derivarla al usuario que inició el pedido.

2. Filtro

   El proxy al recibir las peticiones de los clientes, puede permitir o denegar esas peticiones según ciertas políticas definidas. Por ejemplo, en una Institución Educativa se podría bloquear el acceso a ciertas redes sociales o sitios para adultos.

3. Cortafuegos[2]

   Al ser un intermediario, y muchas veces como puerta de acceso hacia internet, se pueden utilizar para aumentar el nivel de seguridad restringiendo ciertos protocolos o filtrando cierto contenido inseguro por ejemplo.

4. Web Caché

   Puede utilizarse para mantener copias locales de los recursos peticionados por los clientes, y al momento de recibir una petición por un recurso que se encuentra almacenado, se brinda esa copia al cliente. Al servir varios clientes esto incrementa la velocidad de respuesta. Es uno de los usos más importantes de un proxy, ya que reduce notablemente los tiempos de carga de los sitios cuando se produce un caché hit. Esto se verá detalladamente en el Capítulo 6.

[1] Network Address Translation.
[2] Firewall.

5. Proxy Reverso / Surrogate Server

   Puede actuar delante de un servidor web, atendiendo peticiones de los clientes como si fuera él servidor mismo. Esto permite por ejemplo, generar una red de distribución de contenidos (CDN). Recibe una petición de un cliente, y, en vez de devolver el contenido directamente, inicia una comunicación con otros servidores para localizar el recurso pedido, de manera más eficiente. También protege a los servidores web, añadiendo una capa adicional de defensa. Puede distribuir la carga entre varios servidores web.

6. Content-Router

   Pueden redirigir las peticiones a diferentes servidores, basados en las condiciones del tráfico de Internet y el tipo de contenido.

7. Transcoder

   Puede modificar el contenido de los recursos antes de hacer el envío a los clientes. Por ejemplo, transformar imágenes BMP a JPEG para reducir el tamaño, comprimir archivos de texto, e incluso hacer una traducción del contenido a otro lenguaje.

8. Anonimizador

   Permite navegar de manera privada y anónima removiendo ciertos datos de los mensajes HTTP (dirección IP, From header, cookies, etc).

5.3. Ventajas y Desventajas

5.3.1. Ventajas

1. Control

   Al ser intermediario, es el proxy el único que va a realizar el trabajo de comunicación hacia el exterior, es el que tiene la potestad de limitar y restringir los derechos de los clientes, ya que todo pasa a través de él.

2. Optimización de los tiempos de carga

   En el caso de los proxies que ofrecen servicio de caché, se optimizan los tiempos de carga de los sitios, al tener almacenada copias locales que puede brindar directamente al usuario sin tener que realizar la petición al servidor final.

3. Optimización del uso de recursos

   El proxy es el único que realiza el trabajo hacia afuera, es decir, que al utilizar una sola conexión, se maximiza el uso del ancho de banda.

4. Modificación de la Información

   Al tener acceso a los recursos que viajan a través de él, tiene la posibilidad de modificarlos.

5. Filtrado

   Recibir todas las peticiones del usuario, da la posibilidad de poder decidir que recursos o qué sitios son los que están habilitados para su recuperación. Podría manejarse una lista negra[3] o una lista blanca[4] por ejemplo.

6. Tráfico controlado

   Debido a que todo el tráfico pasa a través del proxy, se puede registrar un gran volumen de información que luego puede usarse para auditoría y seguridad.

7. Anonimato

   Permite a los usuarios acceder a los servicios que brinda Internet, protegiendo la red interna. Al acceder al exterior identificándose como el mismo, es difícil para el recurso diferenciar quien es el que está realizando la petición.

[3] Listado de sitios a los que NO se puede acceder.
[4] Listado de sitios cuyo acceso está permitido.

5.3.2. Desventajas

1. Múltiples funciones

   Al estar a disposición de todas las peticiones de los usuarios, es posible que tenga que realizar algunas tareas no específicas de su función, por ejemplo los controles de acceso a sus servicios.

2. Carga de trabajo

   Al ser el intermediario de todos los usuarios, el proxy tiene que realizar el trabajo de todos ellos. La carga de trabajo crece en la medida en que crezcan la cantidad de usuarios que consumen sus servicios.

3. Confianza del Usuario

   Pueden aparecer usuarios que no se sientan cómodos con que todo su tráfico sea interceptado. Además, todas las transacciones realizadas se guardan en archivos de logs[5], es decir que toda la actividad que el usuario realice a través del proxy quedan registradas. En una conexión sin intermediarios, es imposible tener la información completa de las transacciones realizadas ya que se encuentra esparcida en servidores diseminados por todo el mundo.

4. Modificación en el Software de los usuarios

   La utilización de un proxy, requiere que las aplicaciones que interactúan con Internet que los usuarios utilizan en la red interna, se configuren (ver Sección 5.4) para que puedan tener acceso hacia el exterior a través del proxy.

5. Servicios no disponibles

   Existen algunos aplicaciones que no funcionan con un proxy de por medio, por ejemplo el servicio de mensajería Whatsapp[6].

6. Retardo

   Que la comunicación del cliente con el servidor final no sea directa, supone un retardo en las comunicaciones, que muchas veces se ve compensado si algún objeto se encuentra en la caché del proxy.

[5]Registro oficial de eventos durante un rango de tiempo en particular.
[6]http://www.whatsapp.com/

5.4. Configuración

Existen varias maneras de configurar un browser para navegar a través de un proxy.

1. Manual: Se configura desde una opción específica del navegador.

2. Flags[7]: Un proxy puede configurarse con un flag específico en el lanzamiento del proceso, esto permite indicar el proxy previo a la ejecución del navegador. En el caso de Google Chrome / Chromium el flag utilizado es:

   –proxy-server direccion:puerto

   Este flag es el que se va a utilizar más adelante en la parte de experimentación del proxy desarrollado. El listado de banderas completo se encuentra online[8].

3. Archivos PAC[9]: Puede definirse un archivo de Auto-Configuración de proxy, es un archivo Javascript en el que se pueden realizar acciones avanzadas como por ejemplo, identificar los protocolos y redireccionar al proxy indicado. Ejemplo de archivo PAC en el que se direcciona según el protocolo (HTTP, HTTPS a un proxy diferente):

```
function FindProxyForURL(url, host) {
        if (url.substring(0,5) == "http:") {
                return "PROXY proxy.normal.com:8080";
        }else if (url.substring(0,6) =="https:") {
                return "PROXY proxy.seguro.com:8080";
        } else {
                return "DIRECT";
}
```

[7]Bandera
[8]http://peter.sh/experiments/chromium-command-line-switches/
[9]Proxy Auto-Configuration.

Capítulo 6

Caché Web

6.1. Definición

Un caché web es un intermediario entre un cliente (o varios) y un servidor (o varios). Observa las peticiones que se van realizando y va almacenando los recursos solicitados, de manera que, si hay otra petición de la misma URL, el intermediario puede brindar el recurso sin tener que solicitarlo al destino original [37].

El funcionamiento básico de un caché es el siguiente. Cuando se recibe una petición del cliente, se busca el recurso en el almacenamiento local. En el caso de encontrarlo, se realiza la verificación de que el recurso esté "fresco", es decir, que la copia se encuentre actualizada. Luego, se envía como respuesta al cliente, la copia local. Cuando el recurso se devuelve desde la caché, se llama caché HIT[1], y, en el caso de que el recurso no se encuentre, se llama caché MISS[2]. Un caché, opera con almacenamiento limitado (sea memoria o un medio físico), debido a esto, cuando llena su espacio dedicado debe decidir qué recurso debe quitar para poner uno nuevo. A esto se le llama política de reemplazo, se verá en la Sección 6.3.

[1] Acierto.
[2] Desacierto.

Posee ciertos beneficios al proveer un mecanismo eficiente para la distribución de información en la web [52, p. 20].

1. Latencia

   Un caché web cercano a los clientes, reduce la latencia para los aciertos de caché[3]. Los retrasos en la transmisión son menores por la cercanía entre los dos puntos de interacción. Adicionalmente, se reducen los retrasos por retransmisión y las esperas en los routers a causa de que hay menos enlaces intermedios involucrados.

2. Ancho de Banda

   Cuando se utilizan las copias de los recursos almacenados en la caché, se ahorra ancho de banda, ya que no hay que hacer la petición del recurso al destino final.

3. Carga del Servidor

   Reduce la carga de los servidores al disminuir la cantidad de peticiones que se realizan. Un servidor que esta con poca carga de trabajo es más rápido que uno que está muy ocupado, es decir, atendiendo gran cantidad de peticiones de diferentes clientes.

4. Si un servidor remoto no está disponible temporalmente, una copia del objeto pedido se puede recuperar de la caché.

6.2. Tipos

Hay diferentes tipos de cachés web, entre ellos se encuentran los siguientes:

1. Caché de Navegador

   Los navegadores tienen un caché incluido, la información se almacena de manera local en el dispositivo del usuario. Esta limitado a 1 solo usuario, y se obtiene un hit de caché, solamente cuando se visita nuevamente algún sitio que ya se haya visitado.

[3]Cuando un recurso solicitado por el cliente, efectivamente se encuentra almacenado en la caché.

2. Proxy Cachés

   A diferencia de los de navegador, estos sirven a un número grande de usuarios. Al crecer la cantidad de usuarios, también crece la tasa de aciertos de la caché, ya que los usuarios suelen acceder a los mismos sitios (sitios de gran popularidad) [25].

3. Surrogates Servers

   Son intermediarios que actúan con la autoridad del servidor original para servir contenidos como si fueran el servidor mismo [38]. Generalmente se encuentran cerca de los servidores originales, sirviendo el contenido de los mismos, generalmente desde una caché interna.

   Se usan como redes de distribución de contenidos (CDN), para tener replicaciones de los recursos de un servidor en diferentes lugares. Los recursos peticionados por los clientes, son revueltos por el CDN más cercano físicamente. También se usan como aceleradores, simplemente almacenando en la caché las respuestas del servidor.

6.3. Políticas de Reemplazo / Algoritmos de Caché

Para el buen funcionamiento de la caché, hay que definir de qué manera se van reemplazando los contenidos almacenados en la misma. Para esto se utiliza una política de reemplazo de objetos, orientado a ciertas características de los objetos, tales como el tamaño, cantidad de peticiones de dicho objeto, tiempo almacenado en la caché, etc. Hay diversos algoritmos que se detallan a continuación.

1. Primero en Entrar Primero en Salir (FIFO[4])

   Este método es el más sencillo, se trata de una cola en la que el primer elemento en entrar es el primer elemento en salir, es decir, aquel que más tiempo haya estado en la caché es el que más probabilidades tiene de salir.

[4]First In First Out.

2. Aleatorio

   Realiza el reemplazo buscando aleatoriamente un objeto almacenado en la caché.

3. Menos Usado Recientemente (LRU[5])

   Este método, busca reemplazar al objeto que más tiempo haya estado en la caché sin ser peticionado, es decir, aquel objeto que menos peticiones haya tenido en un lapso de tiempo amplio, es el que tiene más posibilidades de ser reemplazado.

4. Menor Menos Usado Recientemente (LRU-MIN)

   Es una optimización del algoritmo LRU, en el cual se busca reemplazar los objetos de mayor tamaño de la caché. quedando así objetos de menor tamaño almacenados.

5. Menos Frecuentemente Usado (LFU[6])

   Se evalúa la frecuencia con la que un elemento es solicitado, el que es menos solicitado es el que tiene más posibilidades de ser reemplazado.

Existen otras políticas más sofisticadas que consideran el costo de cada objeto. Por ejemplo el algoritmo GreedyDual-Size [52], en el cual se asigna un valor a los objetos almacenados basados en el costo de un caché miss y el tamaño del objeto. No se especifica cual es el "costo", lo que provee flexibilidad para optimizar lo que se quiera. El costo podría ser la latencia o la cantidad de paquetes transmitidos para traer el recurso, por ejemplo.

6.4. Control de Caché

Cuando el cliente realiza una petición, y esta coincide con un elemento que tenemos almacenado en la Caché se debe evaluar si es viable enviar la copia local, o hacer la petición nuevamente, a esto se le llama revalidación. Para esto se realizan ciertos controles (extraídos de [37]) en base a los headers de HTTP (vistos en 3.4.1).

[5]Last Recently Used.
[6]Least Frequently Used.

1. El Header *Expires*, indica cuanto tiempo va a estar "fresco"[7] el recurso. Si en el momento de la petición, todavía no expiró el recurso, puedo servirlo de la copia local. Tiene algunas limitaciones, como por ejemplo que el valor permitido es una fecha en GMT[8], lo que lleva a que los relojes del servidor y del caché estén sincronizados, de otra manera no tiene sentido una comparación de fechas. Otro problema que se encuentra es que si se envía este header, pero no está actualizado, siempre va a enviar una fecha anterior a la actual lo que llevaría a generar siempre la petición del recurso.

2. Se puede utilizar el header *Cache-control*[9] que brinda información variada. El formato es: **Cache-control: especificación1, especificación2, especificaciónN**.

   a) *max-age* - Especifica en tiempo en el que el recurso puede ser considerado "fresco" en segundos. Es el similar a *Expires* pero con un valor específico a diferencia de una marca de tiempo.

   b) *s-maxage* - Similar al anterior pero para los cachés compartidos[10].

   c) *public* - Indica que las peticiones que requieren autenticación pueden almacenarse en la caché.

   d) *private* - Permite que el recurso puede almacenarse en aquellos cachés que son solo para 1 solo usuario[11] y no en una caché compartida.

   e) *no-cache* - Fuerza a que el recurso tenga que revalidarse antes de devolver la copia local de la caché al cliente.

   f) *no-store* - Indica que el recurso no debe quedar almacenado en la caché bajo ninguna circunstancia.

   g) *must-revalidate* - Si el recurso luego de validarlo en la caché no esta "fresco", debe revalidarse.

   h) *proxy-revalidate* - Igual que *must-revalidate* pero aplicado a proxies.

[7] No va a tener cambios.
[8] Greenwich Mean Time.
[9] Implementado a partir de la versión 1.1 de HTTP.
[10] Por ejemplo un proxy.
[11] Por ejemplo la caché de un browser.

Cuando ambos headers, *Expires* y *Cache-control* están presentes en la respuesta, *Cache-control* es el que toma mayor importancia.

Para realizar la revalidación se utilizan ciertos headers en la petición. Los servidores utilizan 2 headers para realizar las validaciones, uno es *Last-Modified*, que indica cuándo fué modificado por última vez el recurso. Cuando éste está presente, el cliente puede realizar una petición con el header *If-Modified-Since*:fecha, para que el servidor devuelva el recurso únicamente si se cumple con esta condición, de no ser así, devuelve un mensaje con el código `304 Not Modified`, que indica que el recurso no fue modificado y se puede servir la copia local. Por otro lado, se utiliza un identificador llamado *ETag* que se genera cada vez que el recurso se modifica. Es una cadena de texto que identifica una versión específica del recurso. En este caso, el cliente puede utilizar el header *If-None-Match*:ETag_local, que el servidor responde con el recurso en el caso de que el identificador enviado por el cliente no coincida con el del objeto peticionado.

Capítulo 7

Proxy Adaptativo para Protocolos Web Avanzados

7.1. Introducción

A lo largo de los capítulos anteriores, se ha visto, el crecimiento de Internet, en el Capítulo 2, las deficiencias de los protocolos, en el Capítulo 3, y la problemática de los tiempos de carga y sus posibles optimizaciones en el Capítulo 4. También se ha visto SPDY como propuesta a resolver varios de los problemas actuales de la carga de los sitios, pero también, en ciertos contextos no funciona como lo esperado (ver Sección 4.4.4).

Por todo ello, se propone, desarrolla y evalúa un *Proxy Adaptativo*, que selecciona, de los métodos habilitados que ofrezca un sitio (HTTP, HTTPS, SPDY), cuál es el óptimo para recuperar el recurso, en base a información almacenada de recuperaciones previas. Posee otras funcionalidades tales como, ser MITM[1], caché, cálculo de RTT, recuperación de los métodos habilitados para un sitio, cliente SPDY.

Para el desarrollo del proxy, se escogió Python[2] como lenguaje principal, dada la facilidad del mismo y la gran documentación disponible en la web. Para el almacenamiento de los datos de los sitios se escogió MongoDB[3], por su simple interacción

[1] Man in The Middle.
[2] https://www.python.org/
[3] http://www.mongodb.org/

con Python y su alta velocidad.

Todo el código del trabajo se encuentra alojado en un repositorio de Github[4], que es un repositorio para alojar proyectos de código abierto. El repositorio puede navegarse desde [36].

7.2. Funcionamiento

El proxy se inicia en una dirección y en un puerto, por ejemplo: *localhost:8080* se debe configurar el navegador para que utilice la dirección del proxy para conectarse a Internet. Por ejemplo en Google Chrome se puede iniciar con un flag para configurar el proxy:

chrome –proxy-server="localhost:8080"

Acepta tanto conexiones HTTP, como HTTPS en el mismo puerto. Al realizar la conexión por SSL con el cliente en vez de actuar de "puente" con el destino final, utiliza un certificado SSL para realizar la autenticación.

Cuando recibe una petición HTTP, el método que llega al proxy es *GET*, se consulta la caché para ver si el recurso se encuentra almacenado para retornarlo desde la copia del proxy, si no se encuentra, se pide al servidor correspondiente y se devuelve el recurso al cliente. Luego, se realiza el análisis del recurso (ver 7.2.1) en segundo plano.

Cuando recibe una petición HTTPS, el método que llega al proxy es CONNECT, que es un método especial para solicitarle a un proxy una conexión al servidor final. En este caso, el proxy responde con el mensaje:

HTTP/1.1 200 Connection established

para indicarle que se va a realizar la conexión. Esta primera etapa puede verse en la Figura 7.1.

[4]https://www.github.com

Figura 7.1: Conexión inicial cuando el protocolo es HTTPS

Luego, se inicia la conexión SSL cliente-proxy y comienzan a recibirse las peticiones del cliente, como puede verse en la Figura 7.2, las conexiones[5] se realizan individualmente (no como un túnel HTTPS normal, ver Figura 5.2). Con cada una de las peticiones, se procede de manera similar a HTTP. Se analiza si el recurso se encuentra almacenado en la caché y se devuelve de la copia local, o se solicita el recurso al servidor final. En el caso de que el método seleccionado para devolver el recurso sea HTTS o SPDY, se establece una conexión segura entre el proxy y el servidor final.

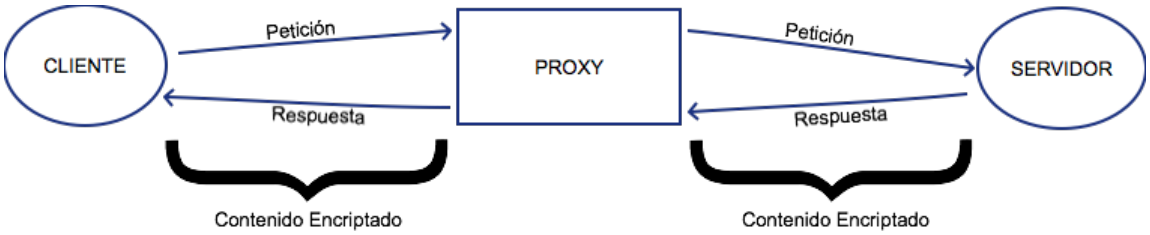

Figura 7.2: Procedimiento una vez realizada la conexión en los 2 extremos

Cabe destacar que, todo el tráfico que fluye entre el cliente y el proxy, y entre el proxy y el servidor final, viaja encriptado. Pero, todo el tráfico se encuentra desencriptado en el proxy, siendo este, un proxy HTTPS de confianza (ver 5.1, discusión en [5]).

7.2.1. Análisis de los Recursos

Cada vez que el proxy recibe una petición del cliente, se analiza si el recurso se encuentra en la caché, en el caso de que el recurso se encuentre almacenado, se devuelve desde la copia local del proxy y se actualiza la caché con el HIT del elemento

[5]Tanto hacia el cliente como hacia el Servidor.

correspondiente. Caso contrario, se peticiona el recurso servidor final. Cada vez que el proxy pide un recurso, se realiza un análisis del mismo en segundo plano:

1. Cálculo del tamaño del recurso.

2. Cálculo del RTT: se realiza el cálculo del RTT al host donde se aloja el recurso.

3. Obtención de Protocolos: se obtienen los protocolos soportados (HTTP, HTTPS, SPDY) del host donde se aloja el recurso.

4. Cálculo de Peticiones a Generar: en el caso de que el recurso sea un HTML plano, se calcula cuantas peticiones generaría. Se realiza analizando el texto y extrayendo los recursos que esa página va a necesitar para su renderización.

Toda esta información, luego es consumida por un árbol de decisión para determinar que protocolo es el más óptimo para recuperar el recurso.

7.2.2. Árbol de Decisión

Una vez que se recibe la petición del cliente, y hay que peticionar el recurso al servidor final, se decide con qué método se debe traer el recurso. Se tomó como referencia, el árbol de "How Speedy is SPDY?" [51], que puede verse en la Figura 7.3.

Este árbol, se retroalimenta con la información que se extrae de los recursos a medida que el proxy está en funcionamiento. Datos tales como tamaño, RTT, peticiones a generar, se obtienen del almacenamiento propio del proxy.

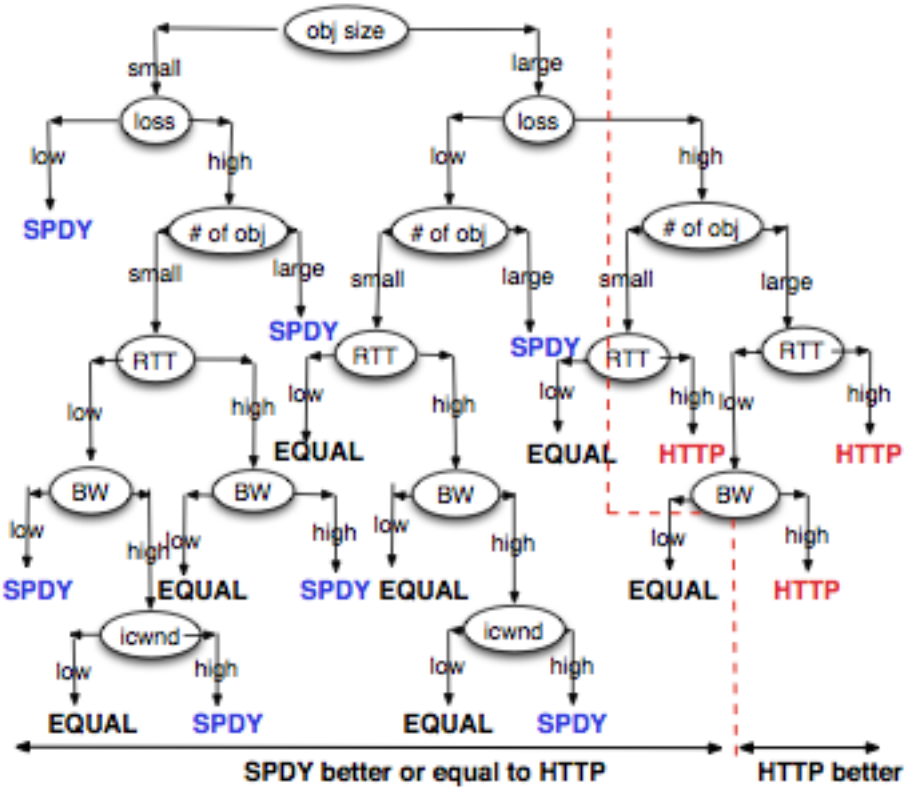

Figura 7.3: Árbol de Decisión, extraído de [51]

7.3. Módulos Adicionales

7.3.1. Cálculo del RTT

Módulo que se encarga de realizar un Ping[6] hacia el host del que se busca obtener la latencia entre ambos nodos. El proxy envía un solo paquete ICMP al servidor y se espera su respuesta. Una vez obtenido el resultado, se almacena en la base de datos local. También, ofrece la posibilidad de realizar peticiones masivas, leyendo URLs desde un archivo de texto. Esta opción es útil por ejemplo, para ejecutar antes de iniciar el proxy, y así obtener mediciones a priori de hosts que serán visitados.

[6]Utilidad que comprueba el estado de otro host por medio del envío de paquetes ICMP de solicitud y de respuesta [13].

7.3.2. Protocolos Habilitados

Módulo que se encargar de identificar que protocolos soporta un sitio en cuestión. Los protocolos de los que se intenta averiguar si el sitio tiene disponible son HTTP, HTTPS y SPDY. El procedimiento es el siguiente:

1. HTTP: Se intenta realizar una conexión al puerto por defecto de HTTP, el puerto 80. En el caso de tener éxito, se marca HTTP como un protocolo soportado.

2. HTTPS: Se intenta realizar una conexión al puerto por defecto de HTTPS, el puerto 443. En el caso de tener éxito, se marca HTTPS como un protocolo soportado.

3. SPDY En el caso de SPDY, se utilizó el cliente desarrollado junto con el proxy (ver 7.3.3). Al igual que con los otros protocolos, se intenta realizar una conexión segura con el servidor final, si la conexión tiene éxito, se intenta iniciar una sesión SPDY con el servidor. Si el inicio de la sesión es correcto, se marca SPDY como un protocolo soportado.

Al igual que el módulo que calcula el RTT (ver 7.3.1), éste posee una opción para realizar la verificación de los protocolos habilitados, leyendo un archivo de texto con las URLs. Tal como el módulo antes descripto, es útil para poseer información previo a la utilización del proxy.

7.3.3. Cliente SPDY

Python no trae soporte nativo para SPDY, por ello se buscó una librería que pueda brindar la funcionalidad del protocolo. La seleccionada fue Spdylay [49] de Tatsuhiro Tsujikawa, que, si bien es para el lenguaje C, provee una extensión para utilizarla desde Python[7]. Utilizando esta librería, se diseño un cliente para poder realizar y mantener una sesión a través de una conexión TCP con un servidor que soporte SPDY. El módulo permite iniciar una conexión con un servidor y luego iniciar la sesión SPDY. Luego, se pueden realizar peticiones a través de la misma conexión.

[7] http://tatsuhiro-t.github.io/spdylay/python.html

Capítulo 8

Experimentos y Resultados

8.1. Introducción

A los efectos de probar el desempeño del proxy, se diseño un experimento con sitios reales para simular un ambiente adecuado para la prueba. Se extrajeron sitios del top de Alexa[1], que es una compañía de Amazon[2] que se especializa en realizar mediciones de tráfico global y brinda las estadísticas obtenidas. También, ofrece un ranking Global de los sitios más visitados de toda Internet, de este ranking se extrajeron los sitios para la experimentación. Se desarrollaron herramientas para extraer una porción del ranking de Alexa y también para automatizar el experimento en sí.

8.2. Ranking de Alexa

El ranking de Alexa se encuentra online en su sitio, pero fue necesario desarrollar una pequeña aplicación para extraer el listado y guardarlo en un archivo de texto para su posterior uso. Esta herramienta se encuentra disponible online [35].

[1] http://www.alexa.com
[2] http://www.amazon.com

8.3. Chrome-har-capturer

Con la idea de automatizar el experimento, se utilizó *Chrome-har-capturer* [23] que, a través de la API de depuración remota (ver [14]) del navegador Chrome o Chromium, permite que la herramienta pueda interactuar con dicha aplicación. Esto permite poder navegar un sitio en particular y obtener un archivo HAR[3] [39] , que contiene los resultados de la interacción del navegador con el sitio.

El HAR obtenido, es un archivo con formato JSON[4] que contiene información de la interacción de un navegador con un sitio [39]. Contiene un registro de cada objeto que está siendo cargado por el navegador. La información acerca de los tiempos que se puede obtener es:

1. Cuanto tarda en recuperar la información de DNS.
2. Cuanto tarda en peticionar un objeto.
3. Cuanto tarda en conectarse al servidor.
4. Cuanto tarda la transferencia desde el servidor al navegador de cada objeto.

De este archivo, se pueden extraer 2 valores que son importantes para evaluar el tiempo de carga de los sitios. Estos valores son:

1. onContentLoad: Tiempo en el que el contenido del sitio se carga.
2. onLoad: Tiempo en el que es sitio se carga según el navegador.

De los cuales, tomaremos como referencia *onLoad* ya que es el tiempo más cercano a la experiencia que tiene un usuario final cuando navega el sitio en cuestión. Es decir, es el valor que está más cerca de lo que tarda el navegador en renderizar el sitio completo.

[3]HTTP Archive
[4]JavaScript Object Notation, es un formato ligero para el intercambio de datos [3].

8.4. Experimentos

El experimento consiste en un navegador conectado a Internet a través del proxy, en el cual se realiza la petición de la página de inicio, con todos sus elementos, de ciertos sitios seleccionados. Se divide en 2 fases, en una, las peticiones se realizan en HTTP plano, y en otra en HTTPS, es decir, que el cliente se conecta de forma segura al proxy.

La comparación se realiza entre un proxy convencional (transparente) y el proxy adaptativo propuesto. Cada una de las fases se realizó con ambos proxies.

La primera fase puede verse en las Figuras 8.1 y 8.2.

Cabe destacar que en ambas fases se deshabilitó la funcionalidad de caché para que siempre sea necesario realizar las peticiones de los recursos.

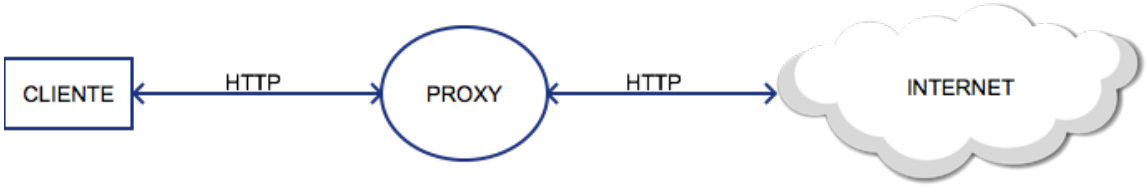

Figura 8.1: HTTP - Proxy Convencional

Figura 8.2: HTTP - Proxy Adaptativo

En la segunda fase en las imágenes 8.3 y 8.4.

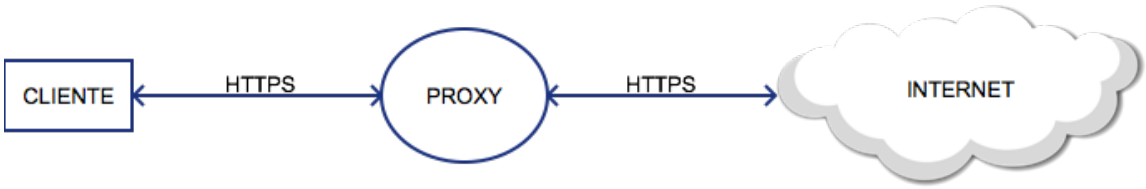

Figura 8.3: HTTPS - Proxy Convencional

Figura 8.4: HTTPS - Proxy Adaptativo

Se seleccionaron 200 sitios extraídos del ranking de Alexa, utilizando la herramienta vista en la Sección 8.2. El listado completo para HTTP y HTTPS se puede ver en la Sección A de los Apéndices.

Previo a iniciar el experimento, se obtuvieron todos los protocolos soportados de los sitios seleccionados, así también como el RTT de los mismos. De esta manera, el proxy ya tiene a priori, algo de información para poder determinar que protocolo va a utilizar para obtener el sitio.

Se diseñó un script para automatizar el experimento. Este lee de un archivo de texto el listado de los sitios del correspondiente protocolo, realiza la petición a través de Chrome, y guarda el archivo HAR generado en una carpeta.

Algorithm 8.4.1: EXPERIMENTO()

$$\begin{cases} \textbf{for } sitio \in sitios \\ \quad \textbf{do} \\ \quad \begin{cases} iniciar\ chrome\ a\ traves\ del\ proxy \\ ejecutar\ chrome - har - capturer \\ cerrar\ chrome \end{cases} \end{cases}$$

Una vez obtenidos todos los archivos de las pruebas, se procesaron para extraer los valores de onConcentLoad y onLoad.

8.5. Resultados

En los resultados se observa que, a lo largo de todos los sitios, el rendimiento del proxy adaptativo es mejor o similar que el proxy convencional. De los sitios seleccionados para la fase de HTTP, 60 soportan los 3 protocolos, de los cuales en 45 sitios el proxy optó por utilizar SPDY. De los sitios de la fase de HTTPS, 75 soportan los 3 protocolos, y en 53 fué seleccionado SPDY.

En el caso de HTTP, puede observarse una mejora promedio de un 5 %, con picos de hasta un 17 % en el mejor de los casos (www.google.gr). La vista general de los sitios que soportan los 3 protocolos puede verse en la Figura 8.5.

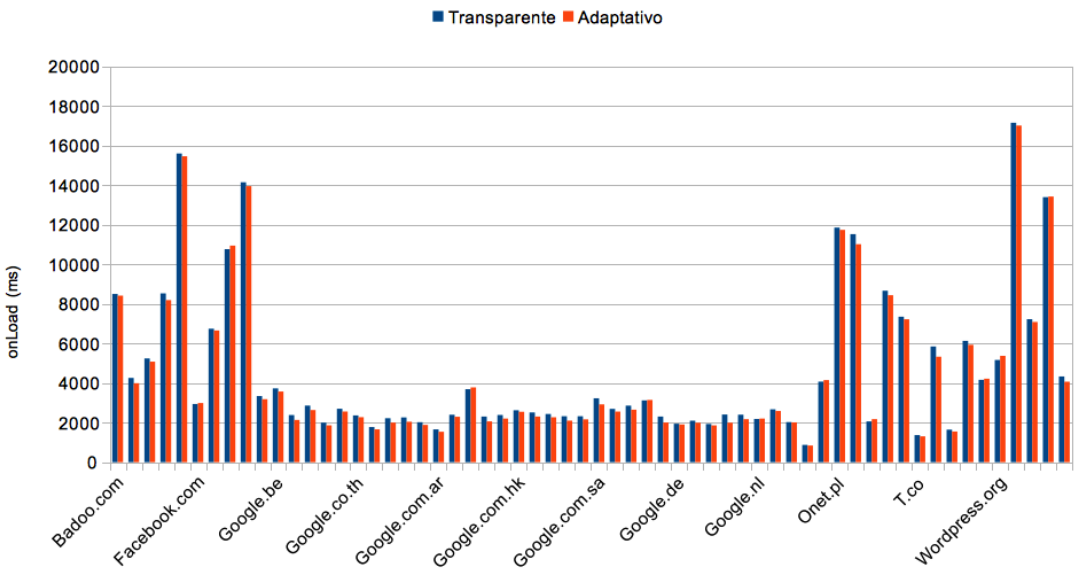

Figura 8.5: Resultados HTTP - Sitios con todos los protocolos soportados

En los sitios que se seleccionó como protocolo a SPDY, la mejora promedio fue del 6 %. En la Figura 8.6 pueden verse los resultados sólo de los dominios que pertenecen a Google. Como puede observarse, en el 90 % de los casos se obtuvieron mejoras.

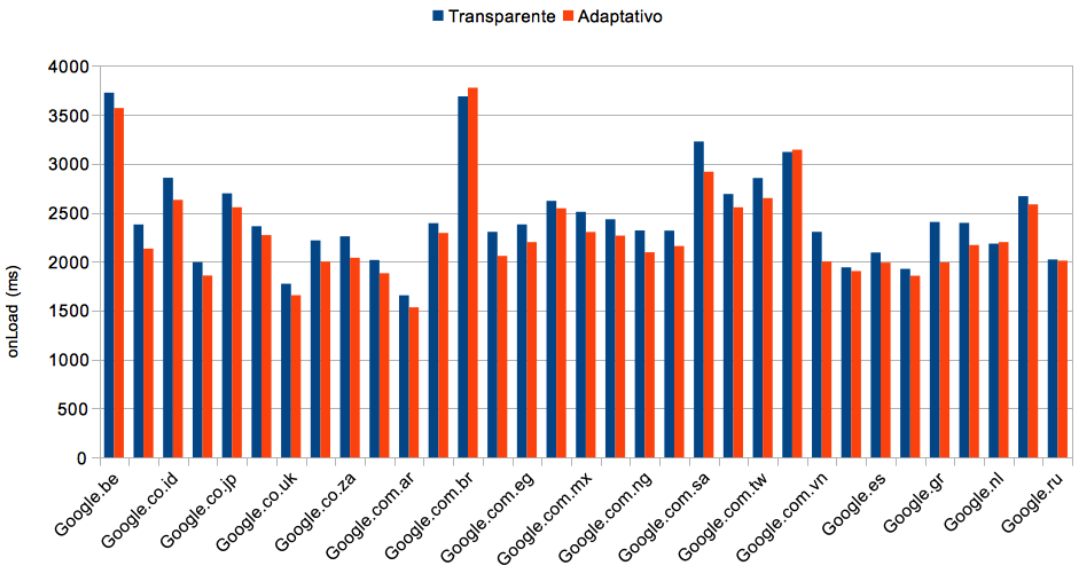

Figura 8.6: Resultados HTTP - Sitios del dominio Google

En el caso de HTTPS, puede observarse una mejora promedio de un 7 %, con picos de hasta un 24 % en el mejor de los casos (www.google.co.uk). La vista general de los sitios que soportan los 3 protocolos puede verse en la Figura 8.7.

En los sitios que se seleccionó como protocolo a SPDY, la mejora promedio fue del 10 %. En la Figura 8.8 pueden verse los resultados sólo de los dominios que pertenecen a Google. Como puede observarse, en el 100 % de los casos se obtuvieron mejoras.

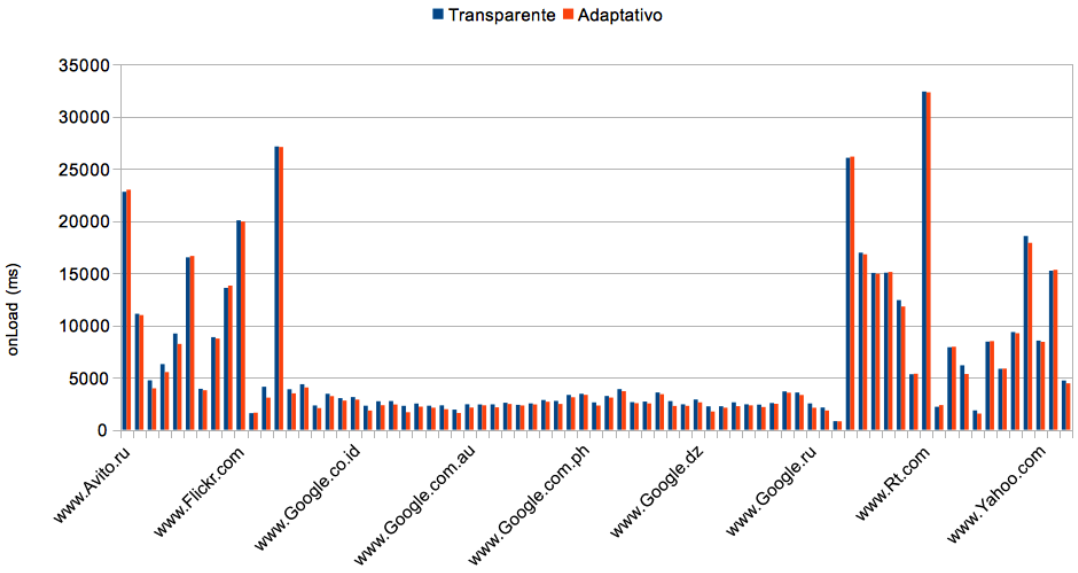

Figura 8.7: Resultados HTTPS - Sitios con todos los protocolos soportados

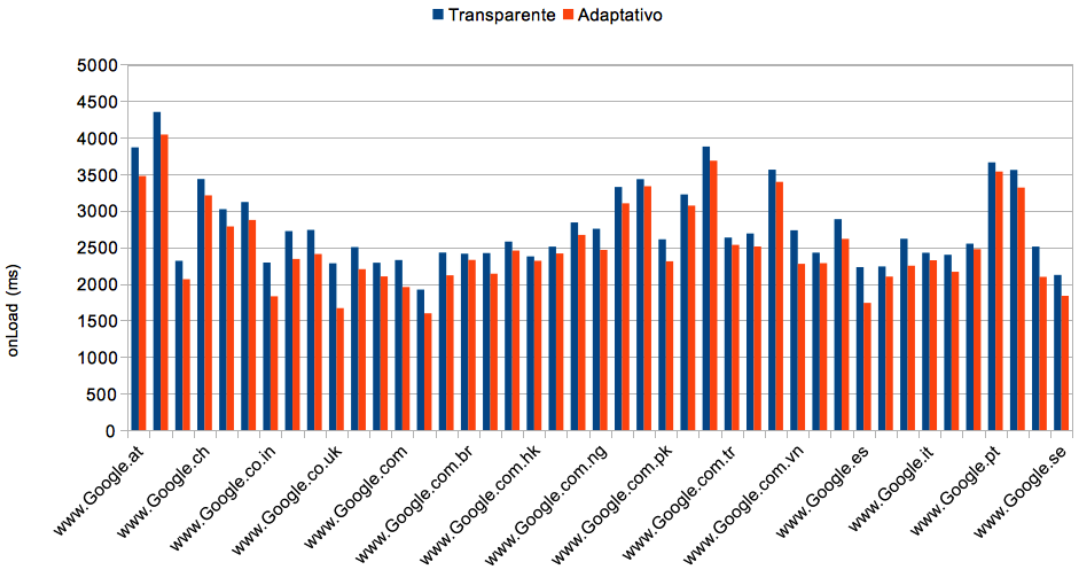

Figura 8.8: Resultados HTTPS - Sitios del dominio Google

En ambas fases del experimento (HTTP y HTTPS) se pudo observar que el sitio que tuvo un rendimiento negativo fué www.sogou.com. Pero, en ninguno de los casos el proxy decidió SPDY como protocolo óptimo, es decir, que la diferencia es debido a las variaciones de la red mientras se realizan las pruebas.

En los cuadros siguientes, se puede observar el rendimiento del proxy adaptativo.

Negativo	Bajo	Medio	Alto
16,5 %	31,5 %	45 %	7 %

Porcentajes de mejora del proxy adaptativo en la fase de HTTP.

Negativo	Bajo	Medio	Alto
16 %	36 %	32 %	16 %

Porcentajes de mejora del proxy adaptativo en la fase de HTTPS.

A continuación, se muestra la decisión del árbol en un caso en el que se obtuvo una mejora del 27 % (ver Figura 8.9) del sitio www.google.co.uk.

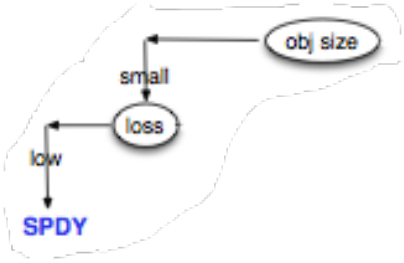

Figura 8.9: Resultado del árbol de decisión para el sitio www.google.co.uk

También se puede observar otro caso en el que el árbol de decisión no optó por SPDY, el rendimiento fue similar al proxy convencional (ver Figura 8.10), el sitio es www.files.wordpress.com.

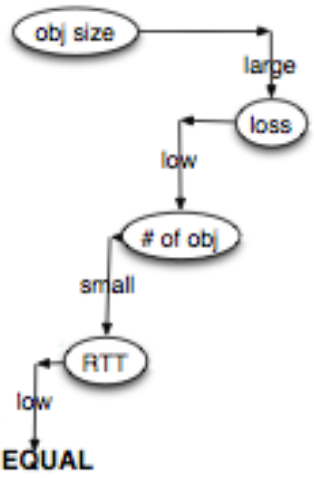

Figura 8.10: Resultado del árbol de decisión para el sitio www.files.wordpress.com

Capítulo 9

Conclusiones

Es necesario abordar los problemas vistos a lo largo de este trabajo, tanto de la parte de los protocolos como del crecimiento de la Web. Si bien existen diversos enfoques para mejorar los tiempos de respuesta de la carga de los sitios, ofrecen una solución dadas ciertas características del contexto en el que se están utilizando. SPDY es un protocolo que muestra que se pueden mejorar ciertos aspectos sin tener un gran impacto en la implementación. Pero, su rendimiento se encuentra relacionado directamente con el contexto en que se está utilizando, cuestiones como el ancho de banda, pérdida de paquetes, tamaño de los recursos, cantidad de recursos peticionados, afectan los tiempos de respuesta.

En este trabajo se propone y se desarrolla un proxy adaptativo capaz de decidir qué protocolo utilizar, dado un contexto determinado, con el cual se optimicen los tiempos de carga de las páginas. Se basa en las características propias de los protocolos en los que se ven beneficiados o no. Con el fin de evaluar la performance, se diseña y se ejecuta un experimento para obtener el tiempo de carga de ciertas páginas y poder comparar el proxy propuesto con un proxy convencional.

Los resultados son favorables en gran parte de los sitios que aceptan los 3 protocolos. La adecuación de los protocolos al contexto en el que se está operando, es decir, utilizar el protocolo que se vea más beneficiado con las condiciones dadas, provee una leve mejora en el rendimiento general de la carga de los sitios. Esta mejora es más significativa en el caso de las conexiones que se realizan con HTTPS.

En cuanto a los sitios del ranking de Alexa a la fecha actual, la mayoría utiliza

HTTPS para operar, pero solo el 20 % soportan SPDY. Con lo cual, no existe esta opción para poder mejorar el rendimiento. Es importante, al menos ofrecer el protocolo alternativo, ya que uno podría, dado el contexto, tomar la decisión por uno u otro dadas las condiciones del contexto.

SPDY sentó las bases del nuevo HTTP 2.0 que, si bien todavía no está implementado, está en vías de implementarse en un futuro cercano. La utilización de SPDY, serviría para poder experimentar con el protocolo y poder adecuar los sitios para que su rendimiento sea óptimo, cuestión importante previendo una futura migración a HTTP 2.0.

Otra cuestión importante es que, la utilización de un proxy que pueda manejar SPDY u otros protocolos en un futuro, brinda la posibilidad de aprovechar las características de dichos protocolos, sin necesidad de que el cliente conectado al proxy, tenga un navegador que soporte dichos protocolos. También, que el proxy actúe de MITM, ofrece la posibilidad de utilizar herramientas como una caché web, para mejorar la performance, en sitios en los que no se puede utilizar esta opción (por ejemplo, HTTPS).

9.1. Trabajos futuros

A partir del desarrollo de este trabajo se detectaron múltiples oportunidades de expansión y nuevas líneas de trabajo. Como continuidad del mismo se propone, extraer el algoritmo de selección de protocolo e implementarlo en un cliente directo, tal como un navegador. Para así tener la ventaja de no tener ningún intermediario y realizar la conexión directamente con el servidor final, ahorrándose las conexiones extras.

Por otro lado, implementar el proxy como reverso, brindaría la posibilidad de ofrecer SPDY para servidores que todavía no lo soportan.

Agregar la funcionalidad de que el cliente pueda conectarse con SPDY como protocolo, brinda la posibilidad de tener conectados 2 proxies más conectados entre sí. Útil por ejemplo para tenerlos funcionando en ubicaciones geográficas diferentes y armar un CDN que se comunica con SPDY, es decir, por una sola conexión TCP.

En un futuro cuando HTTP 2.0 ya se encuentre en funcionamiento, extender el

proxy para aceptar este protocolo y sumarlo al árbol de decisión, da la posibilidad de poder probar su rendimiento.

Glosario

A

Ancho de Banda

Es la longitud, medida en Hz, del rango de frecuencias en el que se concentra la mayor parte de la potencia de la señal. También puede referirse a la tasa media de transferencia de datos exitosa a través de una vía de comunicación. Puede conocerse como capacidad del canal de comunicación.

D

DNS - Domain Name System

Sistema de nombres de dominio. Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

Dominio

Un dominio de Internet es una red de identificación asociada a un grupo de dispositivos o equipos conectados a Internet. El propsito principal de los nombres de dominio en Internet y del sistema de nombres de dominio (DNS), es traducir las direcciones IP de cada nodo activo en la red, a términos memorizables y fáciles de encontrar.

G

GMT - Greenwich Mean Time

Identificador Universal de Recursos. Es un estándar de tiempo que originalmente se refería al tiempo solar medio en el Real Observatorio de Greenwich, en Greenwich, cerca de Londres, Inglaterra, que en 1884 fue elegido por la Conferencia Internacional del Meridiano como el primer meridiano.

H

HTML - HyperText Markup Language

Lenguaje de Marcado de Hipertexto. Es un estándar que sirve de referencia para la elaboración de páginas web en sus diferentes versiones, define una estructura básica y un código (denominado cdigo HTML) para la definición de contenido de una página web.

I

ISO - International Organization for Standardization

Es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepcin de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional.

L

LAN - Local Area Network

Es una red que interconecta computadoras dentro de un área limitada. Se encuentran dentro de una área geográfica pequeña.

Latencia

Retraso en la transmisión de datos desde un punto a otro.

M

MIME - Multipurpose Internet Mail Extensions

Son una serie de convenciones o especificaciones dirigidas al intercambio a través de Internet de todo tipo de archivos (texto, audio, video, etc.) de forma transparente para el usuario. Una parte importante del MIME está dedicada a mejorar las posibilidades de transferencia de texto en distintos idiomas y alfabetos.

N

Netcraft

Es una compañía de servicios de Internet basada en Bath, Inglaterra. Netcraft ofrece análisis de cuota de mercado de servidores y alojamiento web, incluyendo la detección del tipo de servidor web y de sistema operativo.

P

PDF - Portable Document Format

Formato de Documento Portátil. Es un formato de almacenamiento de documentos digitales independiente de plataformas de software o hardware. Este formato es de tipo compuesto (imagen vectorial, mapa de bits y texto). Fue inicialmente desarrollado por la empresa Adobe Systems, oficialmente lanzado como un estándar abierto el 1 de julio de 2008 y publicado por la Organización Internacional de Estandarización como ISO 32000-1.

R

RFC - Request For Comments

Petición de Comentarios. Son una serie de notas sobre Internet, y sobre sistemas que se conectan a internet, que comenzaron a publicarse en 1969. Cada una de ellas individualmente es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet, que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambiguedades.

S

Script

Es un programa usualmente simple, que por lo regular se almacena en un archivo de texto plano. Los script son casi siempre interpretados, pero no todo programa interpretado es considerado un script. El uso habitual de los scripts es realizar diversas tareas como combinar componentes, interactuar con el sistema operativo o con el usuario.

T

Telefonía Móvil 3G

Es la abreviación de tercera generación de transmisión de voz y datos a través de telefonía móvil mediante UMTS (servicio universal de telecomunicaciones móviles).

U

URI - Universal Resource Identifier

Identificador Universal de Recursos. Es una cadena de caracteres corta que identifica inequívocamente un recurso. Ver [19].

URL - Localizador de Recursos Uniforme

Secuencia de caracteres, de acuerdo a un formato modélico y estándar, que se usa para nombrar recursos en Internet para su localización o identificación, como por ejemplo documentos textuales, imágenes, vdeos, presentaciones digitales, etc. El formato general de un URL es: esquema://máquina/directorio/archivo.

W

WAN - Wide Area Network

Es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes. Es cualquier red que une varias redes locales, por lo que sus miembros no están todos en una misma ubicacin física.

Bibliografía

[1] The "data" url scheme. . URL http://tools.ietf.org/html/rfc2397.

[2] Deflate compressed data format specification. . URL http://www.ietf.org/rfc/rfc1951.txt.

[3] Ecma-404 the json data interchange standard. URL http://www.json.org.

[4] El modelo osi. URL http://www.exa.unicen.edu.ar/catedras/comdat1/material/ElmodeloOSI.pdf.

[5] Explicit trusted proxy in http/2.0. URL http://www.ietf.org/id/draft-loreto-httpbis-trusted-proxy20-01.txt.

[6] February 2014 web server survey. URL http://news.netcraft.com/archives/category/web-server-survey/.

[7] Gzip file format specification. . URL http://www.gzip.org/zlib/rfc-gzip.html.

[8] Http over tls. . URL http://tools.ietf.org/html/rfc2818.

[9] httparchive - the http archive tracks how the web is built. . URL http://httparchive.org/.

[10] Hypertext transfer protocol version 2. . URL http://tools.ietf.org/html/draft-ietf-httpbis-http2-13.

[11] Internet growth statistics. URL http://www.internetworldstats.com/emarketing.htm.

[12] La encapsulación de datos, un concepto crítico. URL http://www.redescisco.net/v2/art/la-encapsulacion-de-datos-un-concepto-critico/.

[13] ping(8) - linux man page. URL http://linux.die.net/man/8/ping.

[14] Remote debugging protocol. URL https://developer.chrome.com/devtools/docs/debugger-protocol.

[15] Rfc: Hypertext transfer protocol – http/1.1. . URL http://www.ietf.org/rfc/rfc2616.txt.

[16] Spdy: An experimental protocol for a faster web. . URL http://www.chromium.org/spdy/spdy-whitepaper.

[17] Spdy protocol - draft 1. . URL http://www.chromium.org/spdy/spdy-protocol/spdy-protocol-draft1.

[18] Stream control transmission protocol. . URL http://tools.ietf.org/html/rfc2960.

[19] Uniform resource identifier (uri): Generic syntax. . URL http://tools.ietf.org/html/rfc3986.

[20] Using sctp as a transport layer protocol for http. URL http://tools.ietf.org/html/draft-natarajan-http-over-sctp-00.

[21] Web caching: Making the most of your internet connection. URL http://www.web-cache.com.

[22] Mike Belshe. More bandwidth doesn't matter (much). Agosto 2010.

[23] Andrea Cardaci. chrome-har-capturer. capture har files from a remote chrome instance. URL https://github.com/cyrus-and/chrome-har-capturer.

[24] Forrester Consulting y Inc. Akamai Technologies. ecommerce web site performance today. Agosto 2009.

[25] Duska, Bradley, David Marwood, y Michael Feely. The measured access characteristics of world-wide-web client proxy caches. Diciembre 1997.

[26] Yehia Elkhatib, Gareth Tyson, y Michael Welzl. The effect of network and infrastructural variables on spdy?s performance. Julio 2013.

[27] Jeffrey Erman, Vijay Gopalakrishnan, Rittwik Jana, y K.K. Ramakrishnan. Towards a spdy?ier mobile web? Diciembre 2013.

[28] Bryan Ford. Structured streams: a new transport abstraction. Agosto 2007.

[29] David Gourley, Brian Totty, Marjorie Sayer, Anshu Aggarwal, y Sailu Reddy. *HTTP: The Definitive Guide*. O'Reilly Media, 2002.

[30] Ilya Grigorik. Web-vpn: Secure proxies with spdy & chrome. URL https://www.igvita.com/2011/12/01/web-vpn-secure-proxies-with-spdy-chrome/.

[31] Ilya Grigorik. *High Performance Browser Networking*. O'Reilly Media, 2013.

[32] ISO/IEC. Information technology - open systems interconnection - basic reference model: The basic model. Noviembre 1994.

[33] Balachander Krishnamurthy, Jeffrey C. Mogul, y David M. Kristol. Key differences between http/1.0 and http/1.1. 1999.

[34] James F. Kurose y Keith W. Ross. *Redes de Computadores, Un Enfoque Descendente Basado en Internet*. Pearson, 2013.

[35] Pablo Maximiliano Lulic. Alexa top. . URL https://github.com/maxisoad/alexatop.

[36] Pablo Maximiliano Lulic. Proxy adaptativo para protocolos web avanzados. . URL https://www.github.com/maxisoad/spdyproxypython.

[37] Mark Nottingham. Caching tutorial for web authors and webmasters. URL http://www.mnot.net/cache_docs/.

[38] Mark Nottingham y Xiang Liu. Edge architecture specification. URL http://www.w3.org/TR/edge-arch.

[39] Jan Odvarko. Har 1.2 spec. URL http://www.softwareishard.com/blog/har-12-spec/.

[40] Website Optimization. Average web page size triples since 2008. URL http://www.websiteoptimization.com/speed/tweak/average-web-page/.

[41] International Standard Organization. The measured access characteristics of world-wide-web client proxy caches. Noviembre 1994.

[42] Jitendra Padhye y Henrik Frystyk Nielsen. A comparison of spdy and http performance. Julio 2012.

[43] R.L. Rivest, A. Shamir, y L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Abril 1977.

[44] Carlos E. Quesada Sánchez y Esteban Meneses. Polticas de reemplazo en la caché de web. Diciembre 2006.

[45] Steve Souders. *High Performance Web Sites*. O'Reilly Media, 2007.

[46] NATIONAL INSTITUTE OF STANDARDS y TECHNOLOGY. Data encryption standard (des). URL http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

[47] W. Richard Stevens. *TCP/IP Illustrated, Vol. 1: The Protocols*. Addison-Wesley, 1993.

[48] Terry Sullivan. How much is too much? URL http://www.pantos.org/atw/35654.html.

[49] Tatsuhiro Tsujikawa. Spdylay - spdy c library. URL http://tatsuhiro-t.github.io/spdylay/.

[50] W3C. Http - hypertext transfer protocol. URL http://www.w3.org/Protocols/.

[51] Xiao Sophia Wang, Aruna Balasubramanian, Arvind Krishnamurthy, y David Wetherall. How speedy is spdy? Abril 2014.

[52] Duane Wessels. *Web Caching*. O'Reilly Media, 2001.

[53] Hubert Zimmermann. Osi reference model - the iso model of arquitecture for open systems interconnection. Abril 1980.

Apéndice A

Sitios del Experimento

HTTPS	HTTP
www.google.com	www.google.com
www.facebook.com	www.facebook.com
www.youtube.com	www.youtube.com
www.yahoo.com	www.yahoo.com
www.wikipedia.org	www.baidu.com
www.qq.com	www.wikipedia.org
www.taobao.com	www.qq.com
www.live.com	www.taobao.com
www.twitter.com	www.live.com
www.amazon.com	www.twitter.com
www.linkedin.com	www.linkedin.com
www.google.co.in	www.google.co.in
www.hao123.com	www.sina.com.cn
www.blogspot.com	www.hao123.com
www.tmall.com	www.weibo.com
www.vk.com	www.blogspot.com
www.wordpress.com	www.tmall.com
www.ebay.com	www.sohu.com
www.bing.com	www.yahoo.co.jp

Sigue en la página siguiente.

HTTPS	HTTP
www.google.de	www.vk.com
www.google.co.uk	www.yandex.ru
www.google.fr	www.wordpress.com
www.google.co.jp	www.ebay.com
www.ask.com	www.google.de
www.163.com	www.360.cn
www.msn.com	www.google.co.uk
www.google.com.br	www.google.fr
www.mail.ru	www.google.co.jp
www.microsoft.com	www.ask.com
www.google.ru	www.163.com
www.paypal.com	www.soso.com
www.google.it	www.msn.com
www.google.es	www.google.com.br
www.apple.com	www.mail.ru
www.adcash.com	www.xvideos.com
www.craigslist.org	www.microsoft.com
www.imgur.com	www.google.ru
www.neobux.com	www.paypal.com
www.amazon.co.jp	www.google.it
www.reddit.com	www.google.es
www.xhamster.com	www.apple.com
www.google.com.mx	www.imdb.com
www.stackoverflow.com	www.adcash.com
www.google.ca	www.craigslist.org
www.bbc.co.uk	www.imgur.com
www.ifeng.com	www.neobux.com
www.google.com.hk	www.amazon.co.jp
www.vube.com	www.t.co
www.blogger.com	www.reddit.com
www.google.com.tr	www.xhamster.com

Sigue en la página siguiente.

HTTPS	HTTP
www.googleusercontent.com	www.google.com.mx
www.godaddy.com	www.stackoverflow.com
www.huffingtonpost.com	www.fc2.com
www.kickass.to	www.google.ca
www.wordpress.org	www.bbc.co.uk
www.google.com.au	www.cnn.com
www.amazon.de	www.go.com
www.thepiratebay.se	www.ifeng.com
www.ebay.de	www.aliexpress.com
www.google.pl	www.xinhuanet.com
www.clkmon.com	www.youku.com
www.adobe.com	www.vube.com
www.dailymotion.com	www.google.com.hk
www.alipay.com	www.blogger.com
www.espn.go.com	www.google.com.tr
www.rakuten.co.jp	www.godaddy.com
www.vimeo.com	www.googleusercontent.com
www.google.co.id	www.huffingtonpost.com
www.ebay.co.uk	www.kickass.to
www.redtube.com	www.wordpress.org
www.blogspot.in	www.thepiratebay.se
www.flickr.com	www.gmw.cn
www.amazon.co.uk	www.google.com.au
www.cnet.com	www.amazon.de
www.dropbox.com	www.adobe.com
www.themeforest.net	www.ebay.de
www.google.com.ar	www.google.pl
www.booking.com	www.clkmon.com
www.conduit.com	www.dailymotion.com
www.aol.com	www.chinadaily.com.cn
www.youporn.com	www.espn.go.com

Sigue en la página siguiente.

HTTPS	HTTP
www.google.com.sa	www.alipay.com
www.sogou.com	www.about.com
www.flipkart.com	www.indiatimes.com
www.buzzfeed.com	www.google.co.id
www.google.com.eg	www.rakuten.co.jp
www.slideshare.net	www.vimeo.com
www.yelp.com	www.xnxx.com
www.nytimes.com	www.ebay.co.uk
www.google.nl	www.redtube.com
www.outbrain.com	www.blogspot.in
www.weather.com	www.china.com
www.google.com.tw	www.flickr.com
www.wikia.com	www.uol.com.br
www.fiverr.com	www.amazon.co.uk
www.m2newmedia.com	www.themeforest.net
www.hootsuite.com	www.dropbox.com
www.gmail.com	www.cnet.com
www.mozilla.org	www.livejasmin.com
www.google.com.pk	www.booking.com
www.wikihow.com	www.google.com.ar
www.theguardian.com	www.conduit.com
www.google.co.th	www.youporn.com
www.google.co.za	www.aol.com
www.deviantart.com	www.sogou.com
www.livejournal.com	www.flipkart.com
www.adf.ly	www.google.com.sa
www.bbc.com	www.onclickads.net
www.forbes.com	www.globo.com
www.w3schools.com	www.buzzfeed.com
www.blogfa.com	www.google.com.eg
www.ettoday.net	www.amazonaws.com

Sigue en la página siguiente.

HTTPS	HTTP
www.stumbleupon.com	www.ameblo.jp
www.wikimedia.org	www.slideshare.net
www.files.wordpress.com	www.nytimes.com
www.ku6.com	www.yelp.com
www.etsy.com	www.outbrain.com
www.bankofamerica.com	www.google.nl
www.mailchimp.com	www.wikia.com
www.indeed.com	www.fiverr.com
www.answers.com	www.google.com.tw
www.badoo.com	www.m2newmedia.com
www.google.co.ve	www.weather.com
www.torrentz.eu	www.gmail.com
www.sourceforge.net	www.hootsuite.com
www.spiegel.de	www.mozilla.org
www.avg.com	www.pconline.com.cn
www.zillow.com	www.google.com.pk
www.businessinsider.com	www.canadaalltax.com
www.foxnews.com	www.wikihow.com
www.aweber.com	www.theguardian.com
www.walmart.com	www.directrev.com
www.shutterstock.com	www.google.co.th
www.fifa.com	www.google.co.za
www.github.com	www.deviantart.com
www.mediafire.com	www.livejournal.com
www.google.gr	www.adf.ly
www.hostgator.com	www.bbc.com
www.reference.com	www.livedoor.com
www.addthis.com	www.forbes.com
www.aili.com	www.w3schools.com
www.liveinternet.ru	www.fifa.com
www.4shared.com	www.blogfa.com

Sigue en la página siguiente.

HTTPS	HTTP
www.naver.com	www.so.com
www.google.com.co	www.stumbleupon.com
www.archive.org	www.ettoday.net
www.ndtv.com	www.files.wordpress.com
www.tripadvisor.com	www.wikimedia.org
www.wix.com	www.bankofamerica.com
www.google.be	www.mailchimp.com
www.google.com.my	www.etsy.com
www.skype.com	www.indeed.com
www.onet.pl	www.badoo.com
www.statcounter.com	www.torrentz.eu
www.google.com.ua	www.google.co.ve
www.google.com.vn	www.ku6.com
www.salesforce.com	www.sourceforge.net
www.google.com.ng	www.answers.com
www.bild.de	www.spiegel.de
www.soundcloud.com	www.zillow.com
www.google.se	www.gameforge.com
www.telegraph.co.uk	www.avg.com
www.bleacherreport.com	www.businessinsider.com
www.gamer.com.tw	www.walmart.com
www.wellsfargo.com	www.foxnews.com
www.gigacircle.com	www.loading-delivery1.com
www.amazon.in	www.aweber.com
www.google.ro	www.mediafire.com
www.avito.ru	www.github.com
www.pandora.com	www.shutterstock.com
www.google.dz	www.aili.com
www.google.at	www.google.gr
www.google.com.pe	www.bet365.com
www.doublepimp.com	www.hostgator.com

Sigue en la página siguiente.

HTTPS	HTTP
www.popads.net	www.reference.com
www.rt.com	www.addthis.com
www.weebly.com	www.ask.fm
www.dmm.co.jp	www.stackexchange.com
www.google.com.ph	www.liveinternet.ru
www.espncricinfo.com	www.zol.com.cn
www.ups.com	www.4shared.com
www.php.net	www.naver.com
www.ikea.com	www.archive.org
www.wsj.com	www.google.com.co
www.goodreads.com	www.tripadvisor.com
www.taringa.net	www.yaolan.com
www.google.com.sg	www.google.be
www.snapdeal.com	www.onet.pl
www.amazon.fr	www.google.com.my
www.zedo.com	www.wix.com
www.google.cl	www.statcounter.com
www.rediff.com	www.skype.com
www.jabong.com	www.google.com.ua
www.gmx.net	www.allegro.pl
www.google.ch	www.google.com.vn
www.infusionsoft.com	www.bild.de
www.google.pt	www.baomihua.com
www.myntra.com	www.salesforce.com
www.kaskus.co.id	www.telegraph.co.uk
www.ign.com	www.google.com.ng