¿Como hacemos para ver los posts más interesantes de toda la red, los cuales se encuentran en el perfil personal de Facebook del profesor?

Tradicionalmente se entiende que si abrimos el navegador digitamos la url: Facebook.com/sgrysoft, al tener la sesión iniciada podemos ver los posts del profesor y ya está, pues no, las cosas no son tan simples para los informáticos, pero tampoco es magia negra.

Primero vamos a suponer que tenemos un computador (PC) y un laptop en nuestra casa, ambos se pueden comunicar entre ellos de forma directa mediante un cable de ethernet, pero si se añade un tercer dispositivo ya no podría conectarlos o necesitaría un adaptador y ni hablar si el tercer dispositivo es un celular que no tiene el puerto ethernet.

Este era un problema latente en los inicios de la computación, por lo que se inventó un aparato llamado Switch, este es una cajita con varios huecos y lo que haces es compartir la red con todos los conectados a esos huecos, el switch se encargan de enrutar los datos, y comienza a preguntar a cada dispositivo si el mensaje era para cada uno de ellos, por ejemplo el pc1 quiere mandar un mensaje al pc3, el switch pregunta al pc1 si el mensaje era para él, luego al dos, luego al tres y si el mensaje era para el 3 le envía el mensaje completo, pues inicialmente solo manda una cabecera, esto quiere decir que en red no hay mucha privacidad de datos porque técnicamente todos los recursos son compartidos. Por ejemplo, si tú que eres un maldito enfermo… o una dama muy curiosa, desea abrir una página web de cocina llamada redtube.com que es un sitio donde cocinan carne, el .com es de comida, bueno, el switch va a enviar la petición de esa página por la computadora 1, dos, tres y 4, hasta que encuentre cual es el lugar que le da salida a internet para poder hacer la petición de lugar.

Este mecanismo funciona aunque no sea eficiente, pero no funciona con teléfonos, pues estos se conectan en red mediante un sistema de red llamado WIFI, y para esto

existen un Router Wifi estos son unos aparatos con antenas y conexiones que me dan acceso a internet, esos los puedo conectar al switch para que sean parte de la red, este crea un cable virtual entre el dispositivo conectado (teléfono) y el router, ellos tienen de manera interna una especie de switch por demás inteligente, por lo que no siempre es necesario tener un switch físico adicional.

Los routers tienen software, por lo que podemos decir que son inteligentes debido a que estos necesitan enrutar ciertos datos, a diferencia de los swith, estos almacenan el nombre de la red, lista de ips, contraseña de la red y otros datos.

Un router puede tener wifi o no, el router asigna la ip mediante el protocolo que habíamos visto antes llamado DHCP.

Esta ip es recordada debido a la mac address que tiene cada dispositivo, esta es por interfaz de red, es decir, el ethernet, el wifi, el bluetooh, las antenas de radio, cada una tiene una mac address, esta es el número de identificación de las piezas de hardware que se conectan a una red.

Estos finalmente convergen en la cajita de internet llamada modem de isp que nos haya dado el proveedor de internet, que es un aparato con una entrada y una salida, la entrada por donde recibe internet de la calle puede ser ADSL (cable coaxial) por teléfono de forma directa, por una antena de radio llamada 4g o LTE o por fibra óptica que es la forma mas eficiente hasta el momento.

Todo esto es solo para armar la red interna en tu hogar antes de que esta salga a internet.

Existe algo llamado IP, que no es más que internet protocol, es una serie de números que identifican un computador.

Cada dirección IP está compuesta por 4 números separados por puntos y son una forma de comprender números más grandes y complejos. Las direcciones IP tienen una estructura que las convierten en privadas o públicas y que además hacen parte de la máscara de red y el geteway.

Nuestro pc tiene diversas ips; está por ejemplo la que nos identifica en internet en la red global del planeta, y en nuestra red local tenemos otra, es labor de los routers decidir qué ip nos van a asignar.

La Ip local interna de cada pc es la 127.0.0.1 o conocido como el localhost, es un apuntador que siempre apunta a nosotros mismos, ósea al mismo que pc en el que estemos tecleando.

Pero tenemos una ip de la LAN (local área network) es la red donde están todos los dispositivos del hogar, aquí se nos va a asignar una ip local de la red en cuestión que no se va a repetir dentro del mismo segmento de red, normalmente es distribuido por el router mediante una lista de ips de manera secuencial. Los primeros tres bytes de la ip no suelen cambiar "192.168.0" el que varia es el cuarto byte, pero si tenemos mas de 255 dispositivos, porque las ips no suben más del número 255, o más bien de 254 porque el 255 es reservado para hacer broadcast, entonces voy a tener que verme obligado a realizar una sub red, lo que me da en total unos 65025 dispositivos posibles para conectar en una sub red tomando los 255 del segmento 3 de red.

Todo esto se hace a través de puertos, los puertos son una especie de red virtual dentro de los sistemas operativos estos abarcan desde el 1 hasta el mayor byte posible con dos bytes (65,535), cada puerto tiene funcionamientos diferentes, el sistema operativo al distribuir los puestos mediante de los anillos del sistema (0. Kernel, 1. Drivers delicados, 2. Drivers Accesibles, 3. Aplicaciones) y hay una serie de puertos cerrados por defecto o más bien capturados, reservados por el sistema operativo, que son del 1 al 1024 estos son reservados para que el S.O. los ejecute a través del administrador, hay muchos protocolos corriendo mediante este por

ejemplo el protocolo http que es el 80, es el usado en caso de tener un servidor web corriendo en nuestro pc, pero si tienes un servidor de Torrent en tu pc este usa los puertos desde el 6881al 6889. Nuestro pc puede conectarse a internet de manera cifrada con el protocolo conocido como https, y esto se hace por el puerto 443, si me quiero conectar a otro dispositivo mediante una consola segura (SSH) usaríamos el puerto 22.

La máscara de red o redes es una combinación de bits que sirve para delimitar el ámbito de una red de ordenadores.1 Su función es indicar a los dispositivos qué parte de la dirección IP es el número de la red, incluyendo la subred, y qué parte es la correspondiente al host. Mediante la máscara de red, un sistema (ordenador, puerta de enlace, router, etc…) podrá saber si debe enviar un paquete dentro o fuera de la subred en la que está conectado. Por ejemplo, si el router tiene la dirección IP 192.168.1.1 y máscara de red 255.255.255.0, entiende que todo lo que se envía a una dirección IP con formato 192.168.1.X, se envía hacia la red local, mientras que direcciones con distinto formato de direcciones IP serán buscadas hacia afuera (internet, otra red local mayor, etc…).

La pasarela (Gateway) o puerta de enlace es el dispositivo que actúa de interfaz de conexión entre aparatos o dispositivos, y también posibilita compartir recursos entre dos o más computadoras. Su propósito es traducir la información del protocolo utilizado en una red inicial, al protocolo usado en la red de destino.

La pasarela es normalmente un equipo informático configurado para dotar a las máquinas de una red de área local (Local Area Network, LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones de red (Network Address Translation, NAT). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada “enmascaramiento de IP” (IP Masquerading), usada muy a menudo para dar acceso a Internet a los equipos de una LAN compartiendo una única conexión a Internet, y, por tanto, una única dirección IP externa.

La traducción de direcciones de red o NAT (del inglés Network Address Translation) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

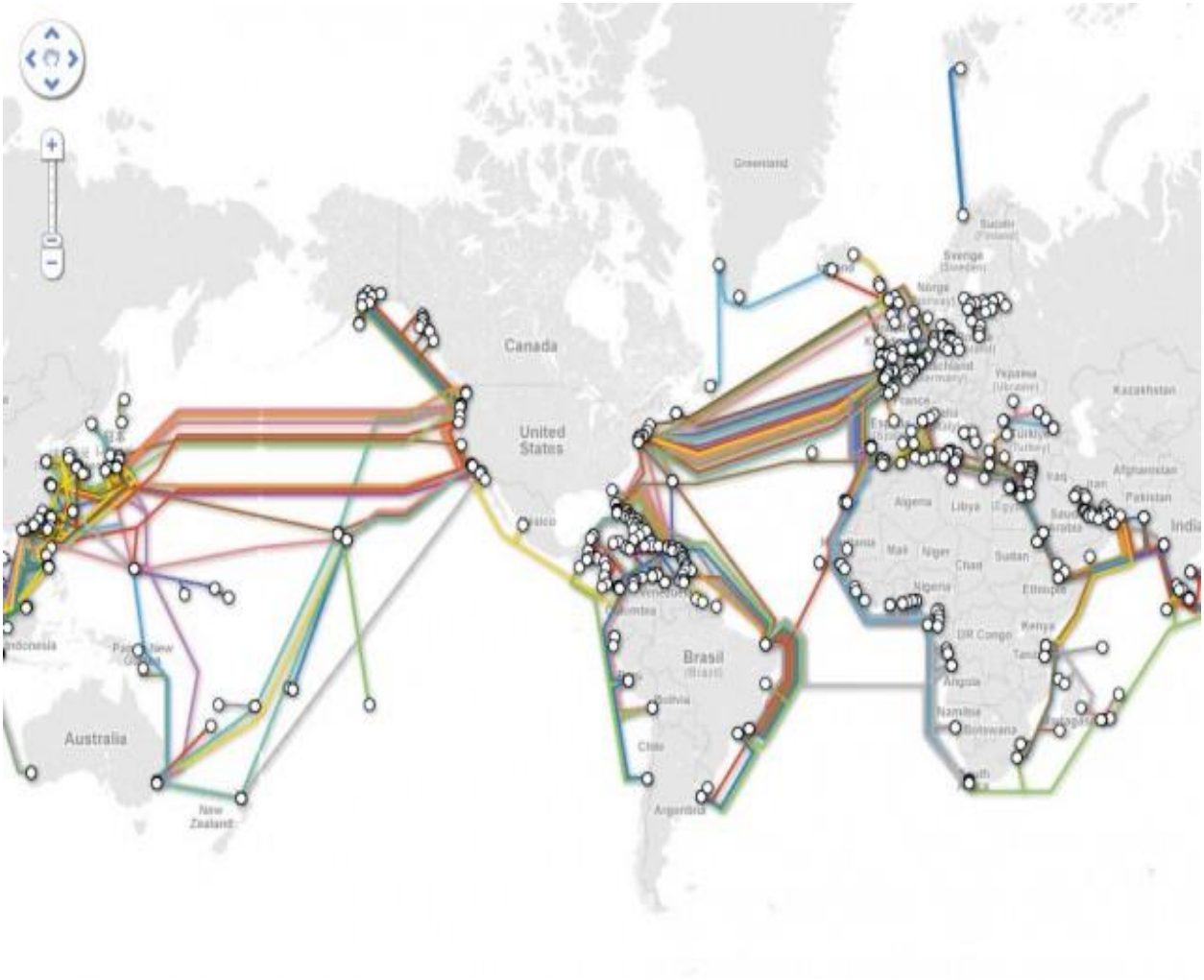
Ya con esto estamos listos para salir a internet, muchos creen que la señal va al espacio y es redireccionada y trabajada por satélites, pues no, apenas el 2% de la comunicación mundial se hace mediante satélites. Así que no es con satélites como realmente funciona, internet funciona con cables, todo nuestro planeta esta lleno de cables, el modem del ISP se conecta mediante ADSL, 4g o fibra al ISP.

El ISP es un lugar físico en algún lugar del mundo, es una empresa de servicios telefónico, claro, viva, Altice, estas son empresas especiales que proveen el servicio de internet, estas son las que nos mandan un cable a nuestras casas, ellos se conectan a internet de una de dos formas.

Existe un concepto llamado NAP network access point, es un lugar enorme donde los países cableaban conexiones de internet super lejanas con otros países y era acceso al NAP que el país le vendía al proveedor de internet y el proveedor se lo revendía al consumidor, pero el mundo cambió y ya no funciona así, no era suficiente que los gobiernos proveyeran el acceso a internet, las empresas se jartaron de esperar y se vieron obligadas a crear sus propios puntos de manera independiente porque le gobierno con su movimiento burocráticos y lentos no podían lograr montar las redes que necesitaba el mundo para conectarse más rápido por lo que se inventó esos diversos lugares en el mundo que son empresas privadas llamadas IXP's, internet xchanges points.

Todas estas conexiones se hacen a través de cables submarinos que a cada rato se viven rompiendo por ataques de tiburones, o por sin oficio que se lo roban o anclas de barcos que lo rompen sin querer, ahora bien, no todos los IXP están conectados entre sí, hay otros que no forman parte de internet en sí, sino de unas redes

privadas, y como el caso de china una super red privada que se conecta a un IXP, es decir, todos ellos se conectan entre si por varios IXP's privados alrededor de toda china y luego salen al mundo a través de un solo canal, por el cual es monitoreado todo.



Entonces un ISP se conecta a uno de estos cables submarinos a través de los IXP y es por ahí que nos da acceso a internet e internamente hay un NAT que traduce la petición y la lleva a internet de verdad, cuando abrimos en nuestra pc "fb.com" lo que hacemos es atravesar estos cables submarinos para llegar a algún lugar especial.

Ese lugar especial es conocido como DNS, Los dns son servidores que tienen una base de datos en la cual saben a qué IP corresponde un nombre, si yo abro fb.com

lo primero que hago es hacerle una petición al dns antes de poder abrir un sitio web, esto es lo primero que hace el isp cuando le pedimos abrir algo, hay muchos server de DNS alrededor del planeta, cada uno de ellos tienen copias de cuáles son los diferentes sistemas de dominio que podemos encontrar afuera. Están por todas partes para que la señal viaje lo mínimo posible.

Estos también tienen subdominios, que pueden tener una ips igual o distinta, y también guarda el servidor especial de envió de Email, que recordemos que funcionan muy distinto a todo lo demás, esto se hace en un apartado especial llamado Mx Records, que es donde se guarda donde vive el servidor de correo, debemos recordar que por ejemplo nosotros podemos tener nuestro propio servidor de email o podemos tener los servidores de email de un tercero como Gmail, es aquí donde se guarda la ruta por donde acceder a estos.

La velocidad es muy importante en internet porque las conexiones son muy caras, internet funciona con cables submarinos que tiene un tráfico compartido por todo el mundo, los proveedores de internet tienen que pagarle a los ixp para poder acceder a ese tráfico, a veces intercambian tráfico uno por el otro, pero siempre hay dinero de por medio, es caro conectarnos a través de los IXP, montar cables submarinos, mantenerlo etc, el dinero viene de nosotros en la famosa última milla.

El isp nos monta a todos en una sub red llamada MAN metropolitan área network para de esa forma si existen datos que ya uno dentro de la red ha descargado entonces redistribuirlo a otro que lo necesite, en el caso de que yo este viendo redtube.com entonces el isp te va a mandar de la información que ya yo descargue el video que tú quieres ver, así que hay un grupo de gente en claro que pueden saber toda la porno que ves aunque estés en modo incognito :D

Pero cuando se va a comunicar con algún computador que ya no está dentro de la MAN si tiene que pasar por el proceso ya explicado previamente, y aquí es que ellos hacen algo llamado QoS quality of services, que en verdad lo que hace es achicar las

conexiones a través de network shapers lo que hace es que cuando me lleguen bytes de llamadas le doy prioridad, emails mayor prioridad, pero videos de youtube o Spotify le bajo la prioridad al máximo, por eso el test de velocidad te puede dar 100mb pero el video tarda mucho en cargar.

Actualmente se llama network shapping o throttling.

Los proveedores de servicios (fb, twitter, Google, microsoft), como saben que existe este inconveniente y que no hay forma de luchar contra ellos, lo que hacen es hacer uso de una herramienta llamada CDN content delivery Network, estos son servidores que cuando los datos no tienen que ser procesados por algoritmos, ósea un video, una foto, cuando son archivos estáticos, lo replican por todo el planeta, por lo regular estos viven en el mismo datacenter de los ixp y los que no viven juntos están cerca, entonces según tu ip ellos te envían al CDN más cercano, por eso no hay un solo servidor de Facebook, hay múltiples alrededor del mundo que están replicando constantemente la conexión, y son estos los que te dan acceso al contenido interno que tiene Facebook, son estos los que hacen posible que internet como lo conocemos funcione y que funcione rápido.

La mayoría de los ISPs (Internet Service Providers) nos venden ancho de banda en Mb y debemos tener claro qué significa, ya que existe una importante diferencia entre Megabits y MegaBytes.

Otro aspecto importante en el funcionamiento del internet es la velocidad. A menudo confundimos la velocidad con el ancho de banda por eso debemos tener en claro que la velocidad del internet se mide obteniendo el tiempo que le toma a la información viajar a través de un punto a otro en milisegundos, a esto se le conoce como ping o latencia.

-No se está vendiendo una conexión de 10Mbps, se está vendiendo una conexión de 10 Megabits, para descubrir la verdadera diferencia es necesario dividir ese valor entre 8.

-¿Cuánto tiempo tarda la conexión en establecerse?: esto se conoce como ping, el cual es el tiempo que tarda la conexión en establecerse, esta se da en milisegundos.

Eso es lo que le toma a la conexión salir de la casa, saltar cada canal, y encontrar el servidor de google para poder establecer la conexión.

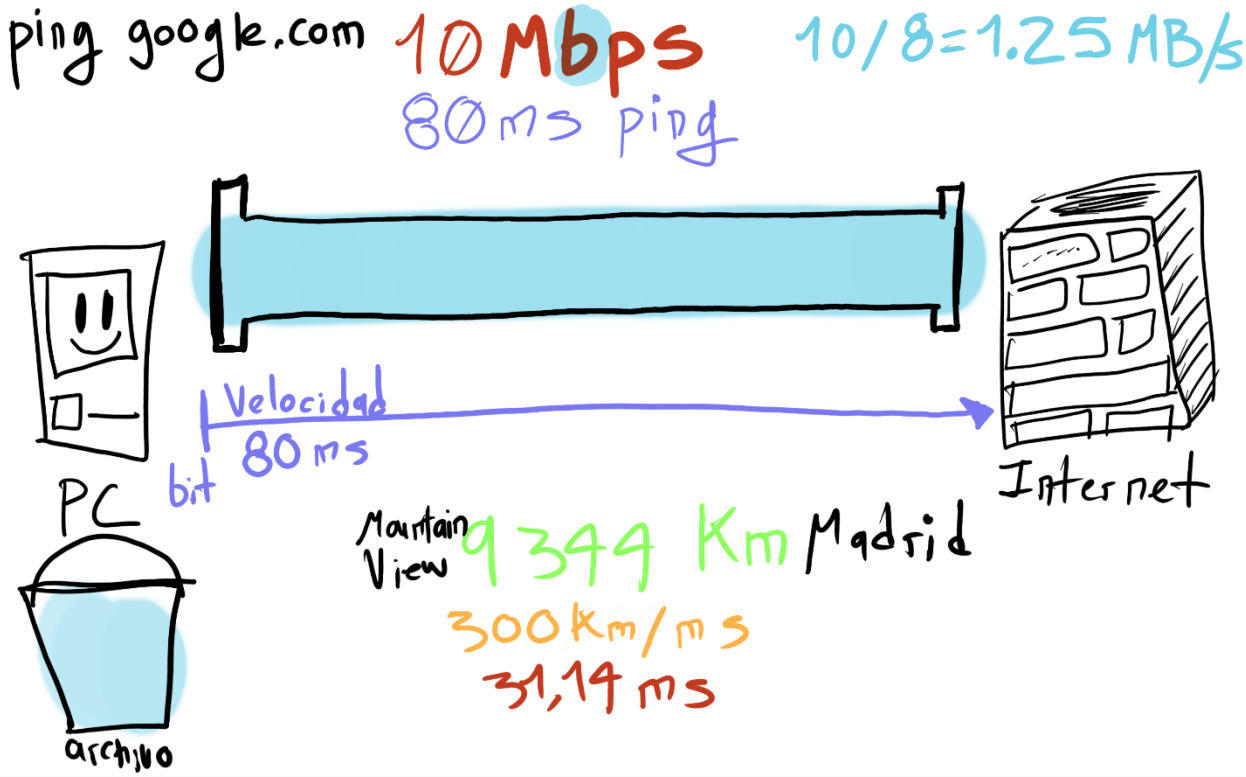
Mb/ps: Cantidad de datos que en un segundo caben por el tubo de la conexión.

-9344km separan Madrid de Mountain View, y la velocidad viaja a 300,000km/s en el vacio.

La forma de medir la velocidad de un ping es dividiendo la distancia entre un punto de conexión y otro entre la velocidad de la luz 300 km/ms

Distancia entre Mountain View y Madrid 9344 km

(9344 km)/(300 km/ms) = 31.14 ms



Qué es el Modelo Cliente/Servidor

El cliente no es más que el navegador, en el cual tu abres un archivo HTML, fin, nos podemos ir para la casa, bueno, no tan simple, porque este HTML invoca un archivo JavaScript, y eso genera un efecto en programación, a esto que se ejecuta en el navegador, normalmente se le llama Front-End.

En este proceso tenemos luego el servidor, que es algo que corre en internet, en la famosa nube y es ahí donde tenemos el Back-End, y este es el que se conecta a las bases de datos.

Estos son los dos mundos de los programadores actuales, frontend y backend, son los mundos donde vas a encontrar empleo en la actualidad, normalmente los programadores profesionales se enfocan en uno de los dos, pero ninguno sabe de una sola cosa, todos los profesionales de verdad aprenden algo del otro al que no se especializaron.

Base de datos existen muchas opciones, tanto relacionales como no relacionales, las relacionales son las que liderearon el mercado de las base de datos legacy, por su robustez y versatilidad a la hora de implementar, pero dada la gran demanda de datos que se necesitan consumir de una entidad en la actualidad, donde no podemos darnos el lujo de normalizar de la forma estándar a cada individuo porque cada caso es único, entonces ahora están tomando auge (y gracias a la recolección de datos) las base de datos no relacionales. Dentro de las relacionales tenemos a MySql (Maria), Oracle, Ms Sql y dentro de las no relacionales, tenemos a MongoDb, Cassandra, Redis entre otras.

En el Backend, las tecnologías de Backend son el código de programación que corren los servidores, que corren las máquinas que están en internet y que procesan estos

datos, el líder indiscutible de tecnología Backend es Php, esto debido en gran medida a que más de la mitad de internet está hecho en WordPress, así que es una medición un tanto desleal, pero tenemos también a Ruby, Python, Node, C#, Go, java, etc. Node es un caso particular, porque este lo que hace es permitir correr JavaScript del lado de servidor a través de algo llamado servidor de eventos.

El servidor es ese software sobre el que se ejecuta el Backend, así como en el lado del cliente es el navegador el que se encarga de abrir e interpretar el HTML, CSS y JavaScript, en el lado del servidor (de la maquina) debe haber un software que procese Python, Node, Php, etc, los servidores más populares son nginx, apache, node, IIS (internet information server), por cierto, nginx corre tecnologías Microsoft, por lo que no siempre es necesario IIS en todos los casos, para estos fines.

El servidor es un software que agarra la dirección, la Url que le colocas en un puerto y te muestra los resultados, los procesa por detrás, el puerto casi siempre es el 80, el navegador internamente sabe que puerto tiene que poner, estos puertos son los huequitos que tienen los servidores por donde se van los datos.

Las tecnologías de Frontend son las que corren en el navegador, las tres fundamentales, son HTML en su versión 5, CSS en su versión 3 y JavaScript en su versión de Ecmascript 6, y basado en estas tecnologías hay librerías como Angular, React, también hay preprocesadores como Stylus, sistemas de plantillas como jeil, etc.

Cuando tienes un grupo de tecnologías esto normalmente se llama Stack (pila), o colección de tecnologías, el stack más popular es LAMP, que significa un servidor Linux en el que corres Apache, donde recurres a una base de datos es MySql y tu lenguaje de programación es Php.

Vamos a ver entonces como funciona una llamada a una página como redtube.com que es un sitio para ver tubos rojos en internet, ya saben que hay gente viendo toda clase de cosas y así como hay gente que le gusta ver gatos, también hay gente que les gusta ver tubos, tu entras a tu navegador, escribes la dirección, después presionas Enter, eso envía una señal de teclado y pasa por los procesos que vimos en el tópico 1, pasa por el ISP que vimos cómo se realiza en el tópico 2, esta petición va al DNS y es donde se cambia esta ruta, este nombre por la IP, que es la dirección en internet del servidor al cual apunta ese nombre de dominio, una vez tengo la IP del servidor de redtube (computadora o lugar físico), el servidor (aplicativo) de redtube recibe la url dentro de su software servidor que asumimos es apache, una vez recibido ese dato redtube le pasa los datos al lenguaje del programación del Backend para que los procese, asumamos que ellos usan Node o Python, esos lenguajes van y se conectan a las base de datos, procesan y luego crean un archivo resultante HTML, JavaScript y CSS, que es el que le mandan al navegador para que renderice (dibuje) los elementos que componen la página y donde están los assets (elementos de la página) como el video que tú quieres ver.

Este es el ciclo de desarrollo de un server hasta generar los datos para el cliente y es así como accedes a la base de datos, algo importante es que tú nunca debes poder acceder a la base de datos directamente desde el cliente, porque no se si te has fijado que cuando uno le da clic derecho al navegador y luego inspeccionar elementos, puedes ver todo el código, incluido el JavaScript, no existe forma real de protegerlo, imagina entonces que tuvieras un código que se conecte a base de datos cualquier puede tener acceso a la misma, es por esto que siempre es necesario tener un Backend que es a quien se conecte el Frontend y basado en algunos datos, como usuario y contraseña el Backend accede a la porción de la información que esté autorizado a recibir, modificar o trabajar el usuario que se autenticó, y así sabe que datos enviarle de regreso al navegador.

Existen muchos métodos para comunicarme desde HTML y JavaScript al server es decir desde el Frontend hacia el Backend, los cuatro principales a pesar de que hay muchos más, son Get, Post, Ajax y Web Sockets.

El GET lo hemos visto muchas veces, es cuando entras a un sitio web y en la url, en la dirección tiene signo de interrogación, variable, igual valor, ampersan (&) variable igual valor, eso es mandarle a través de la url, valores al servidor, variables para que el las procese, esto es un tipo de envió de datos.

www.juegosmentales.online/test.aspx?categoria=infantiles&tipo=desafios

Pero si tu estas mandando un usuario y contraseña, jamás, pero jamás de los jamases deberías usar Get, porque si lo haces la contraseña queda en la dirección y cualquiera puede ir al navegador, mirar el historial, y busca en las url lo que parezca una contraseña y decir que ha hackeado la clave de la novia y ya con eso la hace mojar, porque a las mujeres les gusta sentir que tienen un hacker de pareja, para que no salga en la url, y para que salga por un camino secreto, los sitios deben ser enviados por un formulario, el POST es enviar variables como formularios a través de cambiar la url, pero no colocar los datos en la url, sino colocarlos por debajo, para ser muy técnicos, manda los datos en los headers del protocolo http, recapitulando, cuando tienes un formulario, lo que menos quieres es que se vea lo que envían, por ende tú le envías los datos a la siguiente página, por debajo en un lugar invisible por un túnel de comunicación secreto.

Pero seguro que has visto sitios que cuando colocas cosas, como usuario y contraseña o una publicación, cambia de forma automática, por ejemplo en fb cuando le pones un comentario a una foto inmediatamente aparece el comentario sin tener que recargar la página, en este proceso enviamos los datos de usuario y contraseña al servidor y si es la correcta le digo que tiene acceso a x botón sin necesidad de cambiar la página, ese paso de información y cambio de elementos sin cambiar la url, dentro del body, dentro de la propia sesión de la página se llama Ajax, por cierto, esto fue inventado por Microsoft en Explorer 6, tanto que le tiran al gigante de Montreal.

Sockets es una opción especial que sirve para transmitir información de lado a lado (cliente-servidor) en tiempo real, por ejemplo, los video juegos para intercambiar datos mientras juegas, los chats para mostrar lo enviado en tiempo real, etc.

Cómo funciona realmente un sitio web

Cuando escribimos www.mersyrd.com/login es que el navegador le hace una petición al sistema operativo para ver si en cache tiene el dns para resolver esta página, si usted entra a los sitios muchas veces no tiene sentido estar yendo a los servidores dns a cada rato, el navegador una vez entiende cual es la ip forma en la memoria RAM algo llamado Http Request y este lo organiza usando un formato llamado Get, recuerden que hay 4 formas populares de operar con datos, el Get es decirle al servidor deme, y post es decirle Tome, entonces lo que se hace en la petición es algo como lo siguiente:

Get/Login Http/2 Esta es la versión del protocolo.

Host: www.MersyRd.com El dominio al que quiero acceder, se manda el nombre en lugar de la ip, porque muchas veces en el mismo servidor corren múltiples dominios, por ejemplo en el server de mersy también corre praysoft.net, notasti.com entre otros, entonces la ip, sabiendo cual él es host, sabe cuál es el server al que le tengo que responder, porque una misma ip puede servir múltiples páginas web.

User-Agent: Chorme xx (esto viaja en las cabeceras http, viajan escondidas, el protocolo es mucho más largo, el navegador le dice que tipos de archivos acepta, cuáles no, que tiene instalado, que soporta, etc,

Estos datos los empaqueta y los envía directamente a la ip del servidor, y este los recibe por un puerto en particular, que es el 80 si es http o 443 si es https y es por aquí que se recibe esa petición.

El tercer paso es que nuestro server nos responda, el server normalmente responde en un formato similar. Envía un mensaje similar a este:

http 200 ok	(puede responder también 404 que significa no encontrado o 500 que es error de servidor entre otros, estos llegan directamente en la respuesta de http que es llamado http response
date: xxxxxx	
server: nginx xx (Linux)	
last-modified: xxxx	la última fecha de modificación, es muy importante porque puede que en cache en este instante esté el mismo archivo, por lo que no es necesario cargar otros archivos, este nos permite que el navegador sepa, que si es el mismo archivo que cargo ayer entonces no lo han modificado por lo que no tiene que cargar los assets, no tiene que cargar las imágenes, los css, solo lo dejo así.
content-lenght: 21	(esta es la cantidad de bytes que tiene la petición, a veces son muy largas)
connection: close	el estatus de la conexión, en este caso indicamos que se va a cerrar de forma automática, pero si fuera por ejemplo un chat la conexión debería permanecer abierta.
content-type: text/html	(el tipo de datos que se le está mandando, image/jpg o video/mp4)
Hola mundo	(el contenido del documento)

Si en el HTML yo estoy pidiendo otra serie de recursos, como una imagen, un background de fondo, una hoja de estilos, un código de js y si un código en js empieza a hacer peticiones de Ajax; paso por el mismo camino y ese es el punto número 4, que es hacer un **asset request** que es cuando empiezo a pedir cada uno de ellos de manera independiente, y lo único especial que tengo que hacer es volver al punto 1 con la url del asset sabiendo que esta sale del código HTML, y el navegador

se encarga de conectarse al server, resolver todas esas cosas y traer el asset correcto.

Seguro han escuchado muchas veces el termino cookies, hay formas de enviar y recibir datos del server, como el Get , sin embargo, ¿cómo hace el navegador para guardar mi sesión de usuario?, o ¿cómo hace para recordar un post que estaba redactando cuando se cerró el navegador o para guardar las contraseñas?, el secreto es las cookies, las cuales no van ni en el Request (petición al server) ni en el Response (Respuesta del server), van en ambos lados, son datos guardados muy similar a como funciona un DNS, es un nombre y un valor, es una variable, y eso se guarda en la cookie que se pega al Request, todos los request que yo haga al server traen las cookies como un polizón, y esa cookie va pegadita como otro elemento del protocolo http y se mete dentro del server cuando yo hago la petición, del lado del server yo también puedo cambiar las cookies y esta se actualizan cuando le respondo del server enviando el HTML, es decir el servidor manda la actualización de la cookie y llega la cookie cambiada como parte de la cabecera antes de enviar la respuesta HTML del protocolo http, por ende si mande una galleta de algún tipo al server, este la puede cambiar y responderme con una similar pero modificada con una cookie distinta, se llaman cookies, porque vienen de las galletas de la fortuna que por dentro tienen mensajes, es una forma escondida de mandar datos entre el cliente y el server, solo tengan en mente que estas pesan bytes y si siempre van pegadas tanto en la ida como en la de regreso, la cantidad de cookies que le agregues a un sitio web, van a hacer más pesada una carga tanto el envió de los datos como la respuesta de estos, si tienes 100k de cookies siempre va a tener 100 de ida y 100 de regreso por eso no abuces de estas.

Cosas que hacen posible internet y habitan en este.

Paquetes

Encapsulación de los bytes (datos) para ser transmitidos con un tiempo de vida, llamado TTL.

TTL (transistor-transistor logic o lógica transistor a transistor).

Es un concepto usado en redes de computadores para indicar por cuántos nodos puede pasar un paquete antes de ser descartado por la red o devuelto a su origen.

El TTL forma parte de la cabecera IP con un tamaño de 8 bits. El valor se inicializa en el emisor y tiene la función de ir descontando de un contador una unidad según el datagrama IP viaje de un nodo a otro, por lo que debe de ser recalculado en cada salto. Si dicho contador llega a cero, descarta el paquete recibido y lo reenvía al destino del que proviene en vez de difundirlo. Este campo de la cabecera IP impide la congestión o sobrecarga en las colas de las líneas de trasmisión, ya que, si un paquete está en la cola, el TTL se decrementa también si pasa un largo periodo.

En Internet este campo tiene un máximo arbitrario de 120 segundos, aunque depende del protocolo utilizado. El TTL como tal es un campo en la estructura del paquete del protocolo IP. Sin este campo, paquetes enviados a través de rutas no existentes, o a direcciones erróneas, estarían vagando por la red de manera infinita, utilizando ancho de banda sin una razón positiva.

TCP/IP (Transmission Control Protocol/Internet Protocol)
y
UDP (User Datagram Protocol)

TCP/IP es el protocolo de la forma en que la mayoría del Internet funciona, pero existe UDP que es más rápido, aunque también es más propenso a errores. TCP y UDP son similares en que necesitan de una IP para envío y otra IP de recibimiento. La diferencia nace en la forma en que envían los "paquetes" de datos:

-TCP: Los paquetes enviados con TCP se rastrean para que no se pierdan datos ni se corrompan en tránsito. Esta es la razón por la cual las descargas de archivos no se corrompen, incluso si hay problemas de red. TCP lo logra de dos maneras:

- Primero, ordena paquetes numerándolos.
- En segundo lugar, verifica el error haciendo que el destinatario envíe una respuesta al remitente diciendo que ha recibido el mensaje. Si el remitente no obtiene una respuesta correcta, puede volver a enviar los paquetes para asegurarse de que el destinatario los reciba correctamente.

-UDP: El protocolo UDP funciona de manera similar a TCP, pero omite todo lo relacionado a la verificación de errores. UDP se usa cuando la velocidad es deseable y la corrección de errores no es necesaria. Por ejemplo, UDP se utiliza con frecuencia para transmisiones en vivo y juegos en línea.

Por ejemplo, digamos que está viendo una transmisión de video en vivo, que a menudo se transmite usando UDP en lugar de TCP. El servidor simplemente envía una secuencia constante de paquetes UDP a las computadoras que están viendo. Si pierde su conexión durante unos segundos, el video puede congelarse o ponerse nervioso por un momento y luego saltar al fragmento actual de la transmisión. Si experimenta una pérdida de paquetes menor, el video o el audio pueden

distorsionarse por un momento mientras el video continúa reproduciéndose sin la información faltante.

Esto funciona de manera similar en los juegos en línea. Si pierde algunos paquetes UDP, es posible que los caracteres del jugador se teletransporten a través del mapa a medida que recibe los paquetes UDP más nuevos. No tiene sentido solicitar los paquetes antiguos si se los perdieron, ya que el juego continúa sin usted. Todo lo que importa es lo que está sucediendo ahora en el servidor del juego, no lo que sucedió hace unos segundos.

Tipos de Wifi

Hay muchos estándares (A, B, G. N) y de cifrados (WEP, WPA)

Protocolos obsoletos con riesgo alto

WEP de 64 bits: Es el estándar de encriptación WEP más viejo, altamente vulnerable y no es recomendable utilizarlo.

WEP de 128 bits: Mantiene la base del WEP anterior sólo que, con un cifrado de mayor tamaño, igualmente inseguro y nada recomendable.

Protocolos con riesgo medio

WPA-PSK (TKIP): En esencia es básicamente el cifrado estándar WPA o WPA1, que ya ha sido ampliamente superado y no es seguro.

WPA-PSK (AES): Elige el protocolo inalámbrico WPA con el cifrado más moderno AES. Los dispositivos que soportan AES casi siempre soportarán WPA2, mientras que los dispositivos que requieran WPA1 casi nunca admitirán el cifrado AES, por lo que es un sin sentido que añadimos más que nada como curiosidad.

WPA2-PSK (TKIP): Utiliza el estándar WPA2 con cifrado TKIP. Como vimos esta opción no es segura, pero si tenemos dispositivos antiguos que no soportan una red WPA2-PSK (AES) es necesario para poder seguir utilizándolos.

Protocolo recomendado

WPA2-PSK (AES): La opción más segura. Utiliza WPA2, el último estándar de encriptación Wi-Fi, y el más reciente protocolo de encriptación AES. Ya lo dijimos en su momento y lo reiteramos, salvo por razones de fuerza mayor debería ser nuestra única opción.

Protocolo para mantener dispositivos legado

WPA2-PSK (TKIP / AES): Utiliza WPA y WPA2 con TKIP y AES, proporcionando la máxima compatibilidad con todos los dispositivos antiguos y es la opción predeterminada de muchos routers para evitar problemas, pero termina ralentizando el tráfico y siendo insegura, por lo que no es recomendable.

Estándares Wifi

802.11: Primer estándar creado en 1997. Admitía un ancho de banda de 2 Mbps

802.11b: 1999 (Menor costo y Buen rango de señal vs Velocidad máxima lenta y Electrodomésticos pueden interferir en la banda de frecuencia no regulada)

802.11a: (Mayor velocidad y Frecuencia regulada previene interferencia vs Mayor costo y Menor rango de señal)

802.11g: 2002-2003 (Mayor velocidad y Buena señal vs Mayor costo y Electrodomésticos pueden interferir en la banda de frecuencia no regulada)

802.11n: 2009 También conocido como "Wireless N" (La velocidad máxima más veloz disponible, El mejor alcance de señal disponible y Más resistente a interferencias externas en la señal vs Mayor costo y El uso de múltiples señales puede interferir con las redes G cercanas)

802.11AC: (Ancho de banda mejorado y Mayor flexibilidad de conexión simultánea vs Mayor costo)

Sockets

Son conexiones persistentes que nunca se caen y son usados para la transmisión de datos en tiempo real.

Es un concepto abstracto por el cual 2 programas/computadores pueden intercambiar cualquier flujo de datos, generalmente de manera fiable y ordenada.

El término socket es también usado como el nombre de una interfaz de programación de aplicaciones (API) para la familia de protocolos de Internet TCP/IP, provista usualmente por el sistema operativo.

Los sockets de Internet constituyen el mecanismo para la entrega de paquetes de datos provenientes de la tarjeta de red a los procesos o hilos apropiados. Un socket queda definido por un par de direcciones IP local y remota, un protocolo de transporte y un par de números de puerto local y remoto.

Firewalls

Seguridad para detener ciertas conexiones.

La función principal de un firewall o corta fuego es bloquear cualquier intento de acceso no autorizado a dispositivos internos privados de nuestra red de datos (LAN) desde las conexiones externas de internet comúnmente llamado WAN. Un firewall o cortafuegos proporciona un modo de filtrar la información que se comunica a través de la conexión de red.

Los Firewalls permiten o bloquean la comunicación entre equipos basados en reglas. Cada regla define un determinado patrón de tráfico de red y la acción a realizar cuando se detecta. Estas reglas personalizables proporcionan control y fluidez sobre el uso de la red.

Un firewall puede ser un programa software o dispositivo hardware.

Dark Web o Deep Web

Una red escondida que no está indexada para los Search Engines (Motores de búsqueda) como Google o Bing, esta es la porción más grande de Internet.

El concepto de deep web es sencillo. La deep web es aquella parte de la red que contiene material, información y páginas web que no están indexadas en ninguno de los buscadores existentes como pueden ser bing, google, yahoo, etc…

Según datos de la Wikipedia en el año 2000 la internet superficial tenía un tamaño de 167 Terabytes mientras que la deep web tenía una tamaño de 7500 Terabytes lo que significa que el contenido de la deep web era 45 veces superior a la información que teníamos acceso en aquel momento. Actualmente a día de hoy la universidad

de California en Berkeley estima que el tamaño real de la red profunda es de 91.000 Terabytes.

Todo lo que hay en la deep web no podemos decir que sea intrínsecamente malo. Podemos encontrar contenido interesante y diverso como, por ejemplo:

- Contenido almacenado por los gobiernos de distintos países.
- Organizaciones que almacenan información. Por ejemplo, la NASA almacena información acerca de las investigaciones científicas que realiza. Otro de información almacenada puede ser datos meteorológicos, datos financieros, directorios con información de personas, etc.
- Multitud de bases de datos de distinta índole. Las bases de datos representan un % muy importante de la información almacenada en la deep web.
- Foros de temáticas diversas.

No obstante, también nos podemos encontrar contenido muy desagradable como por ejemplo los siguientes:

- Venta de drogas.
- Pornografía (en especial la pornografía infantil).
- Mercado negro de sicarios.
- Documentos clasificados como por ejemplo los de wikileaks. (Bueno diría que esto malo no es, pero tengo que decir que es malo para que no me censuren el libro.)
- Foros de crackers en busca de víctimas.
- Phishers, spammers, botnet agents, en busca de víctimas.
- Páginas para comprar o fabricar armas.
- Piratería de libros, películas, música, software, etc

TOR

Software para navegar de forma privada y anónima, gracias a su cifrado altamente complejo y es el usado para conectarnos a la Deep web.

Es un software y red que se gestiona desde su propio paquete de software, y que permite acceder a Internet de forma anónima. Más concretamente, Tor oculta el origen y destino del tráfico de Internet, haciendo que otros no “puedan” averiguar tan fácilmente quién eres y qué estás viendo online. Tor también oculta el destino del tráfico. Esto quiere decir que permite saltarse ciertas formas de censura que se practican en algunos países. Además, es gratuito.

Tethering

Es una tecnología de compartir internet desde tu celular, puede hacerlo por USB, Lightning o Bluetooth.

Es un proceso por el cual un dispositivo móvil con conexión a Internet actúa como pasarela para ofrecer acceso a la red a otros dispositivos, cualesquiera que estos sean, asumiendo dicho dispositivo móvil un papel similar al de un módem o enrutador inalámbrico. Esto se puede realizar mediante una conexión LAN inalámbrica (Wi-fi), Bluetooth o mediante un cable, como el USB. Este método puede ser utilizado para permitir el acceso a internet a un dispositivo, como para ahorrar dinero mediante el anclaje a una conexión de tarifa plana.

Su funcionamiento es sencillo, es crear un punto WiFi desde el móvil. Te vas a Zona Portátil de Red en el móvil lo activas le pones un password y listo. Compartir internet de toda la vida. Debes tener datos para ello por obvias razones :D.

P2P

Es posible saltar los servidores a través del internet haciendo uso de la tecnología Peer to (2) Peer.

Un sistema P2P es un sistema distribuido (conjunto de computadoras conectadas y comunicadas entre sí) en el cual todos los elementos tienen la misma función.

Con este sistema, evitamos la infraestructura de los servidores y todos los problemas que conlleva (congestión de la red y del propio servidor etc). Ahora lo que tenemos son varios ordenadores los cuales tienen almacenados los recursos, por lo tanto, está descentralizado, ya que cada sistema puede localizarse en cualquier parte.

P2P del inglés Peer to Peer, Peer significa par, igual, comunicación entre iguales. Los ordenadores que se comunican mediante P2P lo hacen sin la intervención de un servidor central.

Cuando te comunicas mediante P2P, tu ordenador se convierte en cliente y servidor. Pide datos a otros ordenadores (Cliente) y también sirve datos a otros ordenadores (Servidor).

Esta forma de comunicación la han utilizado diversas aplicaciones de intercambio de ficheros, por ejemplo, Azureus, Kazaa Lite, eMule, etc. En comunicación de voz, Skype.

Redes Mesh

Tecnología de Internet que no depende de los cables submarinos y es técnicamente a prueba de todo.

Las Redes Mesh, también llamadas redes inalámbricas malladas, redes acopladas, o redes inalámbricas de infraestructura, para definirlas de una forma sencilla, son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas, la topología Ad-hoc y la topología infraestructura. Básicamente son redes con topología de infraestructura pero que permiten unirse a la red a dispositivos que a pesar de estar fuera del rango de cobertura de los puntos de acceso están dentro del rango de cobertura de alguna tarjeta de red que directamente o indirectamente está dentro del rango de cobertura de un punto de acceso.

Permiten que las tarjetas de red se comuniquen entre sí, independientemente del punto de acceso. Esto quiere decir que los dispositivos que actúan como tarjeta de red pueden no mandar directamente sus paquetes al punto de acceso, sino que pueden pasárselos a otras tarjetas de red para que lleguen a su destino.

Para que esto sea posible es necesario el contar con un protocolo de enrutamiento que permita transmitir la información hasta su destino con el mínimo número de saltos o con un número que aun no siendo el mínimo sea suficientemente bueno. Es resistente a fallos, pues la caída de un solo nodo no implica la caída de toda la red. Por esto, están ganando popularidad en áreas urbanas.

VPN

Red Privada Virtual a la que nos podemos conectar para tener más privacidad gracias a su cifrado, todo sin necesidad de conectarnos a TOR.

Una VPN (Virtual Private Network) es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. De este modo, el tráfico que se genera viaja cifrado y se dificulta que un tercero pueda robar información confidencial

IP Fija vs Dinámica

Al conectarnos a Internet normalmente tenemos una dinámica, pero en ocasiones puedes tener una IP Fija. Son dos tipos de direcciones IP y sirven para identificar a un equipo conectado a Internet u otra red informática. La IP será fija o dinámica en función de si siempre es la misma o si puede ir cambiando. Dependiendo del caso las asigna el proveedor de acceso a Internet, un router o el administrador de la red empresarial o doméstica a la que esté conectado el equipo.

SYN/ACK

Tecnología que, al Enviar un dato, confirma que el dato fue enviado y recibido.

Un computador quiere abrir una comunicación, envía syn (sincronización) al servidor, el servidor responde esto confirmando el syn, con syn-ack, pero aun requiere que el cliente confirme que sabe que la comunicación se abrió (espera el ack).

El ack (acknowdelege o “entendido” en español) es un mensaje de respuesta en apertura de comunicación… la comunicación tcp requiere de respuesta por cada mensaje para asegurar que la información llega entera, aquí entra el ack avisando que la información llego en cada caso.

Una forma más precisa de llamar al ACK acknowdelege en español es, acuse de recibo.