DNS

A lo largo de las actividades de esta/s clase/s se abordará desde distintas aristas uno de los protocolos (sistema de reglas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellas para transmitir información por medio de cualquier tipo de variación de una magnitud física) fundamentales para el correcto funcionamiento de Internet: el sistema de resolución de nombres, basado en el protocolo DNS.

Como los humanos somos mejores recordando palabras que números, se diseñó un sistema mediante el cual se puede acceder a una máquina mediante un nombre en vez de utilizar la dirección IP. A este sistema se lo conoce como DNS (Sistema de Nombres de Dominio, por sus siglas en inglés **D**omain **N**ame **S**ystem)

Cuando accedemos a un sitio web mediante una URL (Localizador Uniforme de Recursos, del inglés **U**niform **R**esource **L**ocator), se traduce dicho nombre a la dirección IP de la máquina en donde está el sitio al que se quiere acceder. Para ejemplificar el funcionamiento del protocolo DNS se realizará una analogía con la organización de un torneo deportivo escolar.

Supongamos que desde el área de Educación Física del colegio Don Bosco se está organizando un torneo deportivo en el cual va a participar el curso. El/la docente que está a cargo de la organización necesita contactarse con todo el curso, pero dispone de poco tiempo para acercarse a la escuela no pudiendo hacerlo hasta la semana siguiente. Por consiguiente, se designa a un delegado quien estará a cargo de listar los números de teléfono, nombre y apellido de todas las chicas y chicos. Además, el delegado deberá pasarle su número de teléfono al docente organizador para que pueda contactarlo.

Para la inscripción son necesarios algunos datos personales como DNI, fecha de nacimiento, deporte en el que quiere participar, etc.

Para conseguir los datos de cada participante el docente ideó una estrategia bien particular:

1. Piensa en un estudiante. Para ejemplificar, suponer que se llama Julieta Soria.
2. Llama al delegado del curso y le pide el teléfono de Julieta Soria.
3. Llama a Julieta Soria y le pide los datos necesarios para poder realizar la inscripción.

Podríamos plantear un montón de alternativas diferentes y más “eficientes” a la arriba mencionada. Por ejemplo: ¿a) Por qué el docente no llama al delegado y le pide todos los teléfonos juntos o por qué no le manda una foto por mensajería?; b) Por qué el delegado no junta todos los datos necesarios y le pasas esa lista al organizador? Obvio que todas estas propuestas también son válidas pero la analogía busca dar cuenta del funcionamiento del Protocolo DNS, que se asemeja más a los puntos 1 a 3 que a las otras alternativas

Esta primera aproximación da cuenta de modo simplificado sobre cómo se traducen las URLs en direcciones IP. En este caso, el organizador sería el usuario que quiere acceder a un sitio ingresando un dirección en el navegador o haciendo clic en un link. Esa dirección refiere a una máquina conectada a Internet que alberga el contenido de ese sitio y tiene una dirección IP particular.

1. Para obtener cuál es esa dirección IP, el usuario se contacta con una máquina que tiene una función muy especial: tiene una gran lista con los nombres de los sitios y sus direcciones IP asociadas.
2. Esta máquina haría las veces de delegado y se la conoce como servidor DNS. El usuario le pregunta al servidor DNS "*¿cuál es la dirección IP de la siguiente URL?*" y el servidor se fija en su lista y le responde cuál es la dirección IP (el número de teléfono en la analogía).
3. Ahora, el usuario ya se puede comunicar directamente con el sitio al que quería acceder porque conoce su dirección IP, pudiéndole pedir todos los datos que desea o, en otras palabras, navegando por el mismo.

En la Imagen 1 se pueden apreciar los pasos que se siguen en la traducción de la dirección de un sitio web.

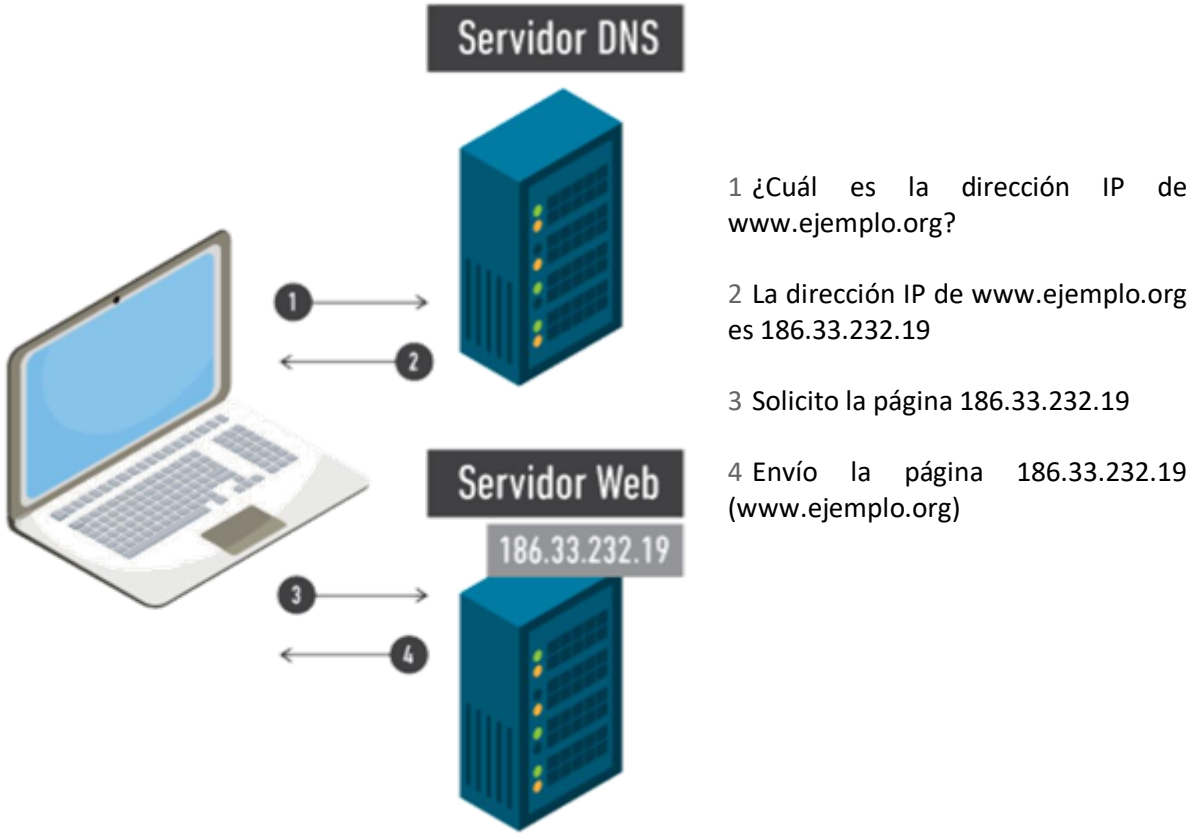


Imagen 1. Primera aproximación a cómo funciona el protocolo DNS.

Debido al éxito que tuvo el torneo realizado, el área de Deportes de la ciudad quiere replicar el torneo pero ampliándolo a todos los cursos de la escuela. El organizador sólo dispone del número de teléfono del docente de Educación Física y el docente posee una lista con los teléfonos de cada uno de los delegados de los cursos. Todo lo demás se mantiene igual.

- ¿Se podría adaptar el esquema organizativo?
- ¿Qué cambios mínimos se podrían incorporar para extender el torneo?

En este caso seguramente pensarán distintas propuestas. El concepto que se aplica es el de cascada o jerarquía:

1. El organizador piensa en un alumno o alumna en particular para contactarse con un chico o chica en particular (Julieta Soria, siguiendo el ejemplo anterior).
2. El organizador llama al docente de educación física de la escuela.
3. El docente se fija en su lista y le pasa al organizador el número de teléfono del delegado del curso de Julieta
4. El organizador llama al delegado para pedirle el número de teléfono de Julieta Soria.
5. El organizador llama a Julieta Soria y le pide los datos necesarios para poder realizar la inscripción.

- Si el torneo fuera a nivel nacional, ¿se podría ampliar esta idea?
- ¿Y qué tiene esto que ver con DNS?

Para ejemplificar, supongamos que se quiere acceder al sitio www.info.ejemplo.org. Siguiendo el primer esquema, se consulta al servidor DNS cuál es la dirección IP del sitio, el servidor responde y luego se establece la comunicación con dicha dirección IP. Esto implicaría que el servidor al que se consulta conoce todos los sitios de Internet existentes. Sin embargo, el esquema real es el de una base de datos distribuida en todo el mundo organizada de manera jerárquica:

1. La computadora que quiere acceder a este sitio le pide la dirección IP a su servidor DNS.
2. El servidor DNS se comunica con el *servidor raíz* que le dice cuál es la IP del servidor que conoce los sitios ".org".
3. El servidor DNS se comunica con el servidor que tiene toda la información sobre".org", el cual responde con la dirección IP del servidor que tiene la información sobre "ejemplo.org".
4. El servidor DNS se comunica con el servidor que tiene la información sobre ".org", el cual responde con la dirección IP del servidor que tiene la información sobre "info.ejemplo.org".
5. El servidor DNS le responde al usuario con la dirección IP del sitio.

Este mecanismo se puede apreciar en la Imagen 2 en donde se detallan cada uno de los pasos

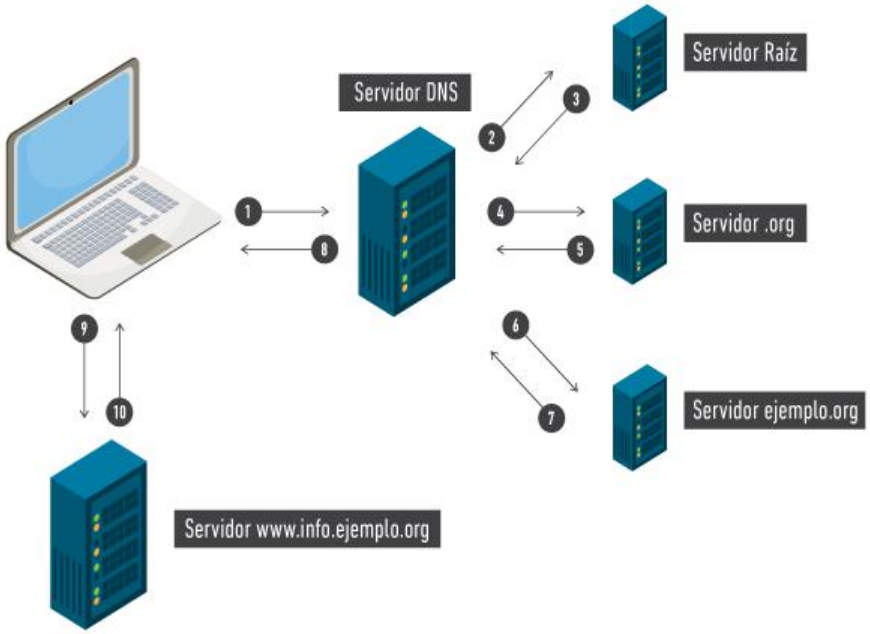


Imagen 2. Funcionamiento del protocolo DNS.

De este modo, no hay un solo servidor que tenga toda la información y resulta necesario ir descendiendo en la jerarquía. En la Imagen 3 se muestra una porción de la jerarquía de los nombres de dominio.

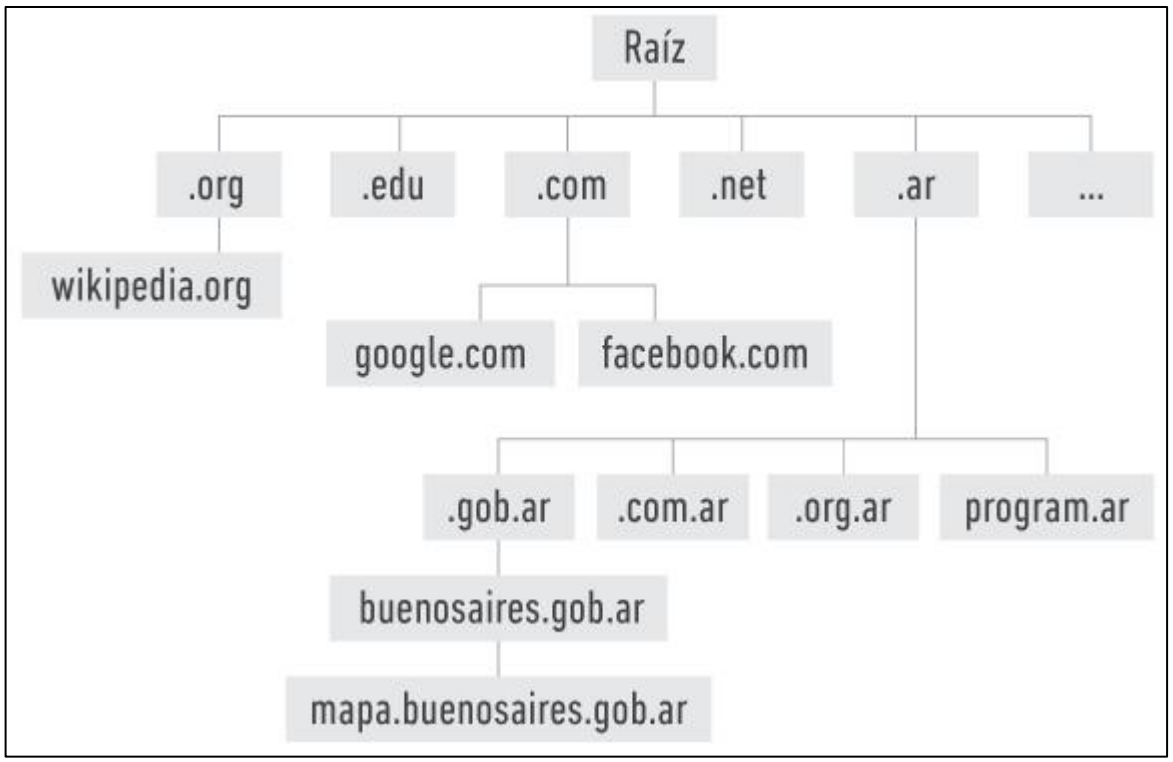


Imagen 3. Estructura jerárquica del protocolo DNS.

- Si alguien cambia de número de teléfono, ¿cómo afecta al esquema?
- ¿Es lo mismo que lo cambie uno de los participantes que el delegado?

Estas dos últimas preguntas apuntan a reflexionar que, al igual que el número de telefóno de una persona, las direcciones IP de los sitios pueden cambiar. En el caso de que el teléfono de alguno de los participantes cambie, el delegado es quien deberá reflejar este cambio en la lista de teléfonos. Si, por otro lado, el que cambiara fuera el teléfono de alguno de los delegados, debería ser el docente quien actualizara su lista.

Lo mismo ocurre en la jerarquía DNS. Si Wikipedia cambia su dirección IP, es el servidor responsable de ".org" el que debe actualizar su lista. Y si el mapa de www.mapa.buenosaires.gob.ar cambia de dirección, será el servidor responsable de "mapa.buenosaires.gob.ar" el que deba actualizar su lista con la nueva dirección IP del mapa. En este último ejemplo se observan cuatro categorías en la jerarquía: ".ar", ".gob.ar", ".buenosaires.gob.ar" y ".mapa.buenosaires.gob.ar".

IMPORTANTE

Un nombre de dominio no es lo mismo que una URL. Las URL identifican un recurso en una máquina conectada a Internet mientras que los nombres de dominio identifican a esa máquina.
Por ejemplo: http://www.wikipedia.org.es/wiki/Dirección_IP identifica el recurso "wiki/Dirección_IP" en la máquina identificada con el nombre de dominio "wikipedia.org.es".
Lo que está después de la "/" indica un recurso y lo que está antes de la "/" el nombre de dominio.

De lo expuesto anteriormente, pueden surgir entre otras, las siguientes preguntas:

- ¿En manos de quiénes están los servidores DNS?
- ¿Dónde están?
- ¿Quiénes tienen más poder en el esquema de jerarquía explicado anteriormente?
- ¿Quiénes son en "la realidad" los dueños de las listas?
- ¿Y si el dueño de alguna lista no responde más el teléfono o se le descompone?

Cuanto más alto se está en la jerarquía del esquema, mayor cantidad de números de teléfono o nombres de dominio dependen de esa lista. Por ejemplo, si el docente que tiene el listado de todos los delegados pierde la lista, el organizador no se va a poder contactar con ninguno de las/los estudiantes de la escuela. Si, en cambio, un delegado pierde la lista, solamente se ve afectado un solo curso.

En el caso de la jerarquía de servidores DNS, el servidor raíz es del que depende el resto del esquema: es el que sabe las direcciones IP de los dominios ".com", ".org", ".edu", ".net", ".gov", ".ar"

Si ese servidor se apaga, sufre una falla o es atacado no se podría acceder más a ningún sitio. Por ello, en vez de un solo servidor, se distribuyeron originariamente 13 alrededor del mundo, los 13 con la misma información. Pero, ¿se distribuyeron efectivamente alrededor del mundo? En la Imagen 4 se aprecia cómo el reparto global resultó con que EE.UU. concentrara 10 de esos 13 servidores.

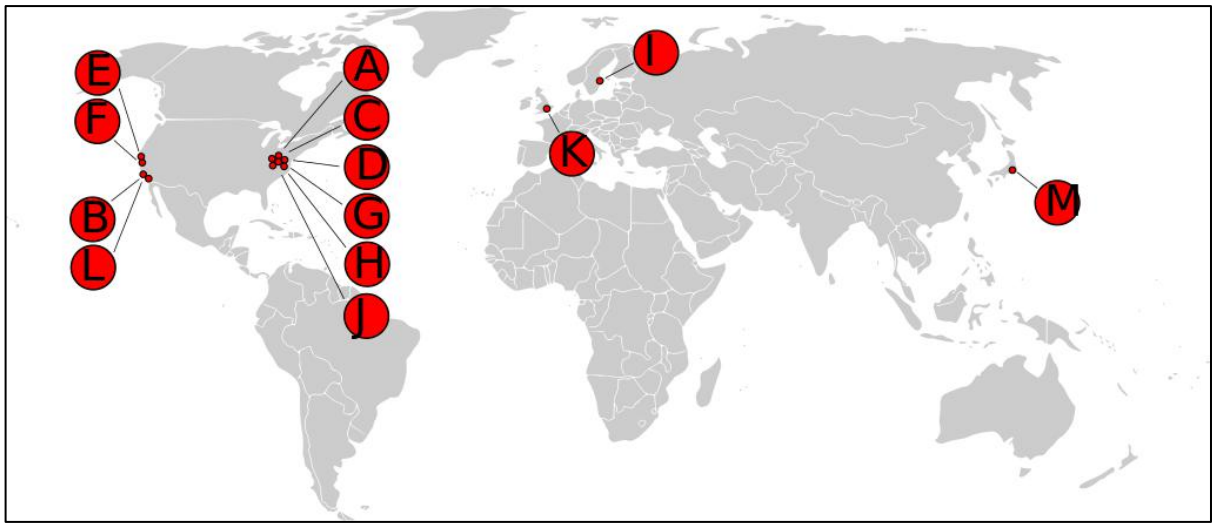


Imagen 4. Distribución geográfica original de los servidores raíz DNS.

Sin embargo, a medida que Internet fue creciendo, ese mapa fue cambiando y se fueron incorporando más servidores en distintos países del mundo. Hoy en día se cuentan con casi mil servidores aunque, como se aprecia en la Imagen 5, la distribución sigue siendo desigual (el mapa se puede explorar y acceder online en www.root-servers.org).

Imagen 5. Distribución geográfica actual de los servidores raíz DNS.

- ¿Y quiénes controlan estos servidores?
- ¿Los países donde se ubican? ¿Países y empresas? ¿ONGs?

Desde el sitio arriba indicado (www.root-servers.org) se puede apreciar en la parte de abajo, quiénes son los dueños de estos servidores raíz:

- Los casi mil servidores son controlados por 12 entidades.
- Una de esas 12 entidades es la empresa Verisign (estadounidense), que además administra el servidor DNS ".com", el dominio que más tráfico genera
- Algunas de las otras 12 entidades son la NASA, la Universidad de Maryland, la Armada de los EE.UU., la Universidad del Sur de California y el Departamento de Defensa de los EE.UU.

Actividad 1

- ¿Alguna vez les apareció la siguiente pantalla (ver Imagen 6) estando conectados a una red?
- ¿Qué podemos inferir del mensaje de error?

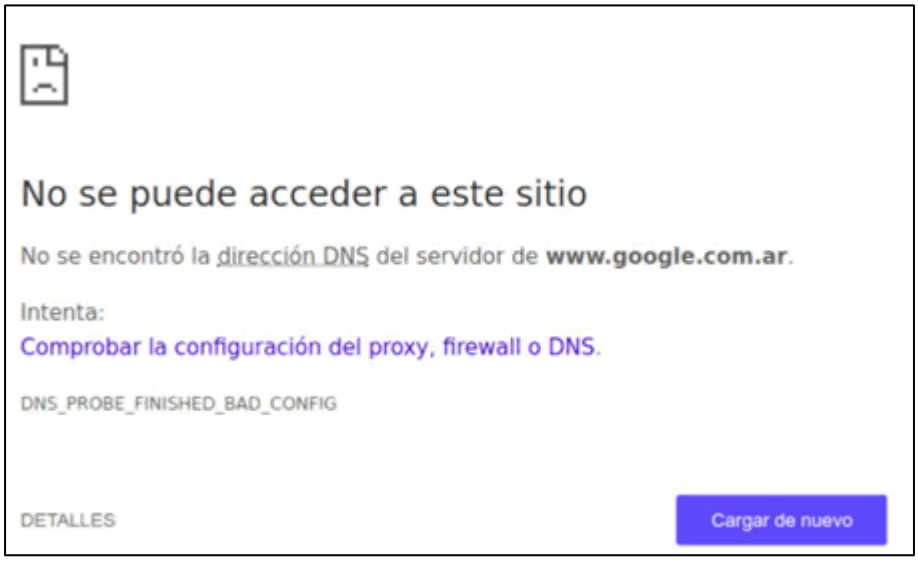


Imagen 6. Error de configuración del servidor DNS.

A veces, una red funciona perfectamente bien, pero, al querer navegar por Internet, aparece este mensaje. Si bien puede deberse a varios motivos, muchas veces pasa que la configuración del servidor DNS está mal o el servidor DNS al cual nuestra máquina se conecta tiene algún problema.

- ¿Se les ocurre alguna manera de verificar si el problema es el servidor DNS?
- ¿Cómo podemos saltear al servidor? ¿Qué servicio ofrece que podamos evitar?

Como se vio anteriormente, el protocolo DNS (a través de la jerarquía de servidores) traduce nombres en direcciones IP. Cuando una máquina se conecta a una red mediante DHCP (en inglés: **D**ynamic **H**ost **C**onfiguration **P**rotocol - protocolo de configuración dinámica de host- es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo de la red), la configuración del servidor DNS que conectará a la máquina con dicha jerarquía se configura por defecto. Si dicho servidor falla, también fallará la traducción de los nombres de los sitios web.

Para constatar si éste es el escenario, se puede "puentear" la traducción verificando si alguna dirección IP conocida es accesible desde nuestra máquina. Para ello se puede utilizar el comando "ping 157.92.5.125" en una consola / símbolo del sistema (ir a inicio, escribir cmd y presionar ENTER).

Ping envía un mensaje a una dirección IP objetivo y, si estamos conectados a Internet, se recibe un mensaje como el que se ve en la Imagen 7. Si no, se recibe un mensaje como el de la Imagen 8.

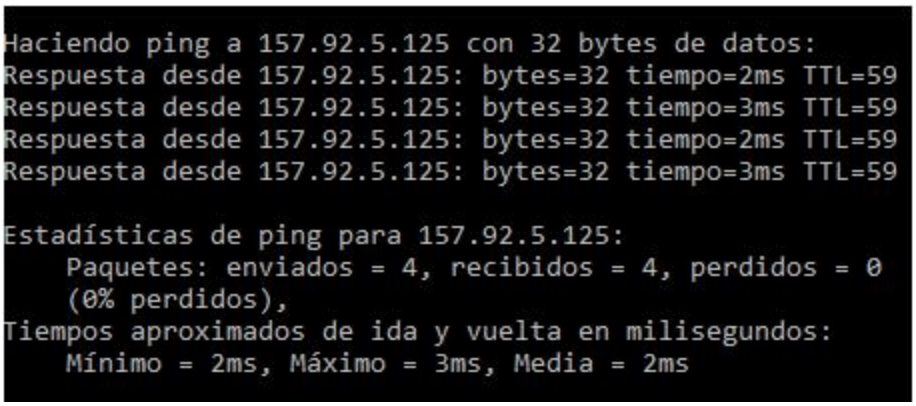


Imagen 7. Respuesta satisfactoria al ejecutar "ping 157.92.5.125" en una consola en Windows.

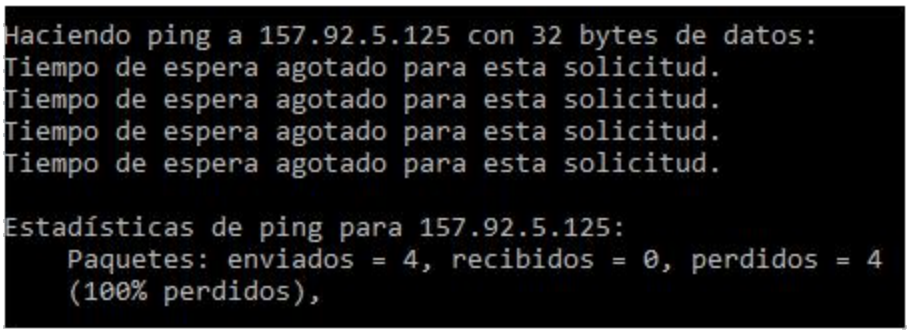


Imagen 8. Respuesta insatisfactoria al ejecutar "ping 157.92.5.125" en una consola en Windows.

IMPORTANTE

Se puede estar conectado a Internet y que la máquina a la que enviamos el ping esté configurada para no responder estas solicitudes, por cuestiones de seguridad.

Google dispone de un servicio de DNS gratuito con el objetivo de hacer más rápido el acceso a Internet. El mismo puede ser tanto la IP 8.8.8.8 como la IP 8.8.4.4. Validar desde la consola / símbolo de sistema que en ambos casos al usar el comando PING la respuesta es satisfactoria.

En el caso de que se identificara que nuestra conexión tiene problemas con el servidor DNS y que la red a la cual estamos conectados está configurada por DHCP (configuración automática), podemos configurar manualmente dicho servidor de DNS. En la Imagen 9 (propiedades de la conexión de red) se muestra cómo realizar esta configuración manual poniendo las direcciones IPs de los DNS de google explicados anteriormente.

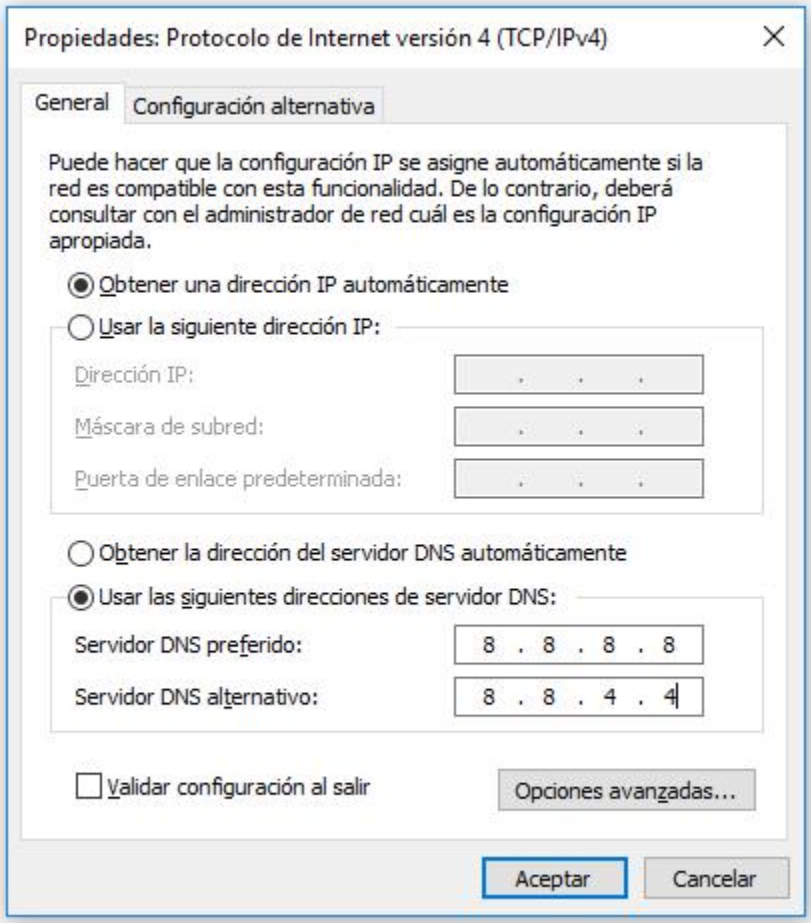


Imagen 9. Configuración manual del servidor DNS en Windows.

Actividad 2

Visualizar el siguiente video que servirá como repaso y resumen de lo visto sobre direcciones IP y DNS: https://youtu.be/5o8CwafCxnU. Cabe destacar que uno de los protagonistas del video es Vint Cerf, ingeniero de software y padre de la Internet.

Investigar y responder las siguientes preguntas:

1. ¿Cómo se hace para obtener un nombre de dominio terminado en ".ar"?
2. ¿Es gratuito o es pago? ¿Siempre fue así? En caso de ser pago, ¿cuánto sale por mes?
3. En los últimos años, ¿subió o bajó la cantidad de dominios ".ar"? ¿A qué se debe?
4. ¿Cuáles son los 15 países que más dominios tienen registrados?
5. ¿Hay alguno que te llame la atención? ¿Por qué?
6. Mencioná, al menos, 3 países en donde registrar un dominio sea gratuito.
7. Imaginá un nombre de dominio para tu sitio web y verificá que no exista. Por ejemplo: batatayqueso.com.ar aún nadie lo registró. ¿Cómo lo verificaste? Pista: no alcanza ingresando el nombre en el navegador ya que el sitio podría estar caído temporalmente.

   Justificar apropiadamente en todos los casos y citar las fuentes utilizadas.

Conclusión

El protocolo DNS y el sistema jerárquico de servidores asociado es uno de los pilares del funcionamiento de Internet. Ideado para que las personas pudieran recordar más fácilmente un sitio web (un nombre en vez de un número), la estructura física que da soporte al protocolo denota una de las marcas de origen: la distribución desigual de la infraestructura física de Internet, tema que se profundizará más adelante.

Infraestructura física

A través de la temática y distintas actividades que vamos a ver en estas clases, la idea es poner de manifiesto el nivel físico que sustenta el funcionamiento de Internet conociendo entre otra cosa, como se conecta Argentina a través de Internet con otros países del mundo. Este puntapié inicial dará lugar a incursionar en el mundo de los cables submarinos y la red global de conexiones. Se discutirá sobre cómo es el mapa y quiénes son los dueños de toda esa infraestructura lo cual permitirá hablar de la jerarquía de los ISPs y la concentración del mercado de los proveedores de nivel 1 (se explicará más adelante)

Comenzaremos este tema (infraestructura física) realizando la siguiente pregunta disparadora que servirá para introducir cómo se conecta Argentina a Internet con otros países:

- ¿Cuál es el destino turístico argentino que más se relaciona con Internet? ¿Por qué?

La respuesta es **Las Toninas**, en el Partido de la Costa de la Provincia de Buenos Aires, es la "capital nacional de Internet" ya que fue la elegida para conectar los cables que comunican a la Argentina con gran parte del mundo. Estos cables llegan a una estación de amarre ubicada en la costa de la ciudad y viajan miles de kilómetros a través del lecho marino.

En la Imagen 10 se muestran algunas capturas sobre cables submarinos de fibra óptica, los cuales pueden atravesar océanos enteros.

Imagen 10. (a) Barco partiendo de la costa para colocar el cable submarino.
(b) Buzo reparando un cable submarino averiado. (c) Cable submarino de fibra óptica por dentro.

- ¿Cuántos cables imaginan que salen desde Las Toninas? ¿A dónde llegan?
- ¿Y las conexiones entre otros países?
- En el planisferio dibujen cómo piensan que son estas conecciones uniendo distintos puntos del mapa mediante líneas que simulen a los cables.

- Mapa real y actual de los cables submarinos a nivel mundial: https://www.submarinecablemap.com/#/ (ver Imagen 11)

- Mapa de todas las conexiones, no solamente las submarinas: http://global-internet-map-2017.telegeography.com/

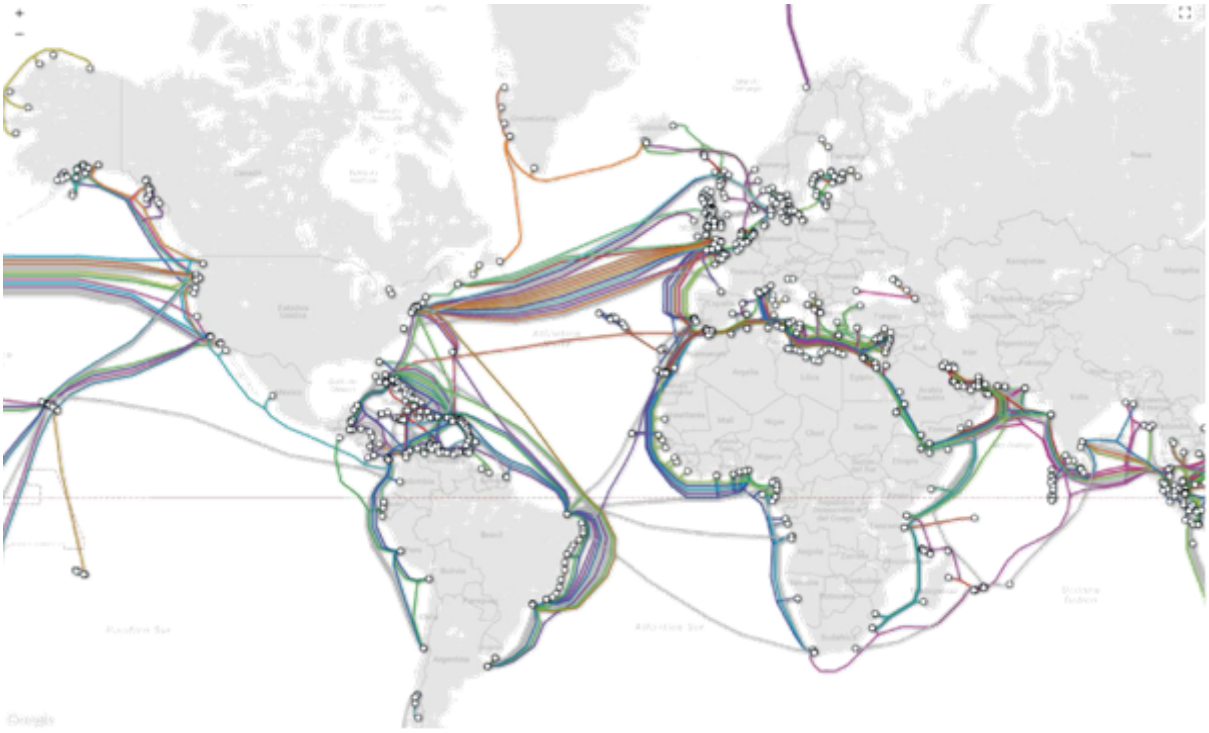


Imagen 11. Mapa global de los cables submarinos de Internet.

- ¿Le encuentran algún problema al mapa real?
- ¿En qué país se concentran la mayor cantidad de cables?
- ¿Si EE.UU. sufriera un gran apagón, qué pasaría con Internet?
- ¿Y si Las Toninas sufre un apagón?

Con estas preguntas evidenciamos que la estructura física de conexiones de Internet está sumamente centralizada teniendo a EE.UU. como uno de sus nodos más fuertes. Esta concentración conduce a que muchas veces se tenga que pasar por ese país para acceder desde Argentina a un sitio radicado en un país vecino, se tenga que pasar por conexiones que pasan por USA. Además, como se ve en la Imagen 12(a), si EE.UU. lo decidiera, podría "apagar" una gran porción de la Internet ya que si

desconecta sus cables muchos países quedarían desconectados entre sí puesto que usan a Estados Unidos como intermediario. En cambio, si hubiese una topología de red más parecida a la Imagen 12(b) permitiría que las conexiones entre los distintos puntos no se vean afectada por la falla en uno solo de ellos.

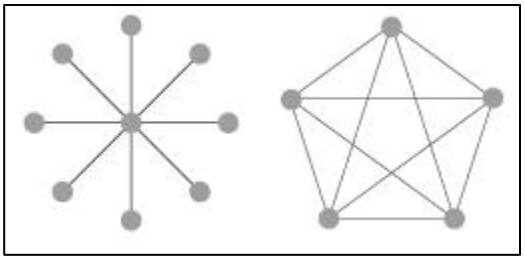


Imagen 12 (a). Topología de red centralizada. 12 (b). Topología de red distribuida.

IMPORTANTE

Colocar los cables en el lecho marino es una tarea de ingeniería que requiere mucha planificación y preparación. Los avances técnicos no suplieron la gran operación humana que se necesita para subir rollos de miles de kilómetros de cable a la bodega de un barco, enterrarlo mil metros saliendo de la costa y luego completar el tendido en el fondo del mar respetando una ruta precisa y previamente definida. ***Para lograrlo se necesita casi lo mismo que en 1850, cuando se instaló el primer cableado entre Gran Bretaña y Francia a través del Canal de la Mancha.***
En el siguiente video se muestran las distintas fases de esta tarea faraónica.
https://youtu.be/H9R4tznCNB0

Actividad 3

Para continuar descubriendo la infraestructura física de Internet, en esta actividad se pondrá el foco en quiénes construyen, mantienen y desarrollan toda esa infraestructura.

Armar grupos de 5 o 6 alumnos máximo y responder las preguntas del siguiente cuestionario luego de su búsqueda e investigación en Internet y basándose en los siguientes links:

a. Internet en pocas manos
b. Por tierra, mar y aire: cómo nos conectamos a Internet los argentinos
c. Internet, pendiente de un cable: corte en Las Toninas desnudó falencias de la conexión argentina

- ¿Qué empresas que brinden Internet conocen?
- ¿Cuántos kilómetros de cables submarinos hay?
- ¿Quiénes colocaron esos cables? ¿Será muy caro? ¿Quiénes los mantienen y reparan si se rompen?
- ¿Con qué países se conecta Argentina de manera directa?
- ¿Cuántos cables submarinos llegan a Las Toninas?
- ¿Quiénes son los dueños de esos cables?
- ¿Son los mismos que nos brindan el servicio de Internet en las redes domésticas de Argentina?
- ¿Cuál es la empresa que concentra más tráfico que el resto? ¿Qué porción del mercado controla? ¿Qué consecuencias imaginás que puede traer esta situación?

En la actividad anterior vimos que la información requiere de conexiones físicas para poder viajar entre 2 puntos cualesquiera del planeta. Establezcamos relaciones entre lo visto sobre ***representación de la información*** (1er trimestre) y las distintas ***representaciones gráficas de Internet***. En función a ello, analizar las siguientes preguntas:

- Cuando enviamos un mensaje, un audio, una foto o un video, ¿cómo se transmite esa información?
- Y antes de enviarla, ¿cómo se representa en cada dispositivo?
- ¿Por dónde viajan esos 0s y 1s? ¿Son 0s y 1s realmente o qué son?

El objetivo de estas preguntas es recuperar las nociones centrales de lo trabajado durante la primera parte de la materia acerca de que para poder representar los distintos tipos de información de manera digital es necesario establecer sistemas de representación que sean conocidos por las partes que van a codificar y decodificar dicha información para poder interpretar correctamente.

Asimismo, es importante destacar que esos 0s y 1s con los que operan las computadoras no son más que una abstracción para referirse a 2 niveles de energía distintos. Por lo tanto, como la cantidad de elementos o símbolos que se utilizan para representar la información en las computadoras es 2, se habla de sistemas binarios.

Las comunicaciones entre computadoras ocurren también mediante el intercambio de bits, es decir, mediante el envío de 0s y 1s. Sin embargo, cómo se abstraen los 0s y 1s dependerá del medio por el que se transmita la información. En el caso de las comunicaciones a través de cables de cobre (como

el que se usa para el teléfono fijo) se utiliza electricidad, en el del WiFi una porción del espectro de las ondas de radio y en el de la fibra óptica la luz (los cables submarinos utilizan la fibra óptica). En cada tecnología se requiere determinar cómo, a través de ese medio, se pueden diferenciar 2 niveles de energía distintos.

Además, cada medio determina cuán rápido viaja la información, cuántos bits se pueden enviar por segundo, si es un medio con mucha interferencia y, por ende, se generan muchos errores (0s que eran 1s y 1s que eran 0s), etc.

Ejemplo:
Cuando Braian le envía información por Internet a Daniela, ésta no viaja directamente desde la computadora de Braian a la de Daniela a través de un único cable que los conecta o una señal inalámbrica súper poderosa, sino que pasa por un montón de computadoras (y redes) intermedias.

En particular, debe pasar por al menos, la puerta de enlace a la que está conectado Braian, la empresa proveedora que le está brindando el servicio de Internet a Braian y, análogamente, el camino inverso hasta llegar a la computadora de Daniela. Eventualmente también podría tener que pasar por otros países a través de cables submarinos.

Por lo tanto, para que la información binaria, representada en cada medio físico de modos diferentes, llegue desde la computadora de Braian hasta la de Daniela, se debe lograr primero que dos computadoras puedan comunicarse entre sí. Suponer que se tienen dos computadoras conectadas y que una le envía a otra la información de la Imagen 13. ¿Cuál es dicha información? Es decir, ¿cuál es la secuencia de 0s y 1s que le envía?

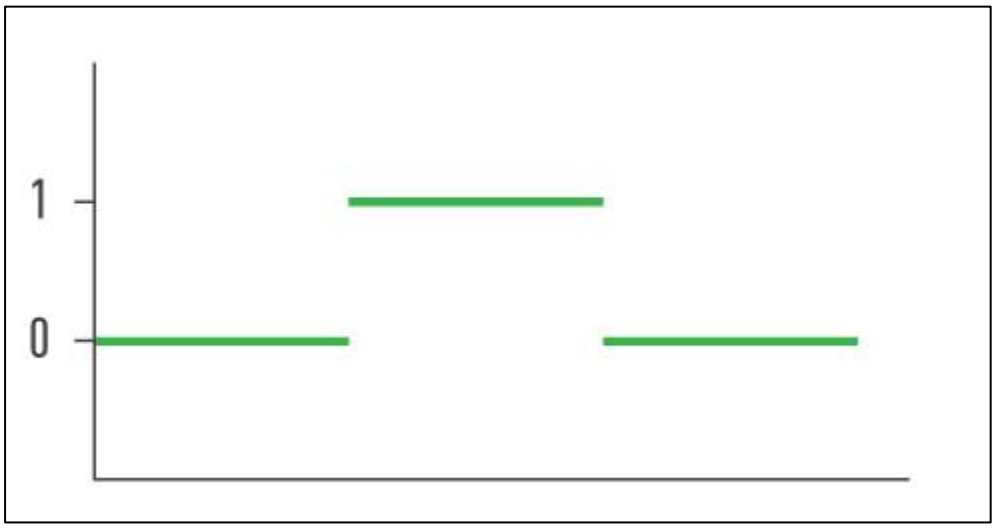


Imagen 13. Mensaje binario transmitido entre 2 computadoras.

Al ver la imagen anterior la tentación es responder “0-1-0”. Sin embargo, también podría ser “0-0-1-1-0-0” o “0-0-0-0-1-1-1-1-0-0-0-0” o cualquier otra tira de igual cantidad de 0s, 1s y 0s. Si la máquina desde donde sale el mensaje envía 3 ceros, 3 unos y por último 3 ceros, ¿cómo puede hacer la computadora que lo recibe para leer la secuencia 0-0-0-1-1-1-0-0-0 y no 0-1-0?

Es importante remarcar que las computadoras lo único que pueden ver son los “ceros” y “unos” que pasan a través del cable. No se pueden enviar otro tipo de señales o mensajes por fuera de este cable.

La respuesta a las preguntas anteriores es la noción de sincronización. La computadora que envía la información escribe 0s y 1s en el cable cada cierto período fijo de tiempo. Para ejemplificar, suponer que lo hace cada 10 ns (nanosegundos), es decir, escribe 1 bit cada 0,00000001 segundos. La computadora que los recibe lee en el cable cada el mismo período de tiempo, es decir, 10 ns. Por lo tanto, ambas computadoras están sincronizadas (cuentan con una surte de reloj interno), escriben y leen los bits a intervalos regulares de tiempo.

En la Imagen 14 se muestra que el mensaje compuesto por 0s, 1s y 0s del ejemplo anterior, al explicitar cuál es el intervalo de tiempo utilizado para sincronizar a la máquina, resulta ser la secuencia "0-0-1-0-0-0-1-1-0".

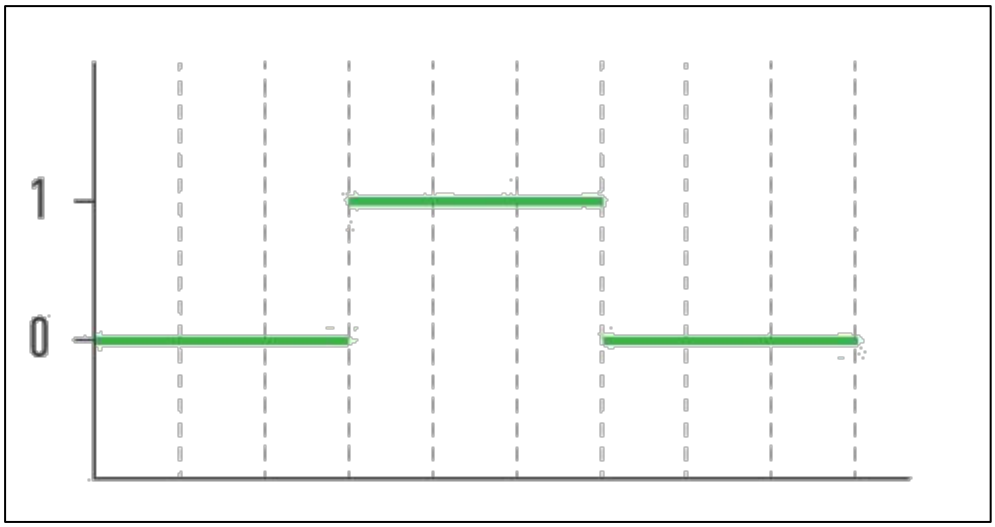


Imagen 14. Mensaje binario transmitido entre 2 computadoras con el detalle de la sincronización.

Lo expuesto anteriormente nos permite incorporar un concepto que probablemente hayan escuchado mencionar: ***el ancho de banda.***

Se refiere a la cantidad de información que se puede enviar por unidad de tiempo por un canal de comunicación. Generalmente el ancho de banda se mide en bit/s, Kbit/s, Mbit/s o Gbit/s, es decir, 1, 1.000, 1.000.000 y 1.000.000.000 de bits por segundo. El ancho de banda depende de la tecnología de comunicación siendo la fibra óptica la más rápida hoy día.

A modo de síntesis de los conceptos trabajados anteriormente, les dejo del siguiente video: https://youtu.be/ZhEf7e4kopM

Conclusión

Conocer el mapa físico de Internet y cuáles son los jugadores principales en este mercado es fundamental para comprender las relaciones de poder y las tensiones que se generan entre empresas, Estados y usuarios. Además de la visión macro sobre la infraestructura física de Internet, comprender cómo hacen 2 computadoras para poder comunicarse entre sí permite establecer una fuerte relación con los aspectos vistos durante la primera parte de la materia y trabajar dos aspectos centrales para la transmisión de información digital: la sincronización y el ancho de banda.

Actividad 4

Nuevamente en grupos de 5 o 6 alumnos como máximo, deberán discutir y determinar en función a ***la comparativa de medios de transmisión de la información***, cuál de las siguientes 5 tablas es correcta justificando apropiadamente la respuesta.

Para ello podrán buscar información en Internet debiendo indicar/nombrar la fuente utilizada.

Medio	Se usa para transmitir información	Tecnologías asociadas	Velocidad	Pérdida de señal	Costo
Ondas de radio	Sí	3g, 4g, WiFi, Bluetooth, Satelital	Rápida	Sí	Depende de la tecnología
Microláminas de grafito	No	-	-	-	-
Cable de cobre	Sí	Ethernet, ADSL	Rápida	Sí	Accesible
Fibra óptica	Sí	Ethernet	Muy rápida	No	Cara
Rayos gamma	No	-	-	-	-

Tabla 1

Medio	Se usa para transmitir información	Tecnologías asociadas	Velocidad	Pérdida de señal	Costo
Ondas de radio	Sí	3g, 4g, WiFi, Bluetooth, Satelital	Rápida	No	Depende de la tecnología
Microláminas de grafito	No	-	-	-	-
Cable de cobre	Sí	ADSL	Rápida	Sí	Accesible
Fibra óptica	Sí	Ethernet	Muy rápida	Sí	Cara
Rayos gamma	No	-	-	-	-

Tabla 2

Medio	Se usa para transmitir información	Tecnologías asociadas	Velocidad	Pérdida de señal	Costo
Ondas de radio	No	-	-	-	-
Microláminas de grafito	No	-	-	-	-
Cable de cobre	Sí	Ethernet, ADSL	Rápida	Sí	Accesible
Fibra óptica	Sí	Ethernet	Muy rápida	No	Cara
Rayos gamma	Si	3g, 4g, WiFi, Bluetooth, Satelital	-	-	Depende de la tecnología

Tabla 3

Medio	Se usa para transmitir información	Tecnologías asociadas	Velocidad	Pérdida de señal	Costo
Ondas de radio	Si	3g, 4g, WiFi, Bluetooth, Satelital	Rápida	Sí	Depende de la tecnología
Microláminas de grafito	Sí	Ethernet	Lenta	Sí	Cara
Cable de cobre	Sí	Ethernet, ADSL	Rápida	Sí	Accesible
Fibra óptica	Sí	Ethernet	Muy rápida	No	Cara
Rayos gamma	Si	-	-	-	-

Tabla 4

Medio	Se usa para transmitir información	Tecnologías asociadas	Velocidad	Pérdida de señal	Costo
Ondas de radio	Si	3g, 4g, WiFi, Bluetooth, Satelital	Rápida	Sí	Depende de la tecnología
Microláminas de grafito	No	-	-	-	-
Cable de cobre	Sí	Ethernet, Satelital	Muy rápida	Sí	Cara
Fibra óptica	Sí	Ethernet, ADSL	-	-	-
Rayos gamma	-	-	-	-	-

Tabla 5

Actividad 5: Sincronización

- Armar grupos de a dos (parejas)
- Cada pareja debe hacer una suerte de tarjeta que de un lado será azul y del otro roja.
- Los dos miembros de la pareja deberán disponerse enfrentados y la tarjeta se colocará en el medio entre ellos.
- Uno deberá cumplir con el rol de emisor y el otro con el rol de receptor.
- Quien sea el emisor, deberá enviar los mensajes de la imagen 15 a su compañera o compañero.
- Los mensajes consistirán en una secuencia de azules y rojos. Para enviar un mensaje, el emisor sólo podrá dar vuelta o dejar como está a la tarjeta azul y roja que está dispuesta entre ambos.
- El receptor deberá ir tomando nota de los colores que el emisor vaya mostrando y, al finalizar todas las secuencias, corroborarán si todos los mensajes se corresponden entre emisor y receptor.
- Una secuencia comienza cuando el emisor dice la palabra clave “ya” y finaliza cuando dice “listo”.
- Durante la emisión de los mensajes no es posible para ninguno de los dos participantes puedan decir nada más.
- El único medio de transmisión de información será la tarjeta y las palabras “ya” y “listo” para iniciar y finalizar el envío de un mensaje respectivamente.

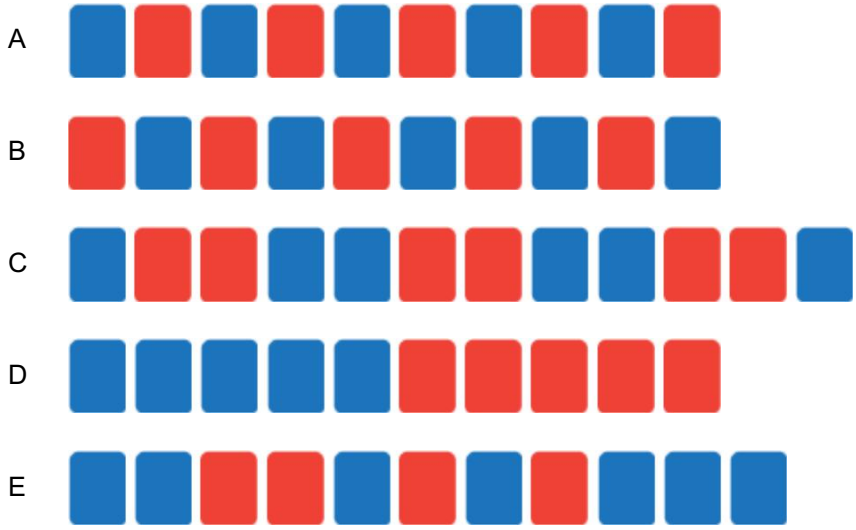


Imagen 15. Mensajes binarios que el emisor envía al receptor.

En los primeros 2 mensajes, al tratarse de mensajes en donde se alterna constantemente la tarjeta, es probable que haya coincidencia entre el mensaje que se quiso enviar y el que se recibió. A partir del tercero, como la alternancia entre colores no es uno y uno, es probable que haya diferencias entre los mensajes, a menos que el emisor haya utilizado alguna estrategia para “marcar el pulso”. Si éste fuera el caso, habrán recurrido a la sincronización para poder enviar mensajes de longitud arbitraria con un mismo símbolo.

Conclusiones

Problemas

- Con las reglas actuales no hay forma de saber cuántas tarjetas seguidas del mismo color ocurrieron, salvo por la intuición del receptor. ¿Y en qué se basa la intuición del receptor?

- ¿Qué aprendieron de los mensajes (a) y (b)? Justamente, dichos mensajes le deberían dar al receptor una idea de cuánto tarda el emisor en dar vuelta una tarjeta (más allá de que no sepa que el mensaje es perfectamente alternado), información que podría utilizar el receptor para inferir en el resto de los mensajes.

- Sin embargo, hay situaciones en las que el emisor tarda más, indicando que posiblemente esté enviando varias veces el mismo color. Si bien esto solamente es una intuición que el receptor pudo haber generado, está atacando el problema central: tratar de sincronizarse con el emisor.

De lo expuesto anteriormente, surge la siguiente pregunta:

¿Qué elementos se pueden utilizar para que el emisor y el receptor estén sincronizados y ambos dos sepan cuánto dura el envío de un color?

Alternativas de solución

- Utilizar un reloj o un cronómetro y asignar cierto tiempo al envío de cada color. Por ejemplo, se enviará 1 color cada 5 segundos.
- Otra idea podría ser utilizar un metrónomo (aparato utilizado para indicar tiempo o pulso de las composiciones musicales) que marque el tiempo de cambio de color.
- Otra posibilidad es utilizar algún método de sincronización sonoro como, por ejemplo, que el emisor de un golpe a la mesa cada vez que envía un color.
- En todos los casos, tanto emisor como receptor se garantizan estar sincronizados respecto de cada color que se está enviando.

IMPORTANTE

Si bien puede ocurrir algún error en la transmisión del mensaje, es probable que con cualquiera de los métodos de sincronización explicados, al comparar los mensajes del emisor y del receptor, haya poca diferencia entre ambos.
A las computadoras también les ocurre que tienen errores en la transmisión, errores que pueden ocurrir por falta de sincronización. ¿Cómo se sincronizan las computadoras? Con relojes de altísima velocidad que fraccionan el tiempo y permiten a la computadora sensar el canal de comunicación a una frecuencia constante.

Ruteo

En el recorrido realizado hasta ahora ya surgió una de las características constitutivas de Internet: cuando dos dispositivos quieren comunicarse entre sí, en general no están unidos punto a punto, sino que se conectan a través de varias redes intermedias.

El objetivo principal de este tema es comprender cómo hace la información para "atravesar" todas estas redes intermedias y llegar a buen puerto. Para ello realizaremos una "actividad interactiva" en la cual las/los estudiantes harán las veces de routers y para comprender cómo sucede que la información llegue de un punto a otro de la red.

Actividad 6

En las clases anteriores vimos que, en general, las computadoras no están conectadas 1 a 1 sino que para que un dato llegue a destino tiene que pasar por varias computadoras entre el emisor y el receptor de dicha información. Por ejemplo, en el gráfico realizado en la clase de protocolo IP vimos que los dispositivos estaban conectados a un router o a una antena que a su vez se conectaba con otras regiones de la Internet. Asimismo, en este apunte vimos que a nivel global existen conexiones entre algunos puntos específicos del planeta y que, para poder llegar a destino, los ISPs locales reenvían la información a otros ISPs de mayor jerarquía. ***Todos estos aspectos enfatizan la condición de "red de redes" de internet.***

- ¿Cómo hace una computadora para saber todo el recorrido que debería realizar la información que quiere enviar a un determinado destino?
- ¿Cómo se determina ese camino?

Imagen 16. Red conformada por Lau, Fer, Mica, Santi y Cami.

Para responder estas preguntas, la actividad constará de dos partes. En la primera 5 estudiantes representarán una red de ejemplo.

En la Imagen 16 se muestra una disposición posible en la que participan Lau, Fer, Mica, Santi y Cami.

Todos están dispuestos de manera tal que se puedan ver entre sí. Las uniones pueden ser hilos, sogas o tubos y representan a las conexiones físicas: ya sea un cable o el alcance de una señal wireless. Las chicas y chicos representan el router de una red, es decir, la interconexión entre 2 redes.

El objetivo es que Lau le envíe un mensaje a Santi. Para ello, se utilizará una pulsera, un círculo hecho de papel o cualquier otro elemento con forma de aro, el cual pueda pasar a través de los hilos. Esta tarea estará a cargo de un sexto alumno X quien deberá ir pasado el aro desde Lau hasta llegar a Santi.

Todas las alumnas y alumnos de la clase, los que están participando de la escena y los que no, deberán elegir un camino que X pueda realizar con el aro para poder entregar satisfactoriamente el mensaje.

Como se muestra en la Imagen 17, hay 2 caminos posibles:

- Lau→Mica→Santi
- Lau→Fer→Santi

De esta primera aproximación se pueden extraer algunas conclusiones (no todas realistas):

- Puede haber varios caminos para que un dato llegue a destino.
- Todos los routers conocen todas las conexiones de la red (lo que se conoce como la topología de la red).
- Cualesquiera de los 2 caminos parecen igual de buenos/malos.

En la realidad de Internet, generalmente ocurre que haya varios caminos (mucho más que dos) pero no es cierto que los routers conozcan toda la estructura de Internet. A su vez, para determinar si un camino es mejor que otro se suelen utilizar distintos criterios: cantidad de pasos o saltos, ancho de banda, distribución de carga, etc.

Por simplicidad, durante esta clase sólo usaremos la cantidad de saltos como métrica para elegir entre 2 caminos posibles. En la representación de recién, los caminos tienen 2 saltos por lo que ambos son igual de buenos.

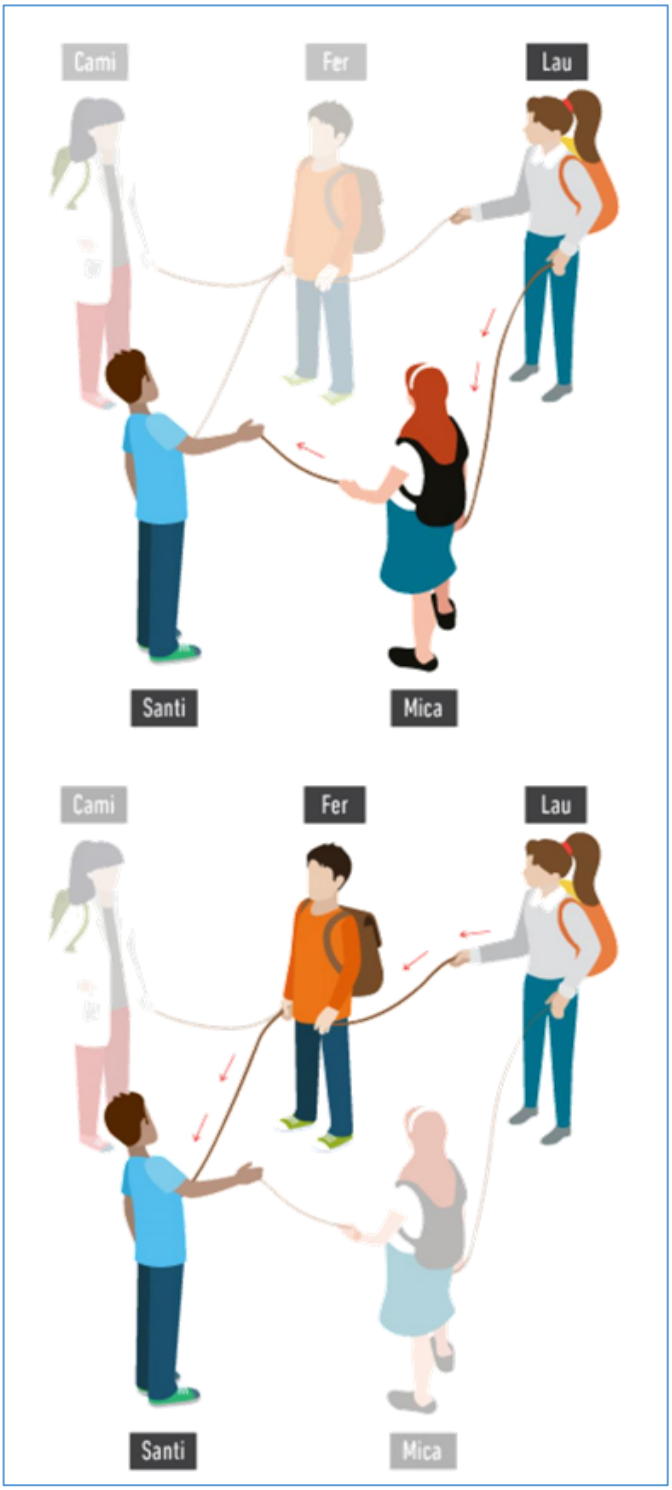


Imagen 17. Caminos posibles que podría tomar un dato enviado por Lau a Santi.

A continuación, se complejizará la actividad anterior con el objetivo de representar a Internet de un modo más realista.

Imagínense otro grupo de cinco estudiantes que tienen los ojos vendados. Esta idea serviría para que no puedan ver cómo es la estructura de red de la que formarían parte (ver imagen 18)

Supongamos que a cada uno se le dice en voz baja con quién está unido a través de su mano derecha y a quién de su mano izquierda.

Por ejemplo, a Juli se le dirá en secreto que en su mano derecha está conectado con Nati y en su mano derecha con Caro.

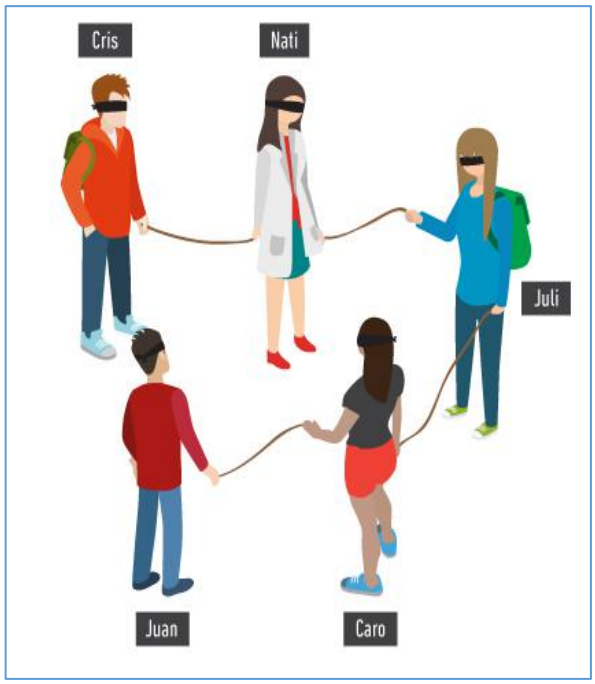


Imagen 18. Red conformada por Juli, Caro, Nati, Juan y Cris.

Supongamos que Juli tiene que enviarle un mensaje a Juan. Para ello, Juli le debe pedir a Her (el encargado de transportar el aro-mensaje) que pase el aro por la cuerda de su mano derecha o por la de su mano izquierda.

Naturalmente Juli no va a poder saber si pedirle a Her que envíe el aro a través de Nati o a través de Caro y, dada la estructura de la Imagen 18, tiene 50% de probabilidades de acertar. ¿Podría Juli asegurar con total certeza por cuál de los dos hilos hay que enviar el mensaje? Con este conjunto de reglas es imposible que Juli pueda asegurar sin riesgo a equivocarse cuál es el camino correcto.

Por lo visto anteriormente y hablando de Internet, nos podrían surgir las siguientes preguntas:

- ¿Cómo se hará en Internet para que los mensajes lleguen a destino?
- ¿Se enviarán mensajes por todos los caminos posibles?
- ¿Se enviará el mensaje por algún camino y si llega bien y si no mala suerte?

Enviar el mensaje por algún camino al azar y que la suerte lo acompañe haría que Internet funcionase realmente mal ya que, en la realidad, son más los caminos incorrectos que los correctos. Por otro lado, si se enviaran mensajes por todos los caminos posibles se saturaría Internet con demasiados mensajes redundantes cuando con enviar solamente uno por un camino correcto basta.

Para resolver este problema cada router arma una tabla en donde se indica, para cada destino de la red, cuál hilo (o interface) utilizar y cuántos saltos se deben hacer para llegar allí.

Para ejemplificar lo expuesto anteriormente, podemos ejemplificarlo con la tabla de ruteo de Nati, como se ve en la Tabla 1

Llegar a	Empezar por	Cantidad de saltos
Cris	Cris	1
Juli	Juli	1
Caro	Juli	2
Juan	Juli	3

Tabla 1. Tabla de ruteo de Nati.

En la Tabla 2, se ven las tablas de ruteo de Juan, Juli, Nati, Cris.

Tabla de Juan		
Llegar a	**Empezar por**	**Cantidad de saltos**
Caro	Caro	1
Juli	Caro	2
Nati	Caro	3
Cris	Caro	4

Tabla de Juli		
Llegar a	**Empezar por**	**Cantidad de saltos**
Nati	Nati	1
Caro	Caro	1
Cris	Cris	2
Juan	Juan	2

Tabla de Caro		
Llegar a	**Empezar por**	**Cantidad de saltos**
Juan	Juan	1
Juli	Juli	1
Nati	Juli	2
Cris	Juli	3

Tabla de Cris		
Llegar a	**Empezar por**	**Cantidad de saltos**
Nati	Nati	1
Juli	Nati	2
Caro	Nati	3
Juan	Nati	4

Tablas 2. Tablas de ruteo de Juan, Juli, Caro y Cris.

Para que Her pueda enviar el mensaje desde Juli a Juan se deberán seguirán los siguientes pasos:

1. Juli le pide al encargado de su tabla de ruteo si para llegar hasta Juan debe enviar el mensaje a través de Nati o de Caro.
2. El encargado de la tabla de ruteo de Juli le dice por dónde empezar (Caro).
3. Her pasa el mensaje desde Juli hasta Caro.
4. Se repite el proceso con Caro y el encargado de su tabla de ruteo.
5. Her pasa el mensaje desde Caro hasta Juan.
6. El mensaje llega a Juan.

Una vez entregado el mensaje a Juan, si se cortará el hilo que une a Caro con Juan:

- ¿Cómo hace Juli para enviarle el mensaje a Juan?
- Así como están, ¿las tablas siguen representando la estructura de la red?
- ¿Qué creen que habría que hacer?

En este escenario, lamentablemente Juli no le va a poder entregar el mensaje a Juan. Lo mismo ocurriría si Juan "se apagara". Estas situaciones pasan constantemente y los algoritmos de ruteo lo que hacen es actualizar dinámicamente sus tablas, es decir, cada cierto tiempo verifican si la tabla que tienen está bien o hay que cambiar algo. En este escenario, Cris, Nati, Juli y Caro deberían poner en su tabla que no es posible llegar hasta Juan, notándolo con algún símbolo específico.

Otra situación que puede ocurrir es que, al actualizar las tablas, cambie la ruta entre dos puntos. Esto ocurre con frecuencia ya que Internet es un sistema dinámico que cambia su estado constantemente por lo que "el mejor" camino entre dos dispositivos puede ir cambiando a lo largo del tiempo.

Para que un mensaje viaje desde una computadora A hasta una computadora B, se debe establecer una ruta entre A y B. Primero, la computadora le envía el mensaje al router al que está conectado. El router se fija en su tabla a qué otro router le tiene que enviar el mensaje para llegar a B y ese proceso se repite hasta que el mensaje llega al router al que está conectado B, el cual se lo envía a B.

En la realidad no ocurre que todos los routers tengan constantemente actualizada la información de todas las redes, sino que, en general, conocen algunas pocas redes. Cuando tienen que enviar un mensaje a una red que no conocen, se lo envían al ISP que les está prestando el servicio y éste se fija en sus tablas (mucho más voluminosas que la de un router estándar) o le pregunta a otros ISPs si saben qué ruta seguir.

Es bastante frecuente que cuando desde un dispositivo situado en Argentina se quiere enviar un mensaje a otro dispositivo situado también en Argentina, el camino que recorre el mensaje pasa por otros países, principalmente por Estados Unidos. Si bien parece anti-intuitivo, muchas veces estos caminos resultan más rápidos que un camino local. Esto se debe a que por razones más históricas y políticas que tecnológicas o geográficas muchas de las conexiones con USA tienen mejor ancho de banda, latencia, etc. que conexiones locales por lo que, a pesar de que la información recorra más distancia, llega más rápido.

El otro aspecto a tratar es lo que sucede cuando se quiere entrar a un sitio web y éste no carga a pesar de que tenemos Internet (podemos enviar y recibir mensajes, entrar a otros sitios, etc.).

¿Está caído el sitio o no hay ninguna ruta que conecte a mi dispositivo con dicho sitio? Para averiguarlo, se pueden utilizar distintas páginas web que, introduciendo el link al que se quiere acceder, verifican si desde otros lugares del planeta sí se puede acceder. Uno de estos sitios es http://downforeveryoneorjustme.com.

En la Imagen 19 se muestra una captura del resultado de preguntar si el sitio www.donbosco.edu.ar está caído o no.

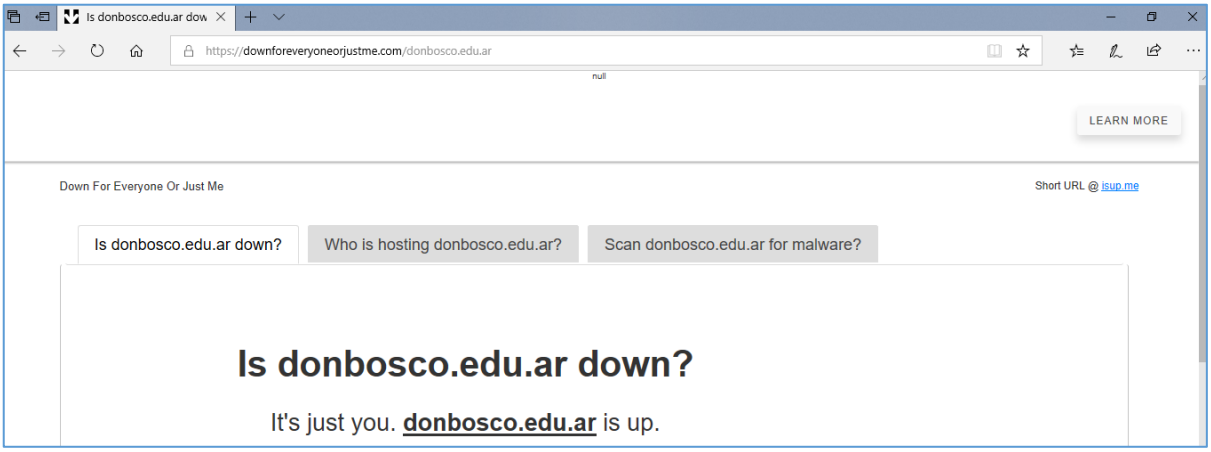


Imagen 19. Resultado de consultar en downforeveryoneorjustme.com si www.donbosco.edu.ar está caído o no.

Conclusión

La información, desde el momento en que es enviada desde un dispositivo de origen atraviesa en su recorrido numerosos routers que la van redirigiendo hasta llegar al dispositivo destino. Este camino generalmente no es único y puede cambiar a lo largo del tiempo. Incluso, podría dejar de existir una ruta que una esos 2 puntos. El ruteo es uno de los aspectos centrales acerca de cómo funcionan las redes y comprender sus fundamentos permite tener una visión más profunda y sistémica sobre Internet.

TCP y paquetes

Gracias a lo visto anteriormente (ruteo), los y las estudiantes ya saben por dónde puede viajar la información, pero ¿cómo se organiza para hacerlo? ¿Qué inconvenientes debe sortear? Ahora abordaremos los conceptos de paquete y protocolo TCP, que nos permitirán responder estas preguntas.

A modo introductorio se comenzará por el siguiente problema:

En una época previa a las comunicaciones electrónicas, dos ejércitos de un mismo bando se preparan para atacar una ciudad desde dos puntos diferentes. Si ambos atacan a la vez, ganarán la batalla, pero si sólo uno de ellos lo hace, perderán. Para precisar los detalles del momento ideal para atacar se envían mutuamente mensajeros, con el riesgo de que puedan ser capturados y los mensajes nunca lleguen a destino. ¿Cómo pueden hacer para coordinar el ataque?

Lo que buscamos ilustrar es el siguiente inconveniente: Si uno de los generales envía un mensaje conteniendo la hora del ataque en el mensaje, no sabe si llega bien a destino y por ende no sabe si su colega también atacará (recordar que si no atacan los dos a la vez serán derrotados). Para evitarlo, el segundo general le deberá enviar una confirmación de recepción. El problema, ahora, será que el segundo general esté seguro de que su confirmación fue recibida, para lo que tendría que esperar otra confirmación, pero del primer general para él. Nos encontramos con una sucesión infinita de mensajes de confirmación de recepción que impedirá que se concrete el ataque.

La certeza absoluta de que ambos saben que el otro sabe, es imposible, pero a efectos prácticos es necesaria, al menos, una confirmación o acuse de recibo para el primer envío y poner un límite a la cantidad de "confirmaciones de la confirmación" que se intercambian, para garantizar el ataque.

Supongamos ahora, dos nuevas situaciones distintas:

1. ***Para anotarse en un torneo de fútbol, a Diego le piden que presente las fichas de cada jugador del equipo, apto físico y fotocopias de DNI, entre otros papeles. La ventanilla donde tiene que entregarlos cuenta con una pequeña ranura por la que no pasa la pila completa de documentación, sólo dos o tres páginas a la vez. Para poder cumplir con todos los requerimientos, Diego debe separar los papeles y pasarlos de a grupos más pequeños.***

2. ***La última evaluación de Historia para aprobar el trimestre consiste en un cuestionario grupal que abarca muchos temas vistos en clase. Para resolverlo, cada integrante del grupo elige las preguntas sobre los temas que lo hacen sentir más seguro y resuelven dividir de esta forma el trabajo. El día de la entrega se encuentran con el trabajo desarmado en partes más pequeñas que hay que organizar.***

En función a las 2 situaciones planteadas anteriormente, algunas preguntas que podrían surgir serían las siguientes:

- ¿Qué problemas se les ocurre que pueden presentarse en las dos situaciones planteadas?
- ¿Qué pasa si la información llega desordenada? ¿Podría ser un problema?
- ¿Y si se pierde parte de la información (las respuestas de la prueba o parte de la documentación)?
- ¿Cómo lo relacionarían con el problema de los dos generales?
- ¿Se les ocurre alguna solución?

Si analizamos cada situación con la finalidad de poder establecer relaciones con la forma de enviar información a través de Internet, es que surge el concepto de utilizar ***paquetes***. Un paquete es un fragmento de información que es transmitido por separado hasta que los envíos sucesivos de paquetes permitan reconstruir el mensaje original.

Cuando vimos el concepto de ruteo se explicó que la información puede tomar diferentes caminos para llegar a destino, y esto mismo ocurre con los paquetes, razón por la cual es posible que lleguen desordenados o se pierdan algunos en el camino. Para reforzar el problema de que los paquetes no lleguen en orden imaginemos tener varias palabras en hojas separadas y tuviéramos que armar dos o más oraciones con ellas. Ej: “Un chico muy mono” y “Un mono muy chico” o “Dulce, traeme un mate amargo” y “Amargo, traeme un mate dulce”.

Además, qué pasa si se omiten palabras (o se pierden paquetes): “Juan le dió de comer sobras de carne de la cena al perro” no significa lo mismo que “Juan le dió de comer carne de perro” o “Por favor, no queremos que tome la prueba el jueves” y “Por favor, queremos que tome la prueba el jueves”.

El objetivo de los ejemplos dados es pensar en los inconvenientes que puede ocasionar que los mensajes no se reciban ordenados y/o completos. Aquí es donde algunas alternativas de solución nos llevan a presentar el **protocolo TCP**, que ***engloba el conjunto de reglas encargado de regular los intercambios de mensajes y evitar estos problemas en las redes***.

El protocolo **TCP** (**T**ransmission **C**ontrol **P**rotocol o Protocolo de Control de Transmisión) es uno de los más utilizados de Internet y resuelve los dos problemas presentados:

- Los paquetes que componen un mensaje son enviados con un número asociado, de manera que a pesar de llegar desordenados puedan ser reconstruidos por el receptor.

- Por otro lado, al momento de recibir un paquete se envía un acuse de recibo (ACK del inglés acknowledgement), lo que garantiza que si un paquete no fue recibido el emisor no tendrá la confirmación y lo podrá volver a enviar hasta que se confirme su recepción.

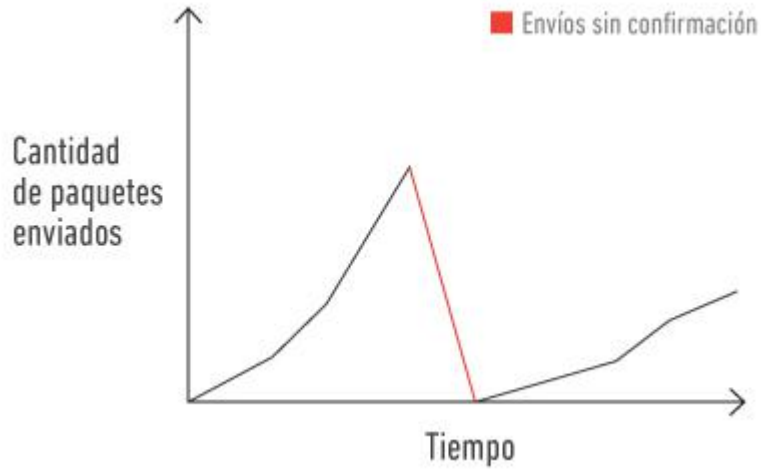
En función de lo explicado anteriormente:

- ¿Qué creen que ocurre cuando se pierden paquetes?
- ¿Cómo lo notan al usar la computadora?
- Internet anda lenta… ¿Por qué puede ser?
- Cuando ven videos o películas online, ¿cómo creen que se resuelve la pérdida de paquetes?

Cuando un dispositivo envía información a otro punto de la red puede detectar que para algún paquete tarda demasiado la confirmación del receptor respecto a otros enviados. En ese caso resolverá volver a enviar dicho paquete hasta tener garantías de recepción del mensaje completo.

Como los caminos que toman los paquetes a lo largo de la red son compartidos con otros envíos de información, puede ocurrir que la red se encuentre congestionada o también puede pasar que el volumen de datos que el receptor puede recibir es menor tan rápido como se los envían. El emisor será el encargado no sólo de reenviar sino de regular la relación entre el tiempo y la cantidad de paquetes que envía, de esta manera podrá detectar el volumen de información que puede enviar sin inconvenientes.

Uno de los mecanismos de regulación funciona enviando una pequeña cantidad de paquetes, si recibe confirmación de todos, incrementará exponencialmente la magnitud del envío hasta que en determinado punto detecte que ya no recibe confirmaciones. En ese momento comenzará a enviar nuevamente una cantidad pequeña de datos que incrementará más lentamente para evitar la pérdida de un volumen grande de paquetes por congestión.



Podemos mencionar que, para otro tipo de transmisiones, las que requieren mantener fluidez en la comunicación como para ver películas y reproducir música, se utiliza otro protocolo muy simple de transmisión denominado **UDP** (**U**ser **D**atagram **P**rotocol, Protocolo de datagrama de usuario) que no proporciona detección de errores debido a que no chequea la recepción de todos los paquetes, ya que la velocidad es más importante que el envío completo de todos los datos.

Resumiendo, las ideas que componen TCP constituyen una gran obra de ingeniería, que soluciona un problema muy complejo: lograr que una red en donde los paquetes pueden perderse y llegar desordenados funcione como si fuera "un tubo", donde la información llega en orden y de manera confiable de un extremo a otro.

Conclusión

TCP es el protocolo más utilizado para regular las comunicaciones en redes. La utilización de paquetes con una identificación numérica y un mensaje de confirmación de recepción y de los conflictos abordados, como la congestión y la pérdida de paquetes, brinda una perspectiva más amplia respecto a qué es lo que puede estar ocurriendo cuando las/los estudiantes se encuentran con conexiones lentas o con interrupciones.

Modelo cliente-servidor y HTTP

Muchas de las formas en que los usuarios utilizan Internet hoy día se basan en esta dinámica en donde una máquina presta un servicio particular: intermediar entre 2 usuarios que quieren comunicarse, navegar por la web, poder jugar un juego en red, etc.

A continuación, abordaremos temas como qué es la Web y cuáles son las características principales del protocolo detrás de ella: HTTP (**H**yper**T**ext **T**ransfer **P**rotocol)**.**

Algunos de los aspectos a trabajar: las páginas se escriben en un lenguaje particular llamado HTML (**H**yper**T**ext **M**arkup **L**anguage), la relación entre sesión y cookies, y el famoso error 404 de HTTP.

Por último, se verá cómo se relacionan todos los protocolos vistos hasta ahora al querer, por ejemplo, acceder a un sitio web.

Actividad 7

En esta actividad trabajaremos con un escenario conocido para las/los estudiantes con el objetivo de problematizar el modelo cliente-servidor, la cual dará lugar para hablar también de la World Wide Web.

En actividades anteriores, vimos que la comunicación entre Braian y Daniela a través de una aplicación de mensajería está mediada por un servidor que recibe y reenvía los mensajes que se envían entre ellos.

En grupos de 5/6 alumnos/as realicen uno o varios diagramas y escriban una explicación de cuáles creen que son los pasos que se siguen para que Daniela vea 1 tilde (salió el mensaje), 2 tildes (mensaje recibido) o 2 tildes en azul (mensaje leído) cuando le envía un mensaje a Braian (al estilo WhatsApp).

En la Imagen 20 se muestra un posible diagrama en donde se detallan los 3 pasos que se deben realizar desde que el mensaje sale del celular de Daniela hasta que ella recibe las 2 tildes azules.

La descripción de la secuencia de pasos es:

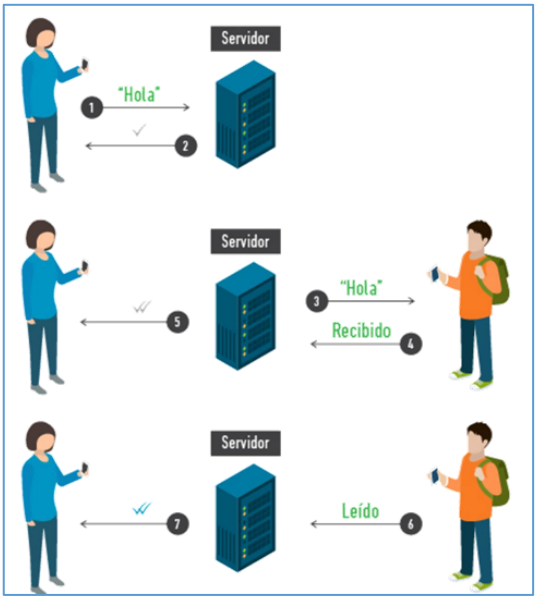


Imagen 20. Pasos que se siguen para marcar un mensaje como enviado, recibido y leído.

1. Daniela envía el mensaje al servidor de la aplicación para que éste se lo envíe a Braian.

2. El servidor le confirma a Daniela que tiene el mensaje en su poder (1 tilde).

3. El servidor le envía el mensaje a Braian.

4. La aplicación de mensajería corriendo en el celular de Braian notifica al servidor que el mensaje fue recibido.

5. El servidor le avisa a Daniela que Braian ya recibió el mensaje (2 tildes).

6. Braian lee el mensaje de Daniela y la aplicación en el celular de Braian le avisa al servidor.

7. El servidor le avisa a Daniela que Braian ya leyó el mensaje (2 tildes azules).

En los diagramas de la Imagen 20 se simplifica el hecho de que los mensajes pasan por distintos routers ya que los celulares no están conectados directamente con el servidor. Esta observación conviene hacerla de manera explícita para establecer relaciones con lo visto en las clases de ruteo y de infraestructura física.

- ¿Qué pasaría si Braian estuviera sin Internet o tuviera el celular apagado?
- ¿Y si Daniela se quedara sin Internet antes de recibir las 2 tildes azules?
- ¿Y si el servidor se apagara en algún momento del proceso?

Desde que el mensaje sale del celular de Daniela y llega al servidor, éste se encarga de concretar el resto del proceso, es decir, que Daniela reciba todas las tildes y que Braian reciba el mensaje. Si alguno de los 2 se quedara sin Internet o no tuviera prendido el celular, el servidor podría tomar dos decisiones: descartar el mensaje porque no lo pudo entregar o tenerlo guardado e intentar reenviarlo más tarde. En general, lo que sucede es la segunda opción. Más aún, los servidores suelen guardar todo el historial de mensajes, no solamente aquellos que aún no ha podido entregar.

A este modelo, en donde una computadora tiene instalada una aplicación que se comunica con un servidor que brinda un servicio de Internet, se lo conoce como ***cliente-servidor***. En este modelo, la computadora cliente lo único que hace es comunicarse con el servidor que es donde corre el servicio.

Por ejemplo, cuando entramos a una red social a través de una aplicación del celular, nuestro celular no tiene almacenada toda la red social sino que se comunica con un servidor de dicha red social a través de la aplicación cliente. El servidor recibe cada uno de los pedidos de los clientes y los va respondiendo. Cada vez que entramos a ver el perfil de alguien, el servidor nos envía el contenido. Y cuando queremos subir un post, la aplicación cliente le dice al servidor “incluí este nuevo post en el contenido que tenés guardado sobre mí”.

Otros ejemplos en donde se usa el modelo cliente-servidor es en los juegos en red y al navegar por la web.

Actividad 8

La web, abreviación de **W**orld **W**ide **W**eb (WWW), se basa en un modelo cliente-servidor en donde los clientes son los navegadores web (Mozilla Firefox, Google Chrome, Safari, Internet Explorer, Opera, etc.) y los servidores son máquinas en donde se guardan los sitios web y que se encargan de enviar dicho contenido a quien lo solicite. Pero…

- ¿Qué es la web?
- ¿Es un sinónimo de Internet? ¿Son cosas distintas?
- Si son cosas distintas, ¿en qué se diferencian?

Responder las 3 preguntas anteriores en grupos de 5/6 alumnos/as. Utilizar sus propias palabras.

Debemos separar de manera explícita la noción de ***Internet*** de la de ***WWW.*** Internet es una red de redes mientras que WWW se "monta" sobre Internet.

Dicho con otras palabras, WWW se refiere únicamente a los recursos disponibles en servidores que saben comunicarse mediante HTTP.

Cada sitio web se almacena en una máquina a la que se la denomina servidor web. Cada vez que alguien quiere acceder al contenido de un sitio web se lo tiene que pedir al servidor web en donde está alojado el sitio. El servidor web responde el pedido enviando el texto, las imágenes, videos, y todo aquel contenido del sitio solicitado. Esta comunicación entre navegador web y servidor web se realiza mediante HTTP (Protocolo de Transferencia de Hipertexto).

- ¿Alguien escuchó la palabra hipertexto alguna vez?
- ¿Y HTML? ¿Qué significa esta sigla?
- ¿Qué tendrán que ver HTTP y HTML?

Todos los sitios web que componen "la web" se escriben en un lenguaje en particular llamado HTML (Lenguaje de Marcado para Hipertextos), el cual permite estructurar y darle formato a todo el contenido de un sitio. En la Imagen 21 se muestra un ejemplo sencillo de un código HTML y cómo se vería el mismo en un navegador web.

```
<html>
    <head>
        <title>El gurú de la Internet</title>
    </head>

    <body>
        <h1>Introducción a HTML</h1>
        <p>El HTML es el lenguaje en que se escriben los sitios web.</p>
        <p>Permite incluir <b>texto</b>, <i>imágenes</i>,
           <mark>videos</mark>, dar formato, etc.</p>
        <img src="gato_y_perro.png" alt="Gato y perro durmiendo.'>
    </body>
</html>
```

Imagen 21. Ejemplo de código HTML y cómo se ve en un navegador web.

Cuando un usuario a través de un navegador web quiere acceder, por ejemplo, al sitio de la Imagen 21, le envía el mensaje “GET www.ejemplo.com.ar HTTP/1.1” al servidor web que tiene guardado el sitio. GET es un mensaje especial del protocolo HTTP con el que se le indica mediante una URL (**U**niform **R**esource **L**ocator - Localizador Uniforme de Recursos-) a qué recurso se quiere acceder. Lo que figura luego de la “/” (1.1) corresponde a la versión del HTTP (esta puede ser 1.0 o bien como en el ejemplo, 1.1)

A continuación, el servidor web enviará el código HTML del sitio mediante HTTP, visualizándose en el navegador web la Imagen 22.

Imagen 22. Recurso faltante al visualizar el sitio web de ejemplo.

Como puede apreciarse, falta la tierna imagen del perro y el gato. Esto se debe a que cada recurso del sitio debe ser pedido (y enviado) uno a uno. Si el servidor no tiene el recurso guardado o justo se corta Internet, el navegador visualizará el sitio con íconos que indican que ese recurso no se puede mostrar correctamente. Si todo funciona bien, el navegador realizará un nuevo pedido mediante HTTP para obtener la imagen referenciada y así poder mostrar la visualización completa (Imagen 21).

En general, cada sitio está compuesto por muchos recursos. Se puede acceder al modo para desarrolladores de los navegadores web y ver la línea de tiempo de todos los recursos que se envían cada vez que se accede a un sitio, como se muestra en la Imagen 23.

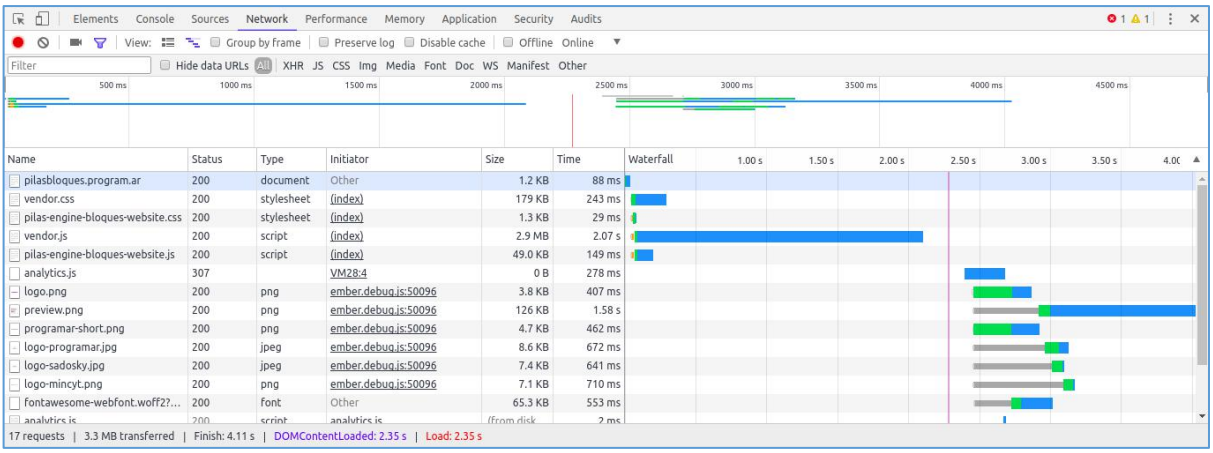


Imagen 23. Línea temporal al cargar un sitio web en el modo desarrollador de Google Chrome.

Si el recurso que no se puede encontrar es el código HTML de la página, es decir, si la página pedida no existe en el servidor, entonces el servidor responde con un código de error bien particular del protocolo HTTP: el famoso error 404 de “página no encontrada” (imagen 24). Esto puede ocurrir porque la URL que se ingresó tiene un error de tipeo o porque efectivamente esa página ya no existe más en el servidor.

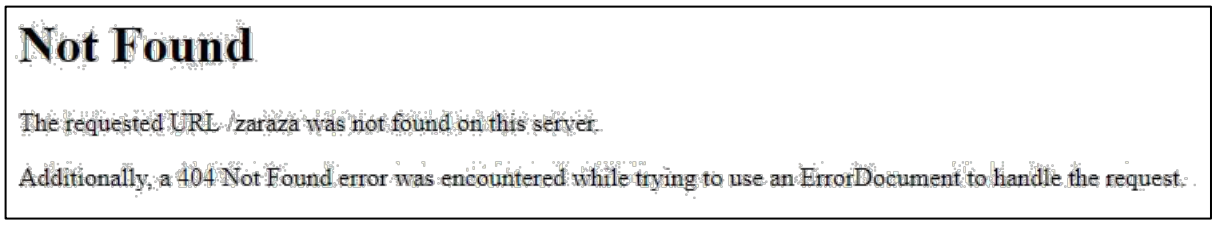


Imagen 24. Error 404 de HTTP: "recurso no encontrado".

Un usuario también podría querer completar partes de la página web a la que accedió como, por ejemplo, ingresando usuario y contraseña para loguearse en el sitio. En este caso, el navegador web envía un mensaje POST al servidor con la información que el usuario haya ingresado. Una vez hecho esto el usuario queda logueado en dicho sitio.

El comportamiento de "quedarse logueado" o de mantener una sesión abierta, incluso cuando se sale del navegador o se apaga la computadora, excede HTTP ya que solamente con este protocolo no alcanza para lograrlo. Para ello, se utiliza una estrategia que se volvió muy conocido en el último tiempo: ***las cookies***.

Una cookie es información que un sitio web guarda en la computadora del usuario para que la próxima vez que ingrese pueda "mejorar su experiencia" en el sitio, donde mejorar puede significar mantenerlo logueado, poder hacerle recomendaciones personalizadas en función de sus búsquedas pasadas, mostrarle determinada publicidad, etc. En la Imagen 25 se muestra el típico cartel que aparece al entrar un sitio web que avisa a sus usuarios que hace uso de las cookies.

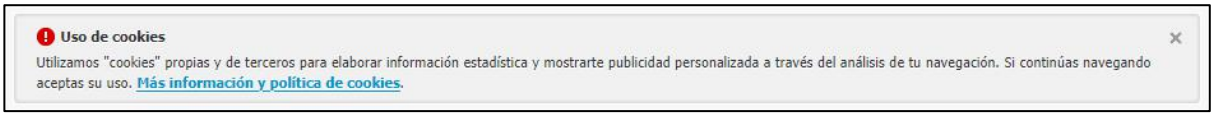


Imagen 25. Aviso de uso de cookies al ingresar a un sitio web.

Si se desea que un sitio web no almacene información personal en la computadora mediante el uso de cookies, se puede navegar en modo incógnito o privado. En este modo el navegador web no permite que ningún sitio almacene en la computadora información sobre la navegación realizada. En la imagen 26 se explica cómo hacerlo desde el navegador Chrome.

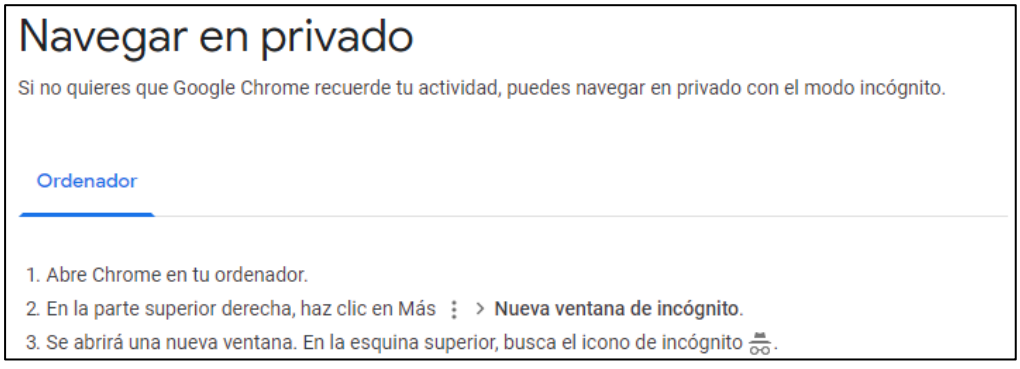


Imagen 26. Como activar en Crome la navegación en modo incógnito.

Hasta ahora vimos distintas facetas que hacen a la estructura y al funcionamiento de Internet: las direcciones IP, cómo los datos viajan desde una computadora hasta otra atravesando varias computadoras en el camino, cómo se resuelven los nombres de dominio mediante DNS, cómo es la infraestructura física a nivel global, cómo hacer para que los datos (casi) siempre lleguen a destino gracias a TCP y cómo HTTP permite navegar por la web.

Si bien cada uno de los temas vistos resuelve un problema en particular, todos están relacionados entre sí, formando distintas capas de abstracción. Cada capa resuelve un problema distinto pero todas juntas colaboran para que Internet funcione como la conocemos. Por ejemplo, al ingresar una URL en el navegador se debe usar:

- DNS para obtener la dirección IP del servidor que tiene guardada dicha página.
- HTTP para pedir los recursos de esa página.
- TCP para asegurar que toda la información llegue a destino (confiabilidad).
- IP para indicar la dirección de origen y de llegada en cada salto de la ruta.
- Ethernet o Wi-Fi para que las máquinas puedan transmitir la información a nivel bit.

En la Imagen 27 se muestran las distintas capas o niveles que componen Internet. Cuanto más arriba, mayor nivel de abstracción.

Capa de aplicación	HTTP, DNS, DHCP
Capa de transporte	TCP, UDP
Capa de red	IP
Capa física	Ethernet, Wireless

Imagen 27. Capas de abstracción y ejemplos de protocolos de Internet.

Por lo tanto, cuando un usuario quiere enviar datos a otra máquina, esos datos se van encapsulando en una tira de 0s y 1s que incluyen la información que requiere cada uno de los protocolos, que luego se traduce en impulsos eléctricos, ondas de radio o pulsos de luz, para atravesar los distintos medios de comunicación física. Si se observara de cerca cada paquete de información que se envía por Internet, se vería una estructura similar a la de la Imagen 28.

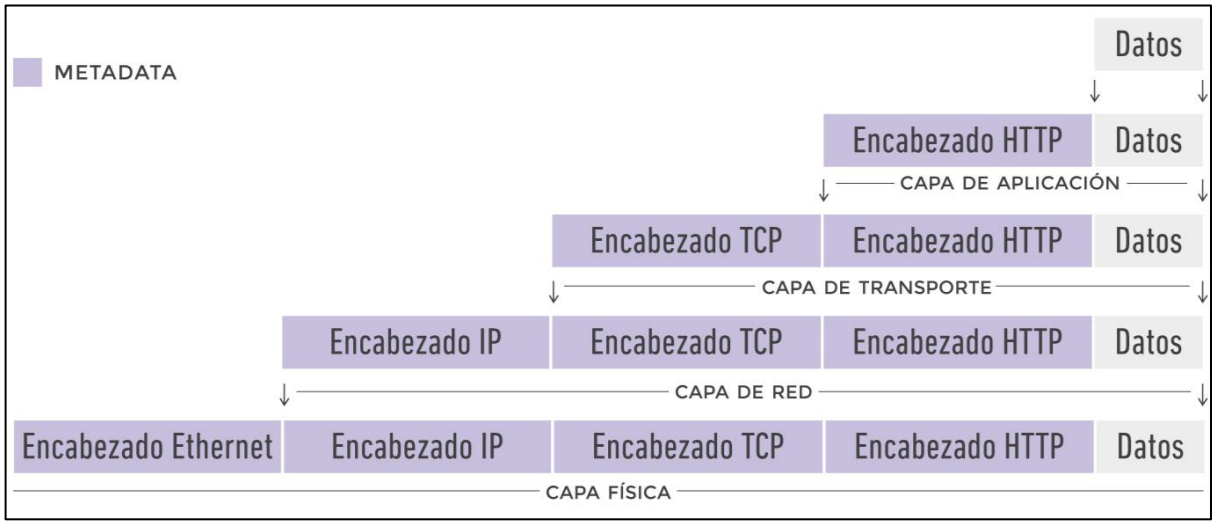


Imagen 28. Encapsulamiento de los datos a enviarse a través de Internet.

Conclusión

El modelo cliente-servidor y el protocolo HTTP constituyen dos de los pilares de la Internet actual.

Conocer sus fundamentos permite comprender mejor las interacciones que realizamos como usuarios al navegar por la web, utilizar una aplicación de mensajería, jugar un juego en red, etc.

Además, el haber podido descomponer un paquete de datos en cada una de las capas, permite recuperar e interrelacionar cada uno de los protocolos vistos en la materia.

Criptografía

La criptografía es la disciplina encargada de brindar seguridad a los sistemas informáticos actuales. A su vez, está basada en ideas altamente ingeniosas, patrimonio de la humanidad.

Comenzaremos hablando sobre un algoritmo clásico conocido como "Cifrado César". Para ello se partirá de un mensaje en clave y se presentará el desafío de tratar de develar el misterioso enunciado. A su vez, se reflexionará acerca de las limitaciones que posee este algoritmo o "sobre cómo hackear el código César".

Luego veremos escenarios reales en donde los algoritmos de criptografía más tradicionales no sean posibles de aplicar. Para resolver este problema se trabajará en la gran idea sobre la que descansa la seguridad informática actual: la criptografía asimétrica.

Por último, se dejará registro de problemas cotidianos y soluciones posibles como certificados, firma digital, HTTPS, WPA2 y criptografía híbrida, adjuntando una breve explicación y links con más información al respecto.

Actividad 9

Usando el escenario clásico del juego ahorcado y partiendo de 12 espacios para completar las letras traten de adivinar la palabra. Como se muestra en la Imagen 29, la palabra a adivinar es “Ujahlgyjsxas”.

Con el objetivo de que puedan terminar de completar la palabra, en grupos de 5/6 alumnos deberán realizarlo en 7 intentos como máximo (que es en la cantidad de chances en el juego original).

Imagen 29. “Ujahlgyjsxas” es la palabra que las/os estudiantes deben “adivinar”.

Aquí nos podrían surgir las siguientes preguntas:

- Alguna/o la conoce
- Si está en español o en otro idioma
- Qué creen que significa

Qué pasaría si tomáramos una hoja y desplazáramos cada letra de la palabra 18 posiciones a la izquierda. Por ejemplo, la letra “s” si se la desplaza 1 posición a la izquierda se transforma en “r”, si se la desplaza 2 posiciones en “q” y se la desplaza 18 en “a”. Si al ir haciendo los desplazamientos el alfabeto se acabara, se vuelve a comenzar desde la “z”. Por ejemplo, la letra “e” desplazada 18 posiciones a la izquierda resulta ser la “m”. ***Se considerará el alfabeto sin la “ñ”, como los caracteres de la codificación ASCII.***

- ¿Qué palabra resultó???
- ¿Alguna/o conoce esta palabra? ¿Qué significa? Pista: es una palabra del español.
- ¿Cómo llamarían a lo que acabamos de hacer?
- ¿Tiene alguna utilidad real este juego?

Lo que realizaron fue descifrar un mensaje que estaba cifrado o encriptado, es decir, que estaba escrito de manera tal que sólo pudieran entenderlo quienes conocieran la regla para descifrarlo.

Desde que el ser humano se comenzó a comunicar de manera escrita, se empezaron a presentar situaciones en donde un mensaje no podía ser enviado sin suponer que pudiera ser capturado por un enemigo. Por ejemplo, supongamos que el César, en la antigua Roma, tenía que enviarle el mensaje "atacar por los flanco Sur y Norte antes del amanecer" a uno de sus generales en batalla. Para ello, enviaba el mensaje con un emisario que se lo haría llegar a su general. Sin embargo, el emisario podría ser interceptado en el camino por el ejército enemigo y, si el mensaje no estuviera cifrado, podrían anticiparse a la estrategia militar del César.

Para que el César y el general se puedan enviar mensajes en clave tienen que haberse puesto de acuerdo en persona previamente sobre cuál va a ser el método para cifrar/descifrar el mensaje (rotar los caracteres del abecedario hacia la izquierda) y cuál es la clave del mensaje (cuántas posiciones moverse: 18 en el ejemplo). De hecho, esta anécdota es real ya que los romanos cifraban sus mensajes. La estrategia de rotar el alfabeto es conocida como "cifrado César".

Nota	Para mostrar el proceso de descifrado pueden utilizar el programa CrypTool disponible para Linux y Windows. En un documento se copia el texto a descifrar, se va al menú *Cifrar/Descifrar → Simétrico (clásico) → César / Rot-13…*, se eligen los parámetros que se muestran en la Imagen 30 y se aprieta el botón "Descifrar". Link para descargar CrypTool: https://www.cryptool.org/en/ct1-downloads

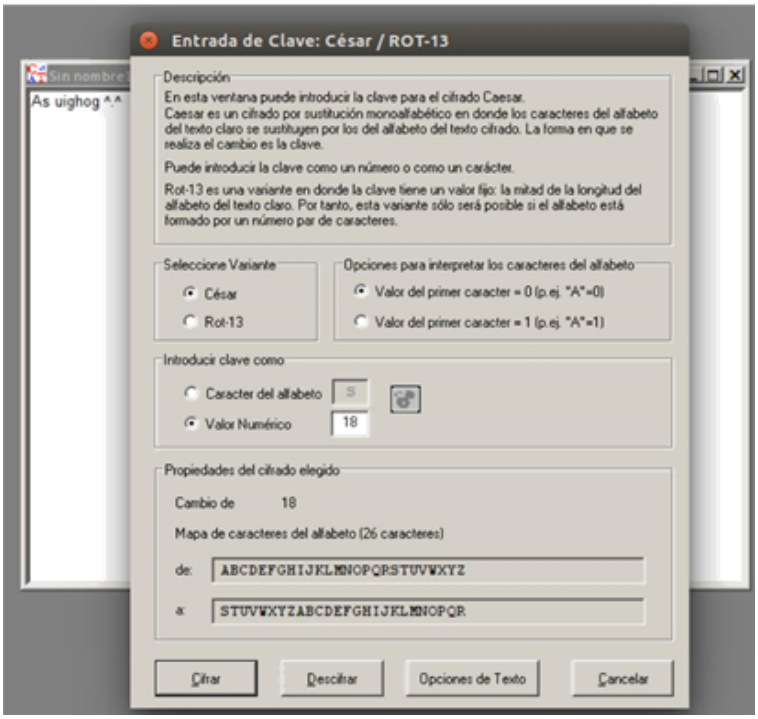


Imagen 30. Cómo cifrar/descifrar un mensaje usando la herramienta CrypTool.

- ¿Le encuentran algún problema a este método?
- Si interceptaran un mensaje sin conocer la clave, ¿cómo harían para descifrarlo?
- ¿Cuánto tiempo creen que le podría tomar a una computadora descifrarlo?
- ¿Sería lo mismo si la clave fuera 14 en vez de 18?

Este método de cifrado es muy fácil de quebrar ya que se podrían probar las 26 rotaciones posibles hasta dar con el mensaje original. Por ejemplo, en el caso del mensaje "Ujahlgyjsxas" se prueba con:

1 rotación	→	"Tizgkfxirwzr"
2 rotaciones	→	"Shyfjewhqvyq"
3 rotaciones	→	"Rgxeidvgpuxp"
…		
18 rotaciones	→	"Criptografia"

Para resolver este problema se diseñaron otros algoritmos de cifrado que toman muchísimo tiempo de descifrar, incluso para una computadora. Para todos ellos el concepto es el mismo: hay que conocer una única clave o "llave" que se utiliza tanto para cifrar como para descifrar el mensaje. Ambos, emisor y receptor deben conocer cuál es esa llave si se quieren comunicar de manera cifrada y que nadie más pueda comprender sus mensajes.

A este tipo de algoritmos de cifrado se los conoce bajo el nombre de "**criptografía simétrica**" ya que la misma clave que se usa para encriptar se utiliza para desencriptar; son procesos simétricos.

¿Sabías qué?

Durante la Segunda Guerra Mundial, los alemanes utilizaban un método de cifrado simétrico que era realizado por una máquina apodada "Enigma". El británico, y pionero de la computación, Alan Turing, junto con un equipo de criptógrafos lograron encontrar, luego de varios meses de trabajo, la forma de descifrar los mensajes capturados de las comunicaciones alemanas. Sobre este tema existen 2 películas muy interesantes que se pueden ver: "The Imitation Game" ("El código Enigma" en español) y "Codebreaker".

Actividad 10

Volviendo 2000 años en la historia, suponer ahora que una espía, apodada Teresa, necesita recibir un mensaje encriptado pero la clave del sistema de cifrado simétrico que usaban con su agencia de inteligencia fue descubierto y Teresa está a miles de kilómetros en una operación encubierta por lo que no puede volver a su país de origen para que ella y la agencia se pongan de acuerdo en una nueva clave de cifrado.

- ¿Qué puede hacer Teresa?
- ¿Se les ocurren otras situaciones en donde 2 personas se quieran comunicar de manera privada pero no puedan ponerse de acuerdo en persona sobre la clave a utilizar?
- ¿Les parece que es un problema que se pueda dar en Internet? ¿Por qué?
- ¿Sabían que todo el tráfico que están recibiendo y enviando sus celulares y computadoras puede ser leído usando softwares muy sencillos? ¿Estarán "seguros" sus datos?

Por ejemplo, cuando una persona quiere loguearse en Facebook, Instagram, Twitter o cualquier otra red social o sitio web, escribe su usuario y su contraseña y se los envía a la empresa que brinda el servicio para que verifique sin son correctos. Como vimos en clases anteriores, estos datos pasan por un montón de máquinas intermedias que los van reenviando hasta llegar al servidor de la red social a la que la persona se quiere conectar. ¿Alguien que tenga acceso a alguna de esas máquinas podría robar los datos?

¿Alguna vez se pusieron de acuerdo con Facebook o Instagram sobre una clave común para cifrar los datos?

Sus celulares y sus computadoras al estar conectados vía Wi-Fi o datos, emiten ondas de radio que cualquier dispositivo cercano podría leer. Por ejemplo, al conectarse a una nueva red Wi-Fi privada hay que ingresar una contraseña. ¿Alguien que quiere "robar" Wi-Fi podría capturar todo el tráfico que va hacia el router a la espera de que otra persona ingrese la clave para así poder conectarse a dicha red?

En la actualidad, la seguridad ya no es solamente una cuestión de espías incomunicados sino que establecer comunicaciones en donde los datos puedan viajar de manera segura entre dos partes que no se conocen es un requisito de la mayor parte de las acciones que se realizan en Internet. Y el punto clave es que el canal por el cual viaja la información es intrínsecamente inseguro: cualquiera que quisiera podría leer las señales de radio o "pinchar" el cable por donde viajar los datos. ¿Cómo hacer para encriptar la información si no se puede enviar la clave por ese canal y tampoco las partes se pueden reunir en persona para acordar una clave común?

Los algoritmos de cifrado simétrico tienen el problema de que las partes deben ponerse de acuerdo en una clave compartida para cifrar y descifrar los mensajes. Como ya se mencionó, en la mayoría de los casos de la vida en red no es posible hacer eso mediante un canal seguro. La solución que se inventó hace apenas 5 décadas, allá por los años `70, fue la de usar una ***clave para cifrar*** y ***otra distinta para descifrar***. A la ***clave de cifrado*** se la conoce como ***clave pública*** y a ***la clave de descifrado*** se la conoce como ***clave privada***.

Volviendo al problema de Teresa (la espía), la agencia de inteligencia genera un par de claves compuesto por la clave pública X1 y la privada X2. Luego distribuye por todos los medios la clave X1 que sus agentes utilizan para cifrar los mensajes que desean enviar a la oficina central de la agencia.

Esta es la clave pública de la agencia y cualquier persona, sea agente o no, incluso agentes del recontraespionaje, la puede conocer y usar. Teresa, entonces, cifra el mensaje que quiere enviarle a la agencia con la clave pública X1 y lo envía a través de Internet. ¿Quiénes pueden descifrarlo? Sólo la agencia, que es la única que posee la clave privada X2 que sirve para descifrar los mensajes. Cualquier otra persona que acceda al mensaje cifrado de Teresa no podrá descifrarlo ya que no posee la clave X2, la cual sólo está en poder de la agencia, quien la guarda con extremo cuidado. En la Imagen 31 se ilustra este proceso.

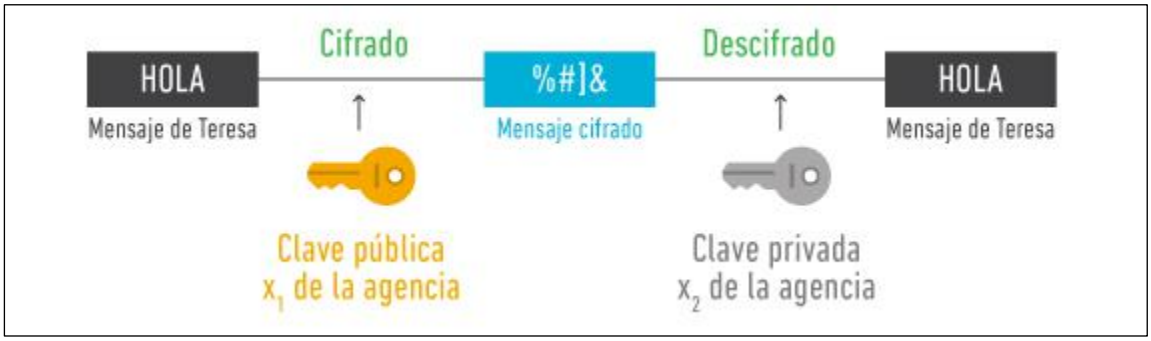


Imagen 31. Proceso de cifrado y descifrado mediante clave pública y clave privada.

Por otro lado, la agencia, para enviarle mensajes encriptados a Teresa hace algo similar: conoce la clave pública Y1 de Teresa, la cual utiliza para cifrar los mensajes y enviárselos por Internet. Teresa los recibe y utiliza su clave privada Y2 para descifrarlos.

Esta idea de tener una ***clave o llave para cifrar y una distinta para descifrar*** se la conoce como ***criptografía asimétrica***, ya que el proceso de encripción y desencripción requiere claves diferentes, y es el mecanismo que se usa en Internet para establecer comunicaciones seguras a través de canales inseguros.

Ejemplo: Digamos que tengo que enviar una información importante pero no puedo confiar en el mensajero. Por lo tanto, escribo mi mensaje en un papel, lo meto en una caja de metal, le pongo un candado y lo envío. La caja llega a su destino sin problema, pero el destinatario no puede leerla, pues no puede abrir el candado. Si le envío la llave, aunque sea por otro medio -otro mensajero-, puede verse que hay un nivel de riesgo, al comprometer la seguridad de la llave, confiándola a extraños. Así funciona el ciframiento convencional.

Cambiemos ahora un poco la situación. Digamos ahora que el destinatario me envía previamente un candado, abierto. Es “su” candado, yo no puedo abrirlo si se cierra, pues la llave solamente la tiene él. La llave permanecerá segura en su poder. Recibo el candado, escribo mi mensaje, lo meto en la caja y cierro la caja con el candado que recibí. A partir de ese momento, ni yo mismo, que escribí el mensaje, puedo ya verlo. Está protegido por el candado. Envío la caja y el destinatario la abre con su llave. Así funciona la llave pública y privada. La llave pública es el candado y su pareja es la llave de metal (llave privada) que lo abre. Por supuesto, esta pareja debe ser fabricada una para la otra.

La versión criptográfica es un par de secuencias de caracteres, que usadas por un programa adecuado pueden cifrar y descifrar un texto. La llave pública solamente puede cifrar. La llave privada puede descifrar o hacer las dos cosas, aunque esto último no es tan importante. Yo recibo la llave pública de mi destinatario y con ella cifro la información que le enviaré. Una vez cifrada, yo mismo no puedo ver la información. Envío esta información, en un correo, por ejemplo, el destinatario la recibe y la descifra con su llave privada.

No hay peligro en publicar las llaves públicas porque son precisamente para eso. Y están diseñadas de manera que es muy difícil -casi imposible con la tecnología actual- deducir una llave privada de una pública. Y claro, ambas llaves deben ser generadas previamente, como un par correspondiente, igual que el candado y su llave.

A pesar de que cualquier persona puede capturar el mensaje cifrado y tratar descifrarlo, es prácticamente imposible lograrlo probando todas las posibles claves privadas. Sin entrar en detalles se usa la matemática detrás de esta clase de algoritmos dado que su fortaleza reside en que la encriptación usa productos de números primos muy grandes y hallar la "formula" de desencriptación es computacionalmente muy costoso a nivel temporal en el sentido que puede tomar milenios encontrar la clave privada incluso utilizando las supercomputadoras más potentes del mundo.

La criptografía y, más en general, la seguridad de la información es un tema muy amplio que tiene (casi) infinitas aristas y presenta desafíos sumamente interesantes. A continuación se listan algunos problemas de la vida real que se pueden resolver mediante el uso de la criptografía:

Problema	Solución
Cuando quiero saber la clave pública de alguien X, un atacante me envía la suya diciéndome que es X. Por ende, cifro mis datos con la clave del atacante quien puede decodificar con su clave privada mi información.	Certificados. Una estructura jerárquica de entidades confiables que validan identidades. Más en: https://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica
Algunas páginas web requieren que la comunicación sea altamente segura mientras que para otras no es necesario. ¿Cómo distinguir aquellas que cifran la información de aquellas que no?	HTTPS. Los datos que se envían mediante el protocolo HTTP se pueden cifrar utilizando criptografía de clave pública para que toda la información viaje de manera privada. En el navegador web, el candadito al lado de la URL indica que esa página usa HTTPS. Más en: https://es.wikipedia.org/wiki/Protocolo_seguro_de_transferencia_de_hipertexto
Enviar un documento digital garantizando que se pueda verificar si el mensaje fue adulterado y que quien lo envió no pueda decir que él no envió dicho documento. Por ejemplo, Lucas podría usar la clave pública de Teresa para enviar un mensaje a la agencia haciéndose pasar por ella.	Firma digital. Al texto original se le aplica una función matemática que devuelve un número asociado a ese texto (hash). Luego, se cifra el hash con la clave privada del emisor. El receptor descifra el hash con la clave pública del emisor y vuelve a calcular el hash del texto. Si el hash calculado coincide con el hash descifrado, entonces el documento no fue adulterado. Más en: https://www.descom.es/blog/correo-electronico/firma-digital/como-funciona-una-firma-digital.html
Para garantizar que la configuración de mi red es segura, ¿alcanza con que el router Wi-Fi esté configurado en WEP, WPA o WPA2? ¿Es todo lo mismo?	Lo más seguro es configurar el router en WPA2 y jamás usar WEP ya que este protocolo es muy sencillo de hackear. Más en: https://www.netspotapp.com/es/wifi-encryption-and-security.html
Cifrar los datos usando la metodología de clave pública es sumamente lento en comparación al cifrado utilizando criptografía simétrica.	Criptografía híbrida. Se utiliza criptografía asimétrica para compartir la clave de un algoritmo simétrico. Luego, la comunicación se cifra utilizando el algoritmo simétrico. Más en: https://es.wikipedia.org/wiki/Criptograf%C3%ADa_h%C3%ADbrida

Conclusión

La seguridad de la información resulta indispensable hoy día para un sinfín de tareas cotidianas. Desde loguearse en una red social hasta realizar una transacción bancaria, pasando por enviar un mensaje personal mediante una app de mensajería. Conocer cuáles son las bases de la criptografía actual resulta crucial para poder entender un mundo complejo en donde los mensajes cifrados ya no son sólo cuestión de espías.

La nube

Trabajaremos sobre la información que se comparte a través de aplicaciones y redes sociales en la denominada Nube. Se buscará dimensionar el volumen de la información compartida para entender los requerimientos de infraestructura para almacenarla y dónde se encuentra el negocio de brindar este tipo de servicios de manera gratuita. Para ello se analizarán los permisos que se otorgan a las empresas detrás de toda esa infraestructura y se reflexionará sobre la pérdida de poder de los propietarios originales al momento de compartir información.

Actividad 11

Formar grupos de 5 o 6 alumnos/as. En función a los fragmentos recibidos de términos y condiciones de diferentes aplicaciones y redes sociales, deberán resolver:

- ¿A quién creen que corresponden esos permisos?
- Analizar las consecuencias de aceptarlos y decidir si están dispuestos a acatar esas condiciones respecto a su información personal.

El objetivo será que puedan tomar dimensión de algunas de las implicancias que tiene el uso de redes sociales y el poder que concentran sus propietarios.

Actividad 12

Luego de identificar que las redes sociales, aplicaciones y sitios recopilan mucha información personal, se propiciará un debate con preguntas disparadoras como las siguientes:

- ¿Quiénes tienen acceso a nuestras fotografías, mensajes, videos, publicaciones, etc.?
- ¿Saben los nombres de las personas detrás de las empresas que recopilan toda esa información personal?
- ¿En qué países se encuentran? ¿Cuánto las afectará la legislación local? ¿Las regularán leyes diferentes a las que rigen en nuestro país? ¿Sabemos las consecuencias de nuestro accionar y nuestros derechos en ese marco legal al momento de usar los servicios que nos proveen?
- ¿Cuánta información recopilarán estas empresas?
- ¿Las publicaciones se almacenan en nuestros dispositivos físicos? Si las subimos a alguna aplicación o sitio y después la borramos de nuestro dispositivo, ¿dónde están almacenadas realmente?

De las respuestas a las preguntas anteriores, surge el concepto de ***Nube*** para poder problematizar respecto a que además de ser un espacio virtual, requiere de algún medio físico, ubicado en algún lugar y mantenido por alguien para poder funcionar. Este espacio físico crece minuto a minuto y de manera exponencial (realicen una pequeña estimación sobre cuánta información subieron en los últimos días a la red, y cómo con el correr del tiempo cada vez se comparten en las redes sociales y aplicaciones formatos de información más “pesados” y especialmente mayor cantidad en menor cantidad de tiempo)

Luego escalemos la magnitud de información compartida a diario a la cantidad de estudiantes en el curso, en el colegio, en la ciudad, el país y el mundo: http://www.worldwidewebsize.com/

De la misma manera, analicemos la cantidad de usuarios por país de diferentes sitios: https://internet-map.net/ y https://www.internetsociety.org/map/global-internet-report/

Por todo lo expuesto anteriormente, concluimos que es necesario un gran espacio físico para almacenar todo ese volumen de información, se mostrarán fotografías de diferentes datacenters y se reflexionará respecto al costo de mantener la infraestructura de almacenamiento.

Para el funcionamiento de los datacenters, es necesario: discos, servidores, elementos de refrigeración, consumo eléctrico, el espacio concreto para disponerlos, etc.

Estos recursos necesarios requieren mucha inversión, pero los servicios de las redes sociales mencionadas no parecerían cobrar por sus servicios al usuario final. Analicemos las siguientes preguntas:

- ¿Se paga por usar Google y sus servicios? ¿Y Facebook, Twitter, Instagram, Snapchat, etc.?
- Si tienen que abastecer toda la estructura antes mencionada, ¿dónde está el negocio?
- ¿Quién tiene acceso a la información que compartimos? ¿Solamente las aplicaciones o sitios a los que los subimos?
- ¿Quién o quiénes son dueños de nuestra información?
- Una vez que borro del teléfono algo que compartí, ¿desaparece de la red? ¿Y si lo borro de la aplicación que utilicé? ¿Ocurre lo mismo si mando algo por WhatsApp?
- Entonces, ¿somos los dueños exclusivos de lo que compartimos en Internet?

De lo debatido anteriormente, se deja en evidencia el negocio detrás de la información de los usuarios, la perdurabilidad de la misma y la pérdida de control luego de compartirla.

Los datos publicados se comercializan de diversas formas: para definir perfiles de usuarios, analizar comportamientos, ofrecer y publicitar contenidos y productos. Además, será importante enfatizar que la información deja de ser propiedad de quién la genera. Al momento de enviar o subir algo su privacidad depende de la voluntad de quién o quiénes lo reciban, y por más que se decida eliminarlo de aplicaciones y dispositivos, aquellos que lo hayan descargado podrán distribuirlo tantas veces como quieran.

Además, tengamos en cuenta que ocurre con la voluntad de las personas que aparecen en fotografías utilizadas como memes o videos viralizados y la pérdida de control respecto al uso de su imagen. Lo mismo con la distribución de capturas de pantalla con conversaciones privadas, y las posibles consecuencias que puede ocasionar su uso descontextualizado.

Actividad 13

Como actividad de cierre, les solicito que investiguen sobre diferentes modalidades de recopilación de información privada, formas de extorsión virtual y sobre la importancia del consentimiento del propietario de la información al momento de distribuirla.

Como forma de evaluar dichas investigaciones y ***de manera opcional***, en grupos de 5/6 alumnos deberán diseñar afiches para concientizar a la comunidad educativa respecto a estas temáticas.

Sitio con información y recursos sobre el uso seguro de Internet: https://www.is4k.es/necesitas-saber

Conclusión

Buscamos darle una identidad concreta al concepto de Nube. De esta manera comprendimos por un lado su dimensión física, el tamaño y la costosa infraestructura que requiere y se identificó la existencia de los propietarios de los espacios dónde se almacena la información compartida en redes sociales. Destacamos los intereses de estos dueños de los datos que brindan sus servicios sin costo aparente para los usuarios.
Por otro lado, debemos darle mayor relevancia a la información que se comparte, entendiendo que uno no tiene garantías de poder decidir luego de haber publicado determinados contenidos
Por último, aprendimos los conceptos de ciudadanía digital y cuidado de la información personal para poder reconocer situaciones de riesgo o de violaciones a la privacidad y cómo evitarlas.

Navegando la web

Actividad 14

La clase comenzará identificando aplicaciones y sitios de uso habitual o reconocibles por las/los estudiantes:

- ¿El Facebook que usan es igual al de tus compañeros? ¿Y cuando acceden a otro sitio o aplicación, como Google, YouTube, Netflix, Spotify, etc., todos ven exactamente lo mismo?
- ¿Cuáles son las diferencias entre unos y otros?
- Cuando se crea una cuenta por primera vez en alguno de ellos ¿Encuentran más similitudes entre distintas cuentas que luego de usarlos por un tiempo?

Cuando se accede al mismo sitio web o aplicación el contenido puede variar según el usuario. Los resultados y el orden de las sugerencias que realizan las aplicaciones al ejecutar una búsqueda en, por ejemplo, YouTube, Google y otras aplicaciones, como Spotify, Netflix, Instagram o Twitter desde diferentes cuentas de usuario pueden variar.

En grupos de 5/6 alumnos/as responder las siguientes preguntas:

- ¿Cómo hacen las aplicaciones para saber qué sugerirnos?
- ¿Qué creen que pasará si realizan la búsqueda de “heladería” en su celular en Buenos Aires y luego la realizan en Córdoba?
- ¿Hay publicidades en sus perfiles? ¿Tienen relación con sus intereses o con sus últimas búsquedas? ¿Serán las mismas que vean todos sus compañeros?
- ¿Por qué no nos recomiendan las mismas canciones en Spotify, las mismas películas en Netflix o videos en YouTube? ¿Por qué varían los resultados de las búsquedas?
- ¿Con cuánta libertad creen que eligen lo que quieren ver?

El objetivo de estas preguntas será identificar la personalización con la que funcionan los distintos sistemas de recomendaciones de las aplicaciones de Internet. Si por ejemplo se empieza a seguir usuarios en una red social como Twitter que sean todos fanáticos del mismo equipo de fútbol, seguramente con el tiempo todas las nuevas recomendaciones serán sobre usuarios fanáticos del mismo equipo. Poco a poco se irá aislando el perfil en una burbuja de información muy relacionada con los intereses, la cultura, la ideología, etc. del usuario. Pero también se lo irá alejando de aquellos perfiles que no tengan puntos en común, se irá conformando una construcción de la realidad que reforzará esos espacios de pertenencia y posiblemente dará una percepción errada de la existencia de otros.

¿A quién puede interesarle la información sobre los subconjuntos de usuarios con perfiles similares? Estas formas de segmentar usuarios se utiliza para ofrecer productos y cuando se venden los espacios publicitarios se incluyen los potenciales interesados ya preseleccionados. Por esta razón, las búsquedas recientes condicionan las apariciones de las publicidades en las redes. “El usuario X quiere comprar un helicóptero sumergible, vamos a mostrarle todas las publicidades de los clientes que ofrecen en venta helicópteros sumergibles y productos parecidos”.

Otra forma de utilizar estos subconjuntos es para instalar rápidamente algún tipo de opinión sobre determinado tema. Con este objetivo se utilizan noticias promocionadas, lo que garantiza mayor alcance y luego es replicada dentro de los grupos de usuarios instalando su contenido. Con el mismo objetivo, existen administradores de varias cuentas falsas de forma organizada que publican una perspectiva sobre un tema que es replicada por cuentas reales dentro de sus grupos de influencia, generando así tendencias en las redes y construcciones de la realidad mediatizadas.

¿Sabías qué?

En el año 2012, la campaña de Barack Obama se orientó en recopilar y analizar diferentes perfiles de votantes e ir incorporando información de Facebook para poder estudiar a los indecisos e identificar a aquellos perfiles con intereses que no se vinculaban con el de sus votantes. Basándose en la información recolectada se aplicaron estrategias de comunicación acorde a los intereses y consumos del público filtrado. Por ejemplo, se publicitó en determinadas series.
Utilizando éste y otros ejemplos podrán presentarse conceptos como Big Data, que engloba la recopilación, el procesamiento y el análisis de grandes volúmenes de datos, y Machine Learning (aprendizaje automático), referido a las diferentes técnicas de programación que permiten a las computadoras recopilar información y realizar acciones de manera autónoma basándose en determinados ejemplos y patrones, razón por la cual suele decirse que “aprenden”.

Actividad 15

¿Cómo haría para acceder a información más allá de la “burbuja” a la que suelen inducirlos los diferentes filtros? ¿Cómo suelen hacer para acceder a información en Internet?

Respondiendo las preguntas anteriores y si usamos como navegador de internet por ejemplo a Google Crome, veremos que suelen destacarse los sitios que contrataron el servicio de Google para aparecer en las primeras posiciones como anuncios, luego, otros resultados que, si se puede comparar entre usuarios, no serán exactamente los mismos ni estarán organizados de la misma manera.

De lo expuesto anteriormente, evidenciamos que nuevamente se está estableciendo un orden de recomendaciones, basado en algún criterio, que en general los usuarios no suelen analizar o cuestionar, concluyendo sus búsquedas tomando principalmente las primeras opciones de la lista.

¿Ahora bien, todo lo que muestra el buscador en relación a determinadas búsquedas es todo lo que existe en Internet al respecto?????? Claramente la respuesta es NO. Es aquí donde entra en juego el concepto de ***indexado***. La información posee referencias que utilizan los navegadores y que hay información, por ejemplo, la que pueden volcar en un documento privado, la que se encuentra dentro de un aula virtual o en sitios que requieren loguearse con usuario y contraseña, que no forma parte de los resultados de un buscador. Asimismo, aquella información de la red a la que los buscadores no pueden acceder se denomina ***Internet Profunda, Internet Oculta*** o ***Deep Web***.

La Internet Profunda suele relacionarse con contenidos ilegales o peligrosos, pero incluye todo tipo de contenidos que simplemente no están indexados y no son identificables por los buscadores.

Conclusión

El objetivo de esta clase fue reconocer mecanismos de recopilación de información personal en los sitios, aplicaciones y redes sociales, el funcionamiento de los algoritmos de recomendaciones, la forma de organizar a los usuarios respecto a sus intereses y la utilización de esta información por los denominados filtros burbuja

Recursos

.

Artículo de Adrián Paenza sobre la recopilación permanente de información personal y sitio de Google dónde se almacena

https://www.pagina12.com.ar/80074-mi-actividad
https://myactivity.google.com
https://miactividad.google.com/miactividad

Artículo de Esteban Magnani sobre la recopilación de información en Internet y Big Data.

http://www.revistaanfibia.com/ensayo/quien-toma-tus-decisiones/

Utilización de las redes sociales en las campañas políticas

http://noticias.perfil.com/2017/05/14/macron-trump-y-obama-presidentes-de-las-red es-sociales/

¿Cómo funciona Google?
https://elgatoylacaja.com.ar/destripando-google/

Internet, ¿para todas y todos?

Abordaremos el alcance de la red en los objetos cotidianos, reflexionando sobre Internet de las cosas, sus posibilidades e inconvenientes. Luego, se problematizarán las posibilidades de acceso a Internet con la que cuentan las personas a lo largo del mundo, y las libertades y limitaciones que esto implica, contemplando la dimensión social de Internet.

Actividad 16

En la primera actividad de esta clase se buscará problematizar sobre los alcances de Internet en objetos de uso cotidiano que hasta hace poco tiempo no tenían conectividad. El principal objetivo no será demonizar la presencia de Internet en los objetos sino analizar la relevancia de su presencia y los inconvenientes de que se incorpore sin tomar los recaudos necesarios.

- Partimos de una situación hipotética: Un artista excéntrico y fanático de la tecnología invierte toda su fortuna en una casa inteligente donde la mayor parte de los electrodomésticos tiene conexión a Internet.
  ¿Es tan excéntrico? ¿Qué artefactos tendrán conexión a Internet? ¿Cómo se modificará su funcionamiento? ¿Qué pasará en la vida del artista cuando se corta la luz o se "cae" Internet?

Formar grupos de 5/6 alumnos/as y analizar las diferentes noticias que figuran como recursos al final de este tema. Algunas noticias sobre nuevos electrodomésticos con conectividad y otras con problemas de seguridad de los mismos.

Luego de la lectura de las noticias indicadas anteriormente y de su posterior investigación en Internet, cada grupo tendrá que responder brevemente las siguientes:

- ¿Qué problemas resuelve la tecnología que describe el artículo? ¿Cómo resolverían esos problemas sin que el objeto utilizara Internet?
- Estos dispositivos con cámaras, micrófonos y conexión a Internet, ¿podrían resultar invasivos o peligrosos para la intimidad de las familias y las personas?
- ¿Qué problemas de seguridad podrían ocasionar este dispositivo? ¿Cómo podrían evitarse?

Los objetivos de esta actividad fueron tomar dimensión de la presencia de Internet en todo tipo de objetos y remarcar que no hay garantías de que un sistema sea infalible, por esta razón es que hay que tener especial cuidado sobre la información que se comparte a través de las redes y dispositivos.

Actividad 17

Responder en grupos de 5/6 alumnos el siguiente cuestionario que está compuesto por preguntas para reflexionar sobre las posibilidades y limitaciones para acceder a Internet y sus contenidos y preguntas que servirán para revisar los temas abordados en las clases anteriores:

- ¿Todas las personas, gobiernos, empresas e instituciones deberían poder acceder a Internet por igual?
- ¿Creen que tener acceso a Internet es un derecho?
- ¿Quién debería garantizar el acceso a Internet?
- Si observamos el diagrama de la primera clase de Internet, ¿qué limitaciones físicas se les ocurre que impiden el acceso para todos y todas? ¿Quién es responsable de administrar el acceso a la red en el punto del recorrido que señalaron?
- ¿Qué opinan acerca de restringir contenidos en Internet? ¿Consideraron discursos que contradigan intereses políticos o contenidos sensibles como la pornografía infantil?
- En caso de que se regulasen determinados contenidos, ¿quién debería ser responsable de hacerlo? ¿Esas regulaciones deberían ser para acceder o para compartir contenidos?
- ¿El tráfico de la red debe ser distribuido con la misma prioridad para cualquier finalidad y tipo de usuario?
- ¿De quién es la información que compartimos en la red?
- ¿Existe la privacidad en Internet?
- ¿Qué consecuenciás podría traer la desaparición de la “s” en todos los sitios que comienzan con “https://”?
- Si se apagaran todos los servidores DNS, ¿podríamos seguir navegando por Internet? ¿Por qué?
- ¿Puedo acceder a la Internet oculta desde mi celular?
- ¿Todo el contenido de la Internet oculta están relacionados con la clandestinidad, el delito organizado o algún tipo de contenido prohibido?
- ¿Utilizar el modo incógnito de un navegador es una forma de mantenerse en el anonimato?
- Si se cortaran los cables que ingresan por Las Toninas, ¿qué pasaría con la conectividad de nuestro país? ¿De quién/quienes son esos cables?
- ¿Por qué creen que se abordaron contenidos de Internet a lo largo de las clases?
- ¿Es lo mismo una URL que una dirección IP?
- ¿Cómo buscarían algo en Internet sin utilizar un buscador? ¿Cuáles son las consecuencias de usar uno?
- ¿Los algoritmos de cifrado asimétrico brindan más seguridad que los de cifrado simétrico? ¿Por qué?
- ¿Cuál es la relación entre las cookies y la privacidad?

Actividad 18 (cierre)

Como cierre de los contenidos relacionados con Internet escribir en grupos de 5/6 alumnos/as un cuento de ciencia ficción que incluya alguno de los siguientes temas (en caso de ser necesario, hacer uso de los recursos indicados al final de esta actividad):

- El mundo sin Internet. ¿Cómo imaginan que serían sus vidas sin internet? ¿Cómo serían sus comunicaciones? ¿Qué cosas creen que tendrían que modificar su funcionamiento?
- Internet de las cosas. ¿Qué nuevos objetos irán sumando la conexión a Internet a sus funcionalidades? ¿A qué objetos de la vida cotidiana les agregarían Internet? ¿Qué cambios habría en la vida cotidiana? ¿Qué problemas podrían tener u ocasionar los nuevos objetos conectados?

Conclusión

El eje temático de Internet se compone de distintos abordajes según fueron encarados a lo largo de las distintas clases.

Es importante articularlos permanentemente para no perder de vista que los aspectos físicos, económicos, políticos y sociales

Recursos

Artículos sobre Internet de las cosas:

https://www.clarin.com/tecnologia/aspiradoras-inteligentes-pueden-vulnerar-privacidad_0_S1PJb-BLZ.html

https://hipertextual.com/2017/07/roomba-privacidad/amp?utm_content=buffer4e5ac&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

https://www.bbc.com/mundo/noticias/2015/12/151215_finde_tecnologia_barbie_interactiva_habla_polemica_espia_ninos_lv