

BIBLIOTECA POPULAR DE CULTURA LIBRE

COMPUTADORAS Y REDES LAN



LABORATORIO POPULAR
DE MEDIOS LIBRES
PRESENTA:

BIBLIOTECA POPULAR DE CULTURA LIBRE

COMPUTADORAS Y REDES LAN

Computadoras y Redes Lan

Laboratorio Popular de Medios Libres
Biblioteca Popular de Cultura Libre
2023

Foto de Portada exterior

San Francisco Xochiteopan, Puebla, México.

Foto de Portada interior

Centro de Datos Yanapak.org

Diseño y Diagramación

Chasqui Camilo

Arte y Gráfica

Luna (Portada y contraportada Interior)
animalesdeabajo@gmail.com

Indiosindios. (Linograbado)
indiosindios@gmail.com

laboratoriodemedios.org
contacto@yanapak.org

primera edición



Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

INDICE

- a. Saludo a la lectora (pág. 4)
- b. ¿Qué es una computadora? (pág. 5)
- c. Hardware (pág. 7)
- d. Software (pág. 11)
- e. Software Libre (pág. 13)
- f. Código Binario (pág. 16)
- g. Red de Computadoras (pág. 23)
- h. Equipos de Red (pág. 41)
- i. ¿Cómo funciona una red? (pág. 45)
- j. Red WAN (pág. 52)
- k. Recapitulemos (pág. 56)
- l. Lectura Complementaria (pág. 58)







LABORATORIO
POPULAR
DE MEDIOS
LIBRES


A. SALUDO A LA LECTORA

El texto que ahora sostienes en tus manos es el fruto de la sistematización del trabajo, experiencias y conocimientos que otras han compartido con nosotras, desde que decidimos iniciar la promoción (hace algunos años ya) de la autonomía técnica en las distintas comunidades que utilizan la comunicación como una herramienta para la defensa del territorio.

En este recorrido no nos hemos encontrado con la academia, si no por el contrario nuestra escuela ha sido el conocimiento popular que vive en la boca, mente y corazón de cada una de las valientes que se han decidido a mantener un proyecto de comunicación autónoma. Esa sabiduría es la que humildemente intentamos plasmar en el texto en que se zambullirán en unos momentos.

Queremos agradecer a la comunidad de San Francisco Xochiteopan, en el estado de Puebla y a sus vecinas y vecinos que con mucha paciencia nos abrieron sus puertas y techos para soñar con una red autónoma. Los conocimientos aquí vertidos fueron diseñados inicialmente para la escuela de capacitación en la comunidad, que posteriormente dio vida al primer sistema comunitario de internet en México con la capacidad de auto-sostenerse económicamente. Mucho de lo aprendido en ese proceso sirvió para mejorar este texto.

Ante la creciente centralización, privatización y uso no consentido de nuestra data personal en Internet, creemos fundamental comenzar a cuestionarnos la propiedad de las plataformas e infraestructuras que actualmente sostienen nuestras comunicaciones digitales y, para ello ponemos a disposición en un lenguaje sencillo, los conocimientos que hemos podido compilar con respecto a las **redes de computadoras** en este segundo cuadernillo de la *Biblioteca Popular de Cultura Libre*.

Encontrarás a lo largo de este viaje algunos códigos QR , asegúrate de tener contigo un celular con una app que te permita leerlos, ya que te llevarán varias profundas e interesantes informaciones adicionales.

También te encontrarás con este símbolo , este quiere decir que existe un comando en la terminal de linux (bash) que podrás ejecutar siempre y cuando tengas un sistema operativo GNU/Linux en tu computadora

Esperamos que sea de tu agrado y por favor tómate la libertad de subrayar, dibujar o escribir sobre este cuadernillo. Abrazos.

No odies a los medios, siémbrales libres

B. ¿QUÉ ES UNA COMPUTADORA?

Una computadora es una herramienta que nos permite realizar múltiples tareas, como elaborar cartas o una hoja de vida, hablar con personas a distancia, trabajar, estudiar y hasta ver videos o tomar fotografías. Para ello una computadora todo lo transforma en **dos dígitos**, el 1 y el 0, por ello hablamos de tecnología **digital**.

Gracias al avance del microchip cada vez es posible construir computadoras más y más pequeñas. Hoy en día podemos encontrar una en nuestra vida cotidiana de una manera abismante. La televisión, el celular, el coche, el refrigerador, el reloj y un largo etcétera son o contienen una computadora.

La parte que puedes ver y tocar de estos dispositivos es llamada **hardware**. Es decir, todos los componentes de su estructura física como pantallas y teclados.

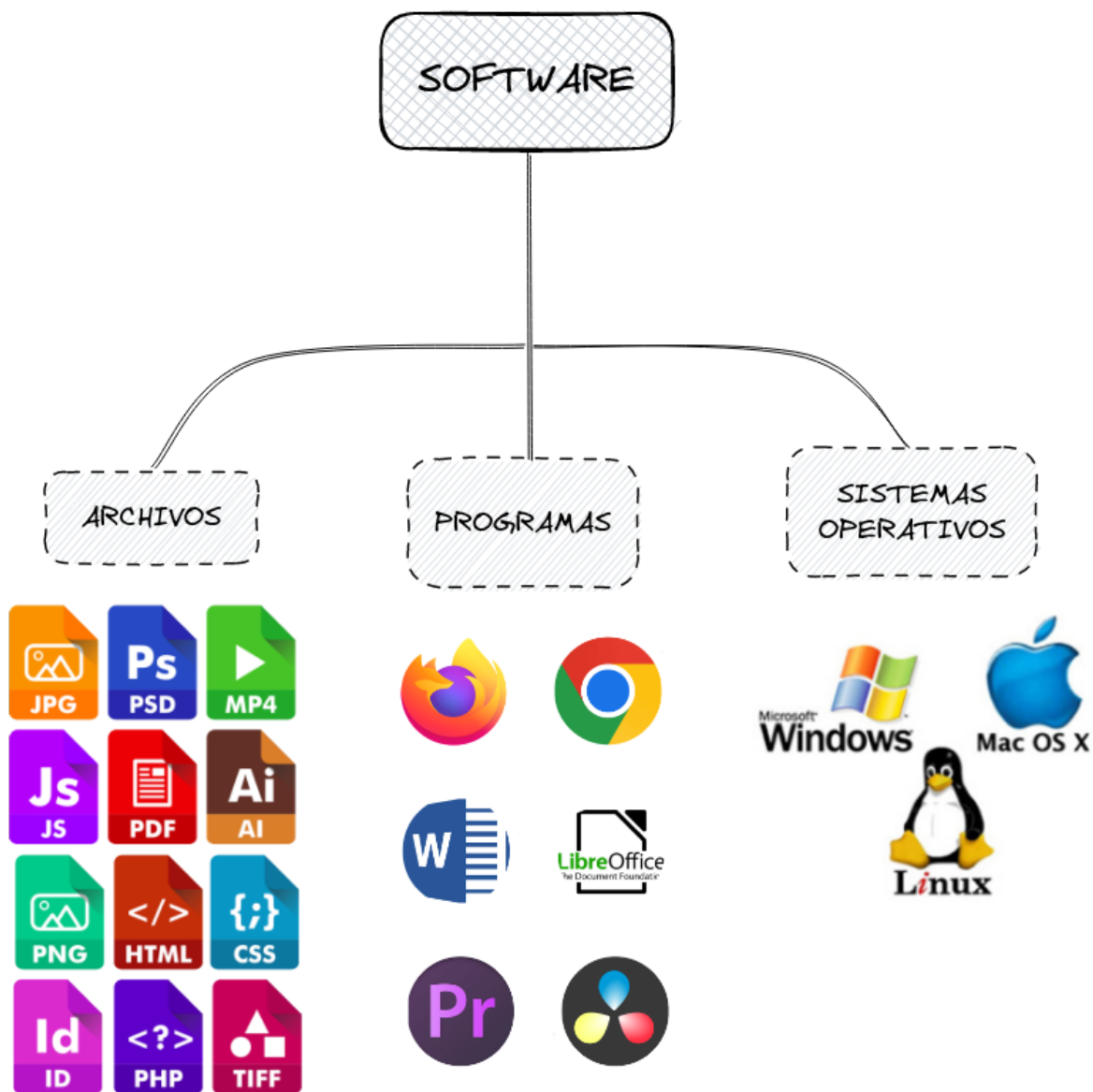


¿QUÉ ES LA INFORMÁTICA?

Rama de la ciencia que se encarga de estudiar la administración de métodos, técnicas y procesos con el fin de almacenar, procesar y transmitir información y datos en formato digital

El **software** es el código de programación que hace posible la ejecución de tareas dentro de una computadora. Es todo lo que está escrito en lenguaje de computadoras (lenguaje digital o binario) y por lo tanto no es "algo" físico que podamos tocar, como el hardware, sino mas bien un conjunto de informaciones e instrucciones..

Por ejemplo, los sistemas operativos, aplicaciones, programas, o los archivos como canciones, películas o un libro en PDF son software.



SOFTWARE Y HARDWARE

Este video explicativo aborda de manera muy amena lo qué son y en qué se diferencian estas dos características

El **software** y el **hardware** siempre trabajan de la mano. Mientras el software aporta las operaciones e instrucciones, el hardware es el canal físico por el cual dichas operaciones e instrucciones suceden.

C. HARDWARE

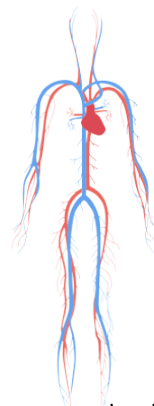
Una computadora es muy parecida a una persona. Por ello podemos analizar las partes de una computadora como si fueran las partes de un ser humano.

TARJETA MADRE → **ESQUELETO**



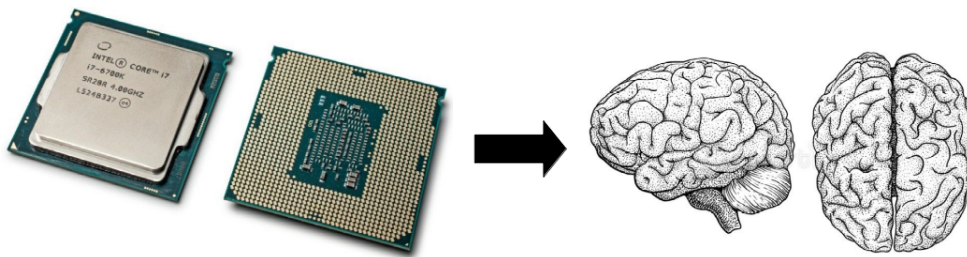
La tarjeta madre es donde se colocan las piezas de una computadora para que se conecten y comuniquen entre ellas. Es como nuestro esqueleto, porque sostiene a los órganos del cuerpo, como la tarjeta madre sostiene los componentes de una computadora.

FUENTE DE PODER → **CORAZÓN Y SISTEMA CIRCULATORIO**



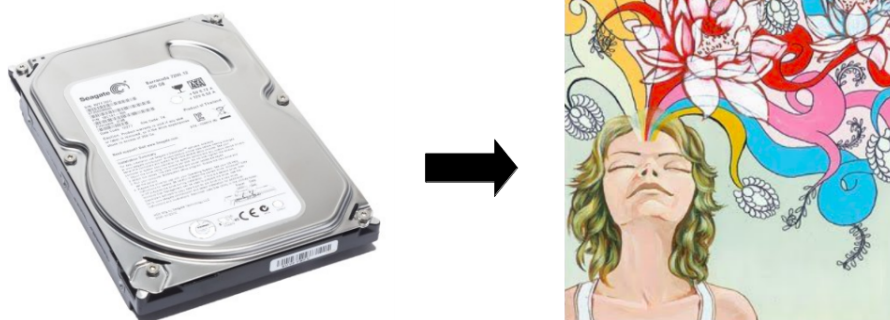
La fuente de poder es la encargada de la tomar electricidad y distribuirla en el voltaje adecuado a las distintas piezas de una computadora. Es cómo nuestro sistema circulatorio que entrega sangre a los distintos órganos de nuestro cuerpo para que éstos funcionen.

PROCESADOR → CEREBRO



El CPU (Central Processing Unit) es el componente encargado de la ejecución de las instrucciones de los programas. Es cómo nuestro cerebro y su capacidad de procesar información.

DISCO DURO → MEMORIA



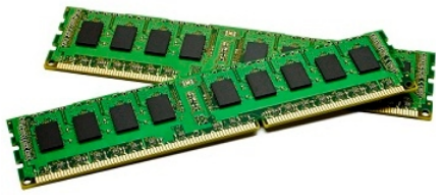
El disco duro es el lugar físico donde se almacena la información de una computadora. Es como nuestra capacidad de recordar, es decir nuestra memoria. Una computadora puede tener uno o varios discos duros.

PARTES DE UNA COMPUTADORA

Para obtener más información puedes escanear o dar clic en el siguiente código QR.



MEMORIA RAM → CAPACIDAD DE HACER VARIAS COSAS A LA VEZ



Las memorias RAM (Random Access Memory) almacenan de forma temporal los datos de los programas que estás utilizando en ese momento; mientras más programas uses más memoria RAM necesitarás. La memoria RAM es cómo nuestra capacidad de hacer varias cosas a la vez, por ejemplo un músico baterista tiene “mucho memoria RAM” porque es capaz de llevar un ritmo distinto con cada extremidad de su cuerpo.

¿QUIÉN INVENTÓ LA COMPUTADORA?

Lejos de ser un invento de una persona en particular, la computadora es el resultado evolutivo de ideas de muchas personas relacionadas con áreas tales como la electrónica, la mecánica, los materiales semiconductores, la lógica, el álgebra y la programación.

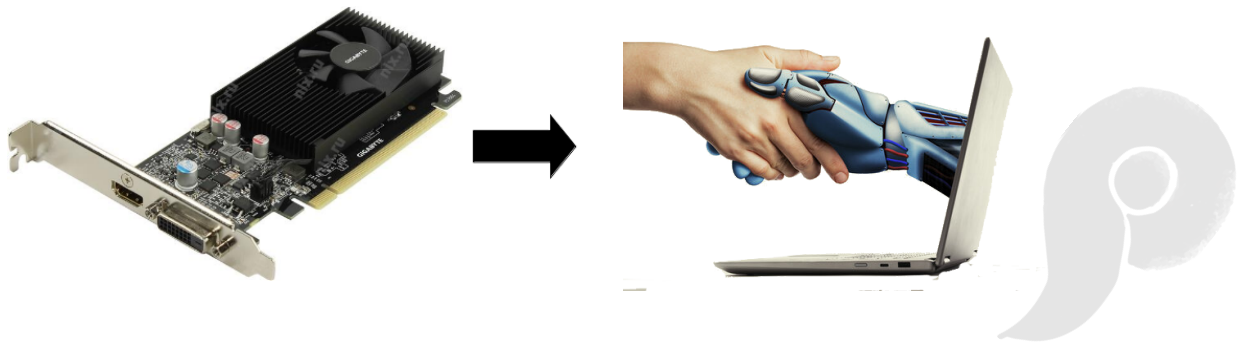


TARJETA DE RED → OÍDOS Y BOCA



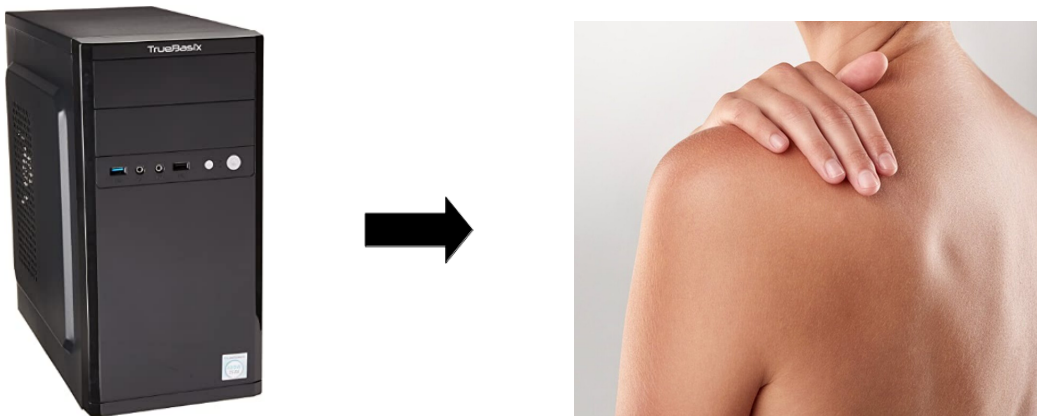
La tarjeta de red es la encargada de comunicar una computadora con otra mediante código binario (lenguaje de computadora). La tarjeta de red puede ser cableada (ethernet) o inalámbrica (wi-fi). Vendría siendo como nuestra capacidad de hablar y escuchar a otras personas.

TARJETAS DE AUDIO Y VIDEO → MANOS



Las tarjetas de video y audio son las encargadas de establecer un puente de comunicación entre una computadora y un humano, ya que permite desplegar en imagen y sonido la información binaria de la computadora. Es la forma que tienen las computadoras de interactuar con el mundo humano, al igual que nuestras manos que nos permiten tocar e interactuar con el mundo físico.

GABINETE → PIEL



El gabinete aloja y mantiene protegido de la intemperie a los dispositivos que componen una computadora. Es nuestra piel, o para algunos más creativos una verdadera “armadura”.

CONOCE TU HARDWARE

Escribe en tu terminal **sudo lshw -short** para obtener información breve y detallada sobre múltiples unidades de hardware en Linux, como CPU, memoria, disco, controladores usb, adaptadores de red, etc.



D. SOFTWARE

Software es el conjunto de programas, aplicaciones, archivos o reglas informáticas que hacen posible el funcionamiento de la computadora. Es todo lo que está escrito en lenguaje de computadoras.

Del inglés:

Soft = blando/a

Ware = herramienta

ARCHIVOS → INFORMACIÓN

Los archivos son información escrita en lenguaje de computadora (código binario), éstos pueden ser fotos, música, descargas de internet o un documento de texto u hoja de cálculo.



Cada archivo se diferencia del resto debido a que tiene un nombre propio (**carta_final.doc**) y una extensión que lo identifica (**carta_final.doc**)

Esta extensión sería como el apellido y es lo que permite diferenciar el formato del archivo y con ello el programa que es capaz de leer ese archivo.

Imaginemos una receta de la abuela que tenemos anotada en un libro, esa receta es un archivo. Es una información útil si contamos con la aplicación o programa adecuado para ejecutarla.

APLICACIONES → SABERES Y HABILIDADES

Las aplicaciones o programas son un tipo de software de computadora diseñado para realizar tareas o actividades específicas. Si necesito escribir una carta en una computadora, le instalo una aplicación procesador de texto. Para una persona son como las cosas que sabe hacer. Por ejemplo, si sé cocinar, es que “tengo instalado” una aplicación de cocina. O, si no sé malabarismo, puedo tomar unas clases y aprender o “instalar” en mi cerebro esa habilidad nueva.



SISTEMA OPERATIVO → PERSONALIDAD

El sistema operativo (SO) es el software que administra y coordina el hardware y el software que utilizamos y de él dependerá en gran medida como se comporte una computadora. Cuando encendemos un equipo, lo que se despliega (comúnmente conocido como escritorio) es el Sistema Operativo, sin él la computadora es inútil.

Existen tres familias de SO: Windows, MacOS y Linux. Windows y MacOS son desarrollos de empresas privadas, mientras que Linux es Código Abierto (Software Libre). El Sistema operativo es como la personalidad de una persona, son las cualidades y características visibles que distinguen a una persona de otra, es decir es el estilo y el sello personal.



E. SOFTWARE LIBRE

SOFTWARE PERO... ¿ABIERTO O CERRADO?

Existen esencialmente dos tipos de software, el software de código cerrado o privativo y el software de código abierto o libre

El software privativo es desarrollado y mantenido por empresas privadas con un interés comercial o militar. Su código es distribuido con licencia de uso y no puede ser inspeccionado, modificado o adaptado por el usuario, como sucede con IOS y Windows.

El software libre es desarrollado y mantenido por la sociedad civil, instituciones educativas o sin fines de lucro. Su código puede ser inspeccionado, modificado o adaptado por el usuario y se distribuye gratuitamente. Un claro ejemplo son Android y Linux

Texto original de **COMPPA**. Sembrando Voces: Manual Teórico Avanzado, revísalo completo en el código QR



Cuando hablamos de **software** nos referimos a los programas informáticos que usa una computadora para realizar tareas. Estos programas son como una lista de instrucciones que alguien escribió. Windows o Ubuntu son nombres que probablemente ya hemos escuchado, estos, son sistemas operativos que usa una computadora para que puedan funcionar otros programas. Hay empresas que venden sistemas operativos para su beneficio económico, al mismo tiempo que existen gobiernos y agencias de seguridad estatal que los usan para aumentar el control o la vigilancia de su población.

Y nosotrxs ayudamos en esto. Cuando usamos los servicios y aplicaciones de estas empresas damos permisos para que usen nuestros datos. Al igual que la tierra, el **software** es un bien que puede estar en manos privadas o ser parte de una comunidad. Las grandes compañías tecnológicas como Apple o Microsoft venden programas que sólo ellas y sus programadores controlan, no se pueden copiar o usar sin su permiso. Este software y su desarrollo está en manos privadas y la llamamos software **privativo**.

“Cuando compramos un programa informático (o nos copiamos uno y lo usamos sin haber pagado), la empresa sólo nos entrega el programa que viene a ser como un plato de comida ya preparado, pero no nos entrega la lista de ingredientes ni la receta y no podemos ver cómo se “preparó” ese programa”.

Milpa digital #12. El software libre.

LAS 4 LIBERTADES

El programador estadounidense Richard Stallman elaboró en 1983 las cuatro libertades del software libre. Estas cuatro libertades aseguran que un programa informático es libre cuando existe:

- La libertad de instalar y usar el programa cómo y dónde queramos.**
- La libertad de tener acceso al código fuente, estudiar cómo funciona el programa y cambiarlo para que haga lo que queramos.**
- La libertad de redistribuir copias para ayudar a otrxs.**
- La libertad de modificar el programa y distribuir copias de estas versiones modificadas**

A su vez surgió el proyecto GNU/Linux para desarrollar un sistema operativo completo que se puede instalar de manera gratuita en cualquier computadora y que se mantiene y desarrolla a través del trabajo colaborativo de sus usuarixs. La declaración de las cuatro libertades potenció un movimiento social que actualmente se conoce como software libre y que defiende estas libertades. La posibilidad de usar computadoras con software o programas libres facilita el acceso a los conocimientos y reduce la llamada brecha tecnológica.



Hoy en día existen un sin fin de programas libres, entre otros para escribir y difundir textos; para editar fotografías, audio y vídeo o para transmitir audio por Internet. Estos programas no son propiedad privada, tienen derechos comunes y colectivos y son compartidos de manera gratuita.

EVALÚA LAS DIFERENCIAS ENTRE PRIVATIVO Y LIBRE

Existen tres puntos claves que diferencian estos dos tipos de software:

EL COSTO

Para usar una licencia de software de fuente cerrada generalmente debes pagar, mientras que los software de fuente abierta son distribuidos de forma pública y gratuita.



EL SOPORTE

Los software de código cerrado, por lo general, te ofrecen soporte técnico y actualizaciones durante el tiempo de vida del producto a un costo económico.



Para usar una licencia de software de fuente cerrada generalmente debes pagar, mientras que los software de fuente abierta son distribuidos de forma pública y gratuita. Cada desarrollo de software libre posee un espacio en internet (foro) donde sus creadoras y usuarias comparten sus experiencias que brindan la guía necesaria para que demos solución a problemas que se puedan presentar.

LA SEGURIDAD

Cuando utilizamos software privativo, quedamos a merced de la empresa con fines comerciales que ha creado ese código, ya que no podemos revisarlo y saber con certeza qué es lo que hace el programa con la información que ponemos en él. Sabemos que el software hace algo, pero no sabemos todo lo que hace.



El software abierto es creado con la finalidad de brindar una contribución a la humanidad, y este sí puede ser inspeccionado por los usuarios y otras desarrolladoras, quienes tienen la capacidad de modificar cualquier característica no deseada de un programa.

F. CÓDIGO BINARIO

¿CÓMO SE COMUNICAN LAS COMPUTADORAS?

El sistema de numeración decimal ha sido usado por muchas civilizaciones a lo largo del tiempo y se compone por diez dígitos que van del 0 al 9, con los cuales formamos cifras. Sin embargo las computadoras utilizan el sistema binario, es decir con solo dos dígitos, el 0 y el 1.

Para una computadora, que básicamente trabaja con impulsos eléctricos, es mucho más fácil procesar dos estados, encendido y apagado. La unidad básica del lenguaje binario es el BIT.

0 = 1 BIT

1 = 1 BIT

Esto puede formar un código simple, donde podemos representar solo dos opciones, por ejemplo

si - no
avanza - retrocede
arriba - abajo

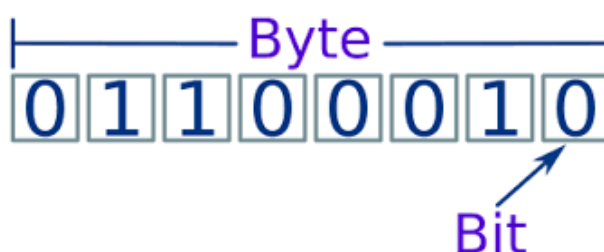
¿QUÉ ES UN BYTE?

Para tener más opciones que encendido - apagado, si - no, avanzar - detenerse, en el lenguaje binario, se utilizan los BYTES, que es una combinación de 64 unos y ceros (64 bit), formando un código o "palabra".

0101001011010100010101010010100100001110010001111001010101010011 = **1 BYTE**

Como dijimos, un BYTE es como una palabra del lenguaje binario. Tu computador rápidamente procesa este lenguaje de 18.446.744.073.709.551.616 palabras y lo transforma en instrucciones que le indican qué hacer.

Los BYTES determina el tamaño de nuestros archivos. Entre más información tenga un archivo, más BYTES posee. Por ejemplo, un video de alta resolución está conformado por millones de unos y ceros.



01101100

01101111

01110110

01100101

El **código binario** representa la información utilizando exclusivamente dos dígitos diferentes, 0 y 1.

Todas las computadoras, ya sean PC, smartphones, tablets o calculadoras, dependen del código binario para funcionar.

32 y 64 BIT

Actualmente es común encontrarnos con computadoras de 32 y 64 Bit, ¿qué quieres decir esto? Pues a medida que han avanzado la tecnología de los procesadores (cerebros) de computadora, también la capacidad de procesar código binario más complejo y a mayor velocidad.

Las nomenclaturas de 32 y 64 bits se refieren a cómo se almacenan los datos. Como su nombre sugiere, los sistemas de 32 bits almacenan sus datos en piezas (o "palabras") de 32 bits, mientras que los otros lo hacen con piezas de 64. Esto puede decir que, por lo general, al trabajar con "palabras" más grandes puedes hacer más en menos tiempo.

El que la CPU de tu ordenador tenga 32 o 64 bits depende de algunos aspectos, siendo el principal de ellos la edad. Prácticamente todos los ordenadores que te llevas pudiendo comprar en la última década tienen casi seguro una arquitectura de 64 bits. Pero todavía hay personas e instituciones con equipos muy antiguos de 32 bits, o sea que tanto los sistemas operativos como los desarrolladores de software siguen dándole soporte.

MAS INFORMACIÓN

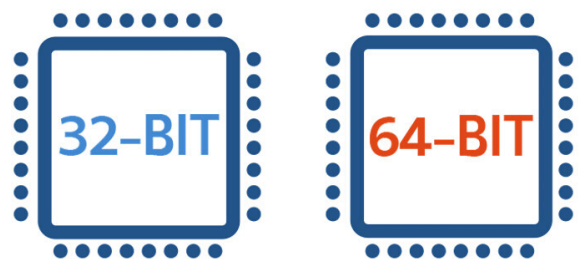
Aquí puedes encontrar más información sobre la arquitectura de un PC



La principal diferencia entre ambas arquitecturas es que los procesadores de 32 bits no son capaces de gestionar tanta memoria RAM como los de 64. Tengas en tu ordenador 8 o 16 GB de RAM, un sistema operativo de 32 bits sólo puede aprovechar un máximo de 4 GB. Los de 64 bits pueden utilizar muchísima más, teóricamente hasta 16 Exabytes, unos 16 millones de Terabytes.

Aún así de momento estamos lejos de que haya ordenadores domésticos capaces de montar tanta RAM, y desde luego los sistemas operativos tampoco llegan a esas cantidades en sus topes.

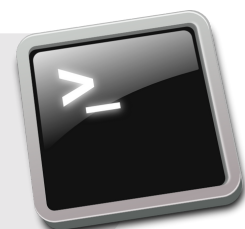
También es importante saber que aunque una CPU de 64 bits puede utilizar un sistema operativo de 32 o 64 bits, las CPU de 32 bits sólo pueden utilizar los de su arquitectura. Eso sí, si en una CPU de 64 bits instalamos un sistema operativo de 32, no podremos utilizar aplicaciones de 64.



¿CÓMO AVERIGUO QUÉ ARQUITECTURA TIENE MI PC?

Escríbe en tu terminal linux:

`lscpu` y aparecerá en el apartado de "Arquitectura"



BYTES EN INFORMACIÓN

¿Pero cómo los bytes se transforman en una fotografía o en un video?... Cuando nos acercamos más y más a una fotografía **digital**, comenzamos a ver que la fotografía va perdiendo resolución y finalmente podemos notar que la imagen está construida a partir de pequeños cuadrados de un color cada uno. Cada uno de los colores conocidos tiene su representación en un BYTE. Una fotografía **con mejor resolución tiene mayor cantidad de píxeles**, es decir utiliza mayor cantidad de BYTES, de aquí que se diga que su "peso" es mayor, ya que la cantidad de BYTES determina el tamaño del archivo, en este caso, de la fotografía digital.



Una fotografía digital en internet puede pesar entre 500 kilobytes y 1,5 Megabytes, para ser transferidas rápidamente. Un archivo de cámara de foto RAW puede llegar a pesar hasta más de 100 Megabytes por fotografía.

De esta manera podemos entender cómo una fotografía es finalmente traducida a un código de unos y ceros que una computadora sí puede entender. A una fotografía construida a partir de ceros y unos se le llama fotografía digital, ya que está hecha a partir de dos dígitos numerales (0-1).

Actualmente muchas cosas tienen su versión en digital. Por ejemplo cuando se habla de la TV o Radio digital, lo que quiere decir que el audio o imágenes que viajan por el aire desde la estación al receptor en casa son ceros y unos, es decir información binaria o digital. Cualquier tipo de información traducida a unos y ceros se le llama información digital (por los dígitos 0 y 1) o información binaria (por ser un código de 2 dígitos)

No existe una única forma de traducir cosas en información binaria, el conjunto de reglas que determinan como se usan los BYTES para transformarlos en una imagen, sonido o en una letra, es lo que conocemos como **lenguajes de programación**, existen muchos, y es muy probable que se inventen nuevos. Un lenguaje de computadora es exactamente eso, un idioma o lenguaje construido a partir de el código binario que utilizan las computadoras.

01101111
01110110
01100101

LENGUAJE DE PROGRAMACIÓN

A grandes rasgos, un lenguaje de programación se conforma de una serie de reglas de sintaxis que definen la estructura principal del significado de los Bytes

MEDIDAS DE TAMAÑO Y PESO

Cuando trabajamos con computadoras e internet una variable siempre presentes son los kilobytes, los megabytes y más actualmente los gigabytes. Los utilizamos para medir el tamaño de disco duro, el peso de una película o la velocidad de internet. Pero ¿A qué hacen referencia estos nombres? Ya sabemos qué es un BIT y un BYTE... ¿se imaginan qué es una MegaByte?

Sabemos que las computadoras procesan una cantidad impresionante de información en un brevísimo lapso de tiempo en comparación con el ser humano. La cantidad de BYTES o palabras digitales que puede procesar una computadora en 1 segundo es un número muy elevado; fácilmente por sobre los cien, mil, un millón o un trillón de BYTES, entonces para simplificarnos la manera de nombrar esas cantidades de información digital, es que usamos un sistema de abreviación que va de esta manera:

Mil Bytes = 1 kilobyte
1 millón de Bytes = 1 megabyte
1 billón de Bytes = 1 gigabyte
1 trillón de Bytes = 1 terabyte

También hacemos esto cuando vamos por las tortillas o el pan, porque no pedimos mil gramos de pan, sino que pedimos 1 **kilogramo** de pan o tortillas... aunque en realidad decimos "1 kilo de pan o tortillas"



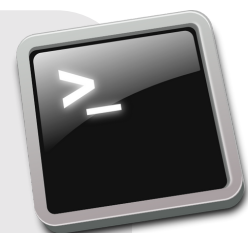
Mil gramos = 1 kilogramo
Mil kilogramos = 1 Tonelada



¿CÓMO AVERIGUO CUANTO PUEDEN ALMACENAR LOS DISCOS DUROS DE MI PC?

Escríbe en tu terminal linux:

df -h y aparecerán tus discos, su tamaño y detalles



Actualmente estamos viendo en el mercado discos duros externos con un tamaño de 4 TeraBytes, esto quiere decir que en ese hardware caben aproximadamente 4 trillones de BYTES en número esto es: 4000.000.000.000 bytes o cuatro mil millones de millones de BYTES... osea muchísimos BYTES. En este caso, con los bytes hemos medido la cantidad de información que puede almacenar un disco duro.

Hay muchas variables en el mundo de las computadoras que utilizan los BYTES y sus múltiplos para medir o cuantificar. Ya vimos que podemos medir el tamaño de un archivo o la capacidad de almacenamiento de un disco duro, pero también los usamos para medir la velocidad de conexión a internet... veamos.

¿QUÉ ES LA VELOCIDAD DE CONEXIÓN?

Es la cantidad de **bytes que podemos enviar y recibir en una comunicación digital durante el lapso de 1 segundo**. Por ello, la velocidad de conexión la podemos medir en bytes por segundo, o bps o también b/s. Por supuesto esta medida es realmente pequeña, y normalmente utilizamos, desde el punto de vista de las redes, los Kilobytes (Kbps) o Megabytes (Mbps), y con más frecuencia los Gigabytes (Gbps).

La velocidad de conexión también podremos expresarla como ancho de banda digital, ancho de banda de red o ancho de banda disponible, todos ellos significan lo mismo, y siempre se transmiten bytes. Si puedo enviar en un segundo 10 Megabyts de datos en una conexión entre dos ordenadores, por ejemplo, significará que tengo un ancho de anda de 10 Mbps.

COMPRUEBA TUS VELOCIDAD DE SUBIDA Y BAJADA

Escanea el siguiente código QR



COMPRUEBA TU VELOCIDAD DE BAJADA RÁPIDAMENTE

Escanea el siguiente código QR

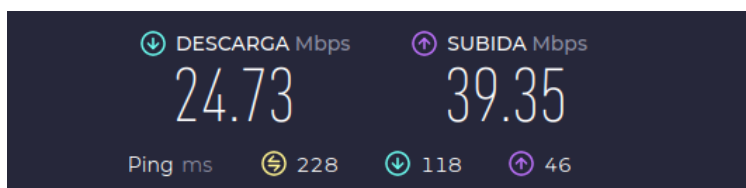


CONEXIONES SIMÉTRICAS y ASIMÉTRICAS

¿Habías escuchado alguna vez este tipo de términos para referirnos a una conexión a internet? Una conexión simétrica es la que tiene capacidad de enviar y recibir información a la misma velocidad sin afectar a la calidad de la conexión. Tanto la descarga como la subida de datos se realizan a la misma velocidad, sin interferir entre ellas.

Muchos servicios de internet ofrecen conexiones asimétricas, lo cual permite una gran capacidad de descarga de datos pero la velocidad de subida es mucho más limitada. Por ejemplo, si tienes contratado un servicio de internet de 20 Mbps, es más que probable que ese dato sólo se refiera a la velocidad de descarga y que **apenas un 10% de esa velocidad esté destinada a la subida de datos.**

Las conexiones asimétricas son las más tradicionales porque la actividad de los usuarios normalmente se centra en la descarga de datos. Un usuario particular, por regla general, consume mucha más información de la que produce y sube a internet.



si vas a transmitir en vivo o subir grandes archivos de video, es importante que tengas una conexión con la mayor velocidad de subida o upload posible

Una conexión a internet simétrica es aconsejable para la mayoría de empresas y profesionales o particulares que se dediquen a la creación de contenidos. Si subes vídeos a YouTube u otras plataformas, si emites en streaming, si necesitas una buena calidad de video para conferencias o en definitiva si envías o intercambias un gran volumen de información a través de internet, siempre será más recomendable la conexión simétrica.

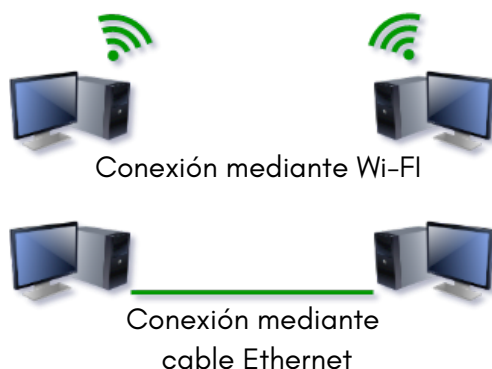
Con esto llegamos a una conclusión muy sencilla, si te identificas como un usuario 'productor' necesitas una buena velocidad de subida de datos, para transferir archivos pesados (por ejemplo videos en alta calidad) lo más conveniente **es una conexión a internet simétrica.**

G. RED DE COMPUTADORAS

Ya hemos revisado las partes y conceptos básicos de una computadora. Conocimos que es el hardware y qué es el software, también vimos la diferencia entre software libre y privativo. Por otro lado nos internamos en el misterio del código binario o lenguaje digital, que no es más que un idioma de computadoras conformado únicamente de unos y ceros. Ahora, lo que prosigue es entender cómo es que se comunican las computadoras entre sí, es decir, cómo funcionan las redes de computadoras. El internet es la gran red de redes, pero para comprender qué es internet, vamos primero a lo más básico y simple.

Una red de computadoras son dos o más computadoras dialogando entre sí. Para poder comunicarse, las computadoras necesariamente deben estar conectadas entre ellas de alguna forma, para esto se utilizan las tarjetas de red. Las tarjetas de red son las encargadas de enviar y recibir paquetes

con datos digitales a través de un medio físico, algunas realizan esta conexión a través del cable Ethernet, y otras de manera inalámbrica mediante radiofrecuencia y el protocolo Wi-Fi.



TARJETA DE RED

La tarjeta de red, también conocida como placa de red, o adaptador de red, es un componente de hardware que conecta una computadora a una red informática y que posibilita compartir recursos (como archivos, discos duros, impresoras e internet).

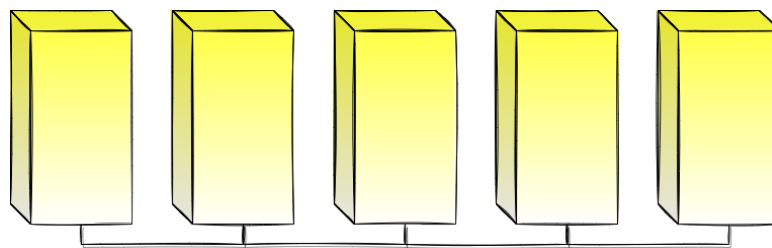
Entonces una red informática está compuesta por equipos que están conectados entre sí mediante líneas de comunicación (cables de red, wi-fi, etc.) y elementos de hardware (tarjetas de red que garantizan que los datos digitales viajen correctamente).

TOPOLOGÍA FÍSICA DE LA RED

Llamamos topología física de red a la disposición de cómo están conectados los dispositivos unos con otros mediante cables o señales inalámbricas. En palabras simples, la topología de red es el mapa de cómo están conectados los dispositivos unos con otros. Claramente las redes pueden tomar muchas formas diferentes dependiendo de cómo están interconectados los dispositivos, pero aquí solo revisaremos las más comunes:

TOPOLOGÍA DE BUS

La topología de bus es la manera más simple en la que se puede organizar una red. En la topología de bus, todos los equipos están conectados a la misma línea de transmisión mediante un cable común o compartido. La palabra "bus" hace referencia a la línea física que une todos los equipos de la red:



La ventaja de esta topología es su facilidad de implementación y funcionamiento. Sin embargo, esta topología es altamente vulnerable, ya que si una de las conexiones es defectuosa, esto afecta a toda la red.

CABLE ETHERNET

Un cable Ethernet es el tipo más común de cable de red utilizado. La conexión por cable proporciona un rendimiento de red más rápido y estable en comparación con la tecnología inalámbrica. Sin embargo, un cable Ethernet sólo puede extenderse a 100 metros.



WI-FI

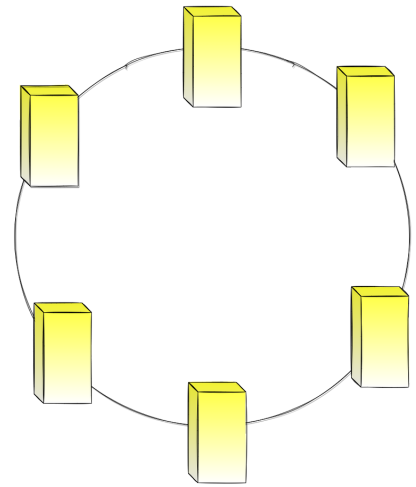
Es una tecnología de transmisión de datos inalámbrica utilizada principalmente para Internet y que se basa en el estándar 802.11. Actualmente es la tecnología estándar para todas las tarjetas de red inalámbricas



TOPOLOGÍA DE ANILLO

Todos los nodos se conectan entre sí formando un lazo cerrado, de manera que cada nodo se conecta directamente a otros dos dispositivos. Este tipo de topología implica que cada dispositivo cuente con dos tarjetas de red, una para cada dispositivo vecino.

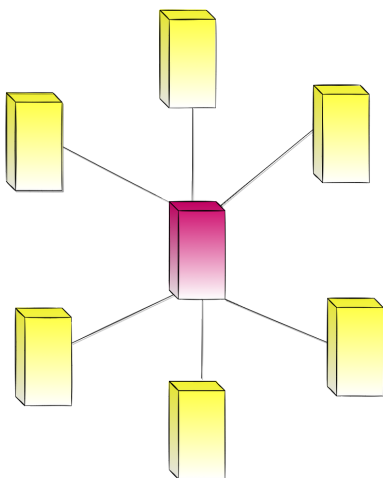
Con esta disposición los datos pasan a través de los dispositivos en ambas direcciones, lo que le permite a la red cierta tolerancia a fallos en caso de que un dispositivo falle.



TOPOLOGÍA DE ESTRELLA

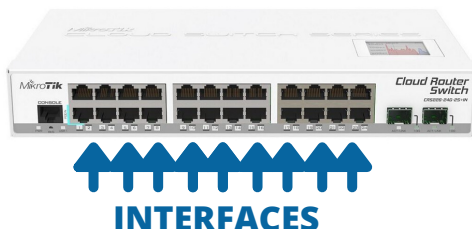
Cada dispositivo se conecta directamente a un concentrador central. En una topología de estrella todos los datos pasan a través del concentrador antes de alcanzar su destino. Esta es una topología común tanto en redes Ethernet como inalámbricas.

En la topología de estrella, los equipos de la red están conectados a un hardware denominado concentrador. Es una caja que contiene un cierto número de interfaces a las cuales se pueden conectar los cables de los equipos. Su función es garantizar la comunicación entre esos equipos:



A diferencia de las redes construidas con la topología de bus, las redes que usan la topología de estrella son mucho menos vulnerables, ya que se puede eliminar una de las conexiones fácilmente desconectándola del concentrador sin paralizar el resto de la red. El punto crítico en esta red es el concentrador, ya que la ausencia del mismo imposibilita la comunicación entre los equipos de la red. Sin embargo, una red con topología de estrella es más cara que una red con topología de bus, dado que se necesita hardware adicional (el concentrador).

Un hardware concentrador básicamente es una computadora modificada que cuenta con una tarjeta de red poderosa. Estas tarjetas de red pueden gestionar varios equipos a la vez, por lo que posee varias conexiones ethernet, llamadas interfaces.



OTRAS TOPOLOGÍAS FÍSICAS DE RED

Conoce en esta página web otras topologías menos utilizadas



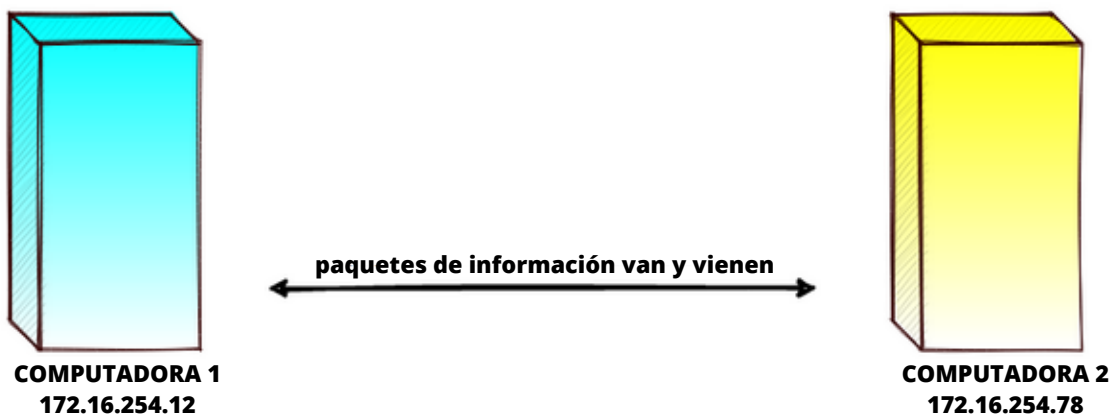
DIRECCIÓN IP

Junto con estar físicamente conectada a través de una tarjeta de red, **toda computadora posee una dirección dentro de una red; justo como en la ciudad cada edificio tiene una dirección postal.** Esta abstracción permite entender cómo se comunican las computadoras a través de una red. A todos los dispositivos (celulares, impresoras, computadoras, enrutadores, televisiones, etc) se les asigna un número en específico al conectarse a cualquier red. La internet protocol address, la dirección IP o simplemente IP, señala la dirección inequívoca de un dispositivo en una red de computadoras.

IPv4: 192.168.178.31

Un número IP consta de 4 bloques separados por un punto, y cada bloque va desde el número 0 al 255.

La dirección IP es el principal dato que utilizan las computadoras para comunicarse entre sí, es gracias a la IP es que una computadora sabe a quién envía mensajes y de quién los recibe. Dos dispositivos conectados a través de la tarjeta de red con IP asignadas, pueden compartir entre sí la información contenida en sus discos duros y enviar órdenes de un dispositivo a otro.



La dirección IP es usada por la COMPUTADORA 1 para saber dónde se encuentra la COMPUTADORA 2 y así poder entregarle paquetes de información y vice versa.

La dirección IP es una información efímera, es decir que se mantiene mientras exista conexión entre el dispositivo y la red, una vez desconectado de la red, la dirección IP desaparece. Esto muy por el contrario de lo que sucede con la dirección MAC.



IPv4

La dirección IP es el identificador perteneciente al protocolo IPv4 (Internet Protocol version 4) y puedes conocerla escribiendo en la terminal **hostname -I**

IPv6

Podrán parecer muchos pero en la actualidad las direcciones IPv4 están prácticamente agotadas, ya que 4 mil millones de computadoras es una cifra bastante normal a día de hoy. De hecho ya en 2011 empezaron a escasear, cuando el organismo encargado de dar direcciones IP en china dio uso al ultimo paquete, así que apareció al rescate el protocolo IPv6 (Internet Protocol version 6), que permitirá entregar IPs diferente a cada dispositivo del planeta. Aunque en la actualidad aún no está funcionando, nuestros equipos ya disponen de una dirección IPv6 en su tarjeta de red.

DIRECCIÓN MAC

Todos los dispositivos para conectarse a una red, requieren de una tarjeta de red. Toda tarjeta de red posee un identificador único, conocido como dirección física, dirección de hardware o MAC Address.

La dirección MAC (siglas en inglés de Media Access Control) es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red y es **única para cada dispositivo**. Es muy similar al número de serie del motor de un coche, el cuál al igual que la dirección MAC, identifica a ese motor en específico y no a otro.

Cada vez que nos conectamos a una red de computadoras, esta nos asigna una dirección IP a cambio de nuestra MAC Address, ya que de esta manera la red identifica a un mismo dispositivo, aunque su dirección IP cambie.

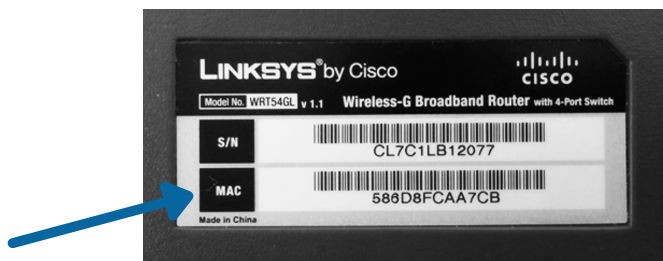
Con esto podemos determinar como si fuera una huella digital, desde que dispositivo se emitió un paquete de datos aunque este cambie de dirección IP, ya que cada dispositivo de red tiene una dirección MAC única globalmente que lo identifica.

Una dirección MAC se ve así:

00:17:4F:08:5F:69

Se conforma por 6 bloques divididos por dos puntos. Los primeros 3 bloques identifica quién es el fabricante del hardware y los 3 últimos bloques refieren al lote de fabricación. La entidad que se encarga de definir cómo se deben asignar las Mac Address es la **IEEE** (Instituto de Ingeniería eléctrica y electrónica).

Disponen de dirección MAC todos aquellos dispositivos con la opción de conectarse y transmitir datos a través de una red. Es decir, ordenadores de escritorio y portátiles, tablets, smartphones, televisores inteligentes, etc. Por lo general podemos encontrar la dirección MAC en la etiqueta con los detalles del equipo.



¿SABES QUIÉN FABRICO TU TARJETA DE RED?

Copia tu dirección MAC y colócala en el siguiente sitio web



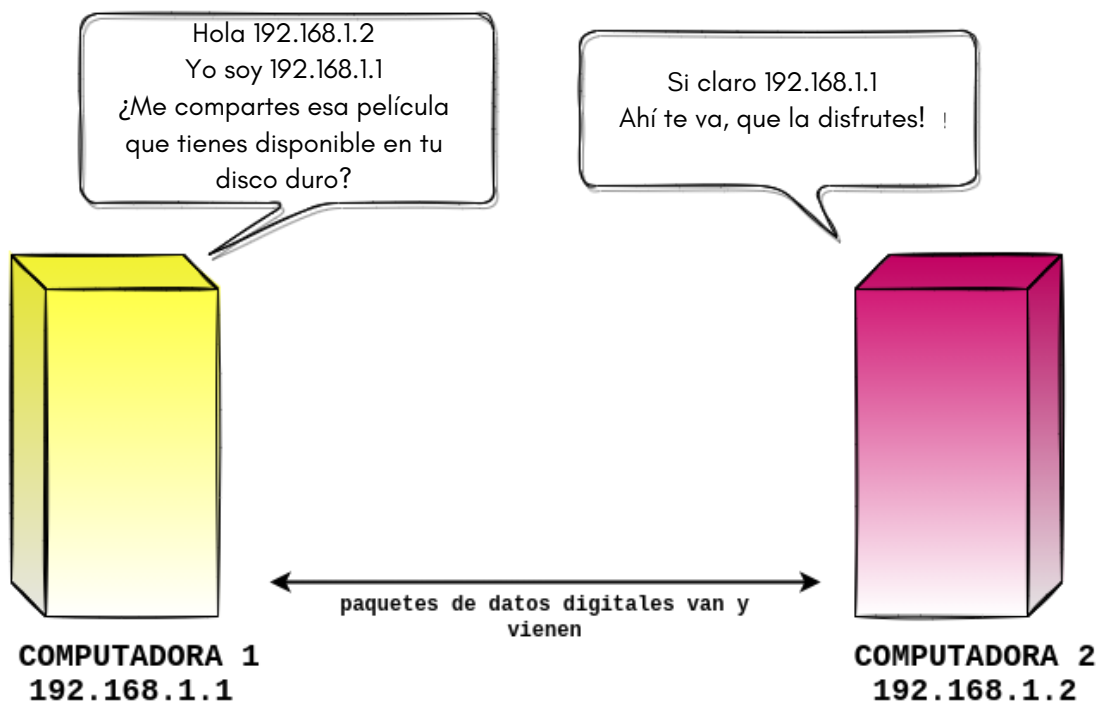
SERVIDOR Y CLIENTE

En una red de computadoras cuando una computadora entrega acceso e información a otra, le llamamos servidor. Es como cuando dos personas dialogan, una es la que habla.

Cuando una computadora accesa a otra para obtener información, le llamamos cliente. Es como cuando dos personas dialogan, una escucha. Al igual que en la comunicación humana, estos roles pueden ser intercambiados.

Los **servidores** son computadoras conectadas a la red que almacenan información y la tienen disponible para que otras computadoras accedan a ellas. Por ejemplo, Facebook, Netflix o tu página web preferida son alojados en servidores.

Los **clientes** son dispositivos que solicitan acceso e información en los servidores. Por ejemplo, tu celular cuando estás viendo un video en Internet.



En el ejemplo la COMPUTADORA 1 es el cliente, que solicita al servidor (COMPUTADORA 2) acceso a la descarga o visionado de un archivo de video.

Potencialmente cualquier computadora puede ser un servidor. Solo basta una conexión y el software adecuado instalado. Por lo general uno tiende a pensar que un servidor es una gran y costosa computadora, lo cual es cierto, pero no es menos cierto tampoco que una computadora antigua podemos reciclarla para transformarla en un servidor web, en un servidor streaming o incluso en un servidor tipo nube.

Como vemos un servidor es una computadora que sirve a otras computadoras a través de la red, por ello es fundamental que el servidor mantenga su conexión con la red en todo momento, si por algún motivo el servidor se apaga o pierde su conexión, la información o contenidos ofrecidos ya no estarán disponibles en línea.

ARQUITECTURA SERVIDOR - CLIENTE

La tecnología denominada Cliente - Servidor es utilizada por todas las aplicaciones de Internet/Intranet. Un cliente funciona en su computadora local, se comunica con el servidor remoto y pide a éste información. El servidor es un programa que recibe una solicitud, realiza el servicio requerido y devuelve los resultados en forma de una respuesta. Generalmente un servidor puede tratar múltiples peticiones (múltiples clientes) al mismo tiempo.

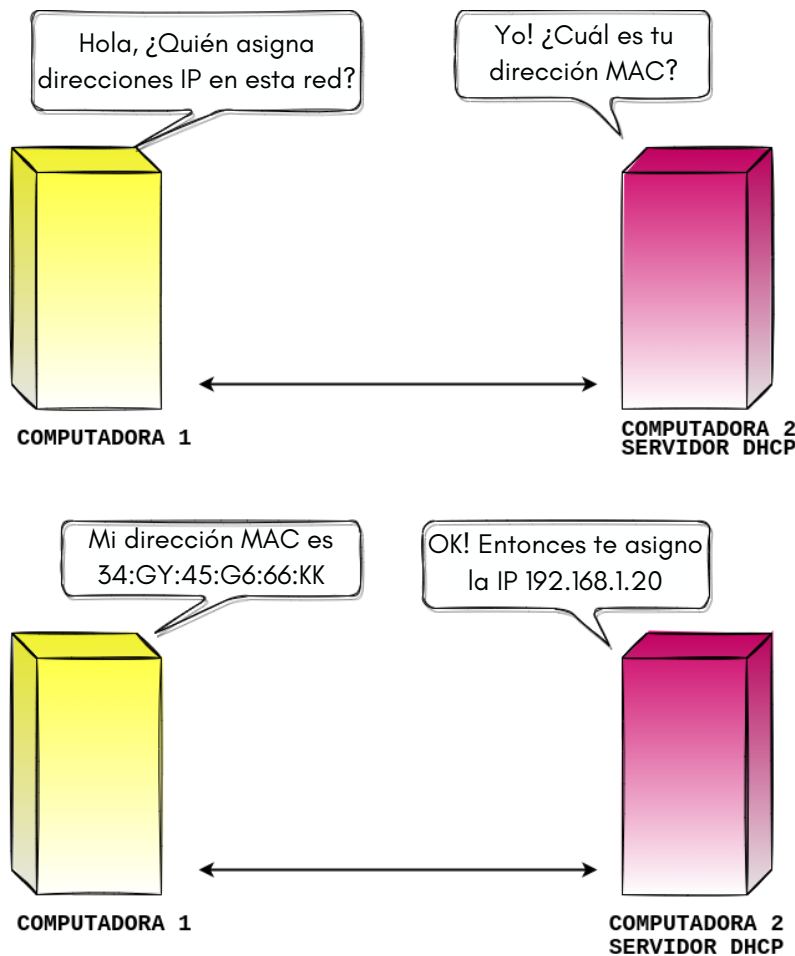
SERVIDOR DE DIRECCIONES IP

Pero quién decide las direcciones IP, ciertamente no lo hacemos nosotras, ¿entonces quién? En una red de computadoras se deben asignar muchas y muy rápidamente las direcciones IP, una por cada dispositivo que se conecta, por lo que esa labor se le encomienda a una computadora con un software específico, que pasa a cumplir las funciones de un servidor de direcciones IP o servidor DHCP dentro de la red.

Cada vez que se conecta un dispositivo a una red, hace una consulta por el servidor DHCP, el servidor DHCP responde y se encarga de asignarle una dirección IP a cambio de su dirección MAC. De esta manera es el servidor DHCP quien genera y almacena las direcciones IP, conociendo así la ubicación de todos los dispositivos que participan de la red.

En un sistema con topología de estrella (la que más utilizaremos y dónde las todas computadoras se conectan a un hardware concentrador), el rol de Servidor DHCP lo cumple el hardware concentrador, que junto con entregar direcciones de red, conoce exactamente en cuál de sus interfaces se ubica cada dirección IP.

Es el servidor DHCP quien nos brinda acceso a toda la red, es a través de él que nos comunicamos con otras computadoras. Por este motivo el servidor DHCP también es conocido como "Puerta de Enlace" o "Gateway".



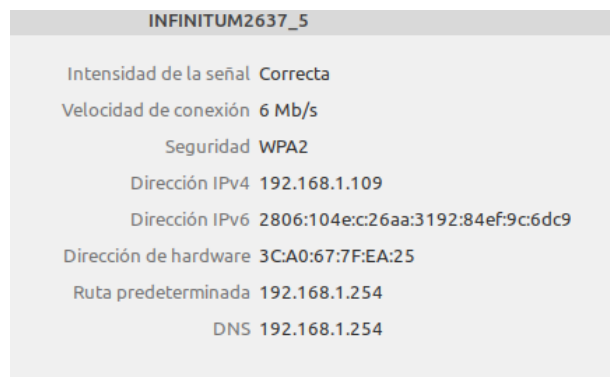
La acción de repartir direcciones IP se le conoce como **Direccionamiento IP**. Cuando sucede el direccionamiento IP, la IP no es la única información que entrega el Servidor DHCP al Cliente. Junto con su IP asignada se le informa al cliente de otros importantes y vitales parámetros para poder participar de la red, como lo es la IP del Servidor DNS y la Máscara de Red.

Imaginemos que nuestra red es una mesa de póker, cada uno de los jugadores es una computadora conectada, y quien reparte las cartas (crupier) es el servidor DHCP.

Al comenzar el juego el crupier reparte cartas a las jugadoras y también se reparte cartas así misma, de la misma manera que el servidor DHCP asigna direcciones IP tanto a los dispositivos que se conectan, como también a sí misma. Cuando se acaba el juego (o la conexión a la red) el crupier retira las cartas (direcciones IP).

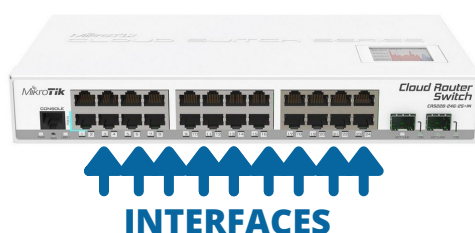
Como en el póker, pueden existir varios jugadores (computadoras conectadas) pero sólo puede haber un crupier por mesa (servidor DHCP) y, los jugadores no hablan entre sí, sino que todos se comunican con el crupier, quién se encarga de administrar el juego.

De igual manera un servidor DHCP juega un rol fundamental almacenando las direcciones de los dispositivos conectados y gestionado el tráfico entre ellas. Cuando una computadora necesita comunicarse con otra, es el servidor DHCP quién conoce dónde existen ambas, es decir conoce la interface o ruta para llegar de una a otra.



*En la configuración de red de tu computadora se despliega la información proporcionada por el Servidor DHCP durante el **direccionamiento IP**: Una IP para sí, la IP de la Puerta de Enlace, la IP del Servidor DNS.*

Los servidores DHCP se montan sobre un hardware concentrador. Estos equipos cuentan con múltiples conexiones o "puertos Ethernet", y se les conoce como interfaces.



INTERFACES

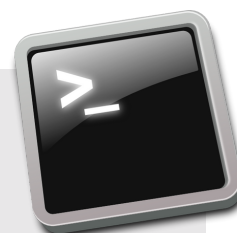
En informática, esta noción sirve para señalar a la conexión que se da de manera física entre dispositivos o sistemas. Este término es un préstamo proveniente del inglés interface, comprendido como "superficie de contacto" entre dos entidades, y se popularizó a través de la tecnología informática.

La interfaz puede ser de distintos tipos. Las más utilizadas para las redes actuales son los cables ethernet, el Wi-Fi y la fibra óptica.

CONFIGURACIÓN DE RED

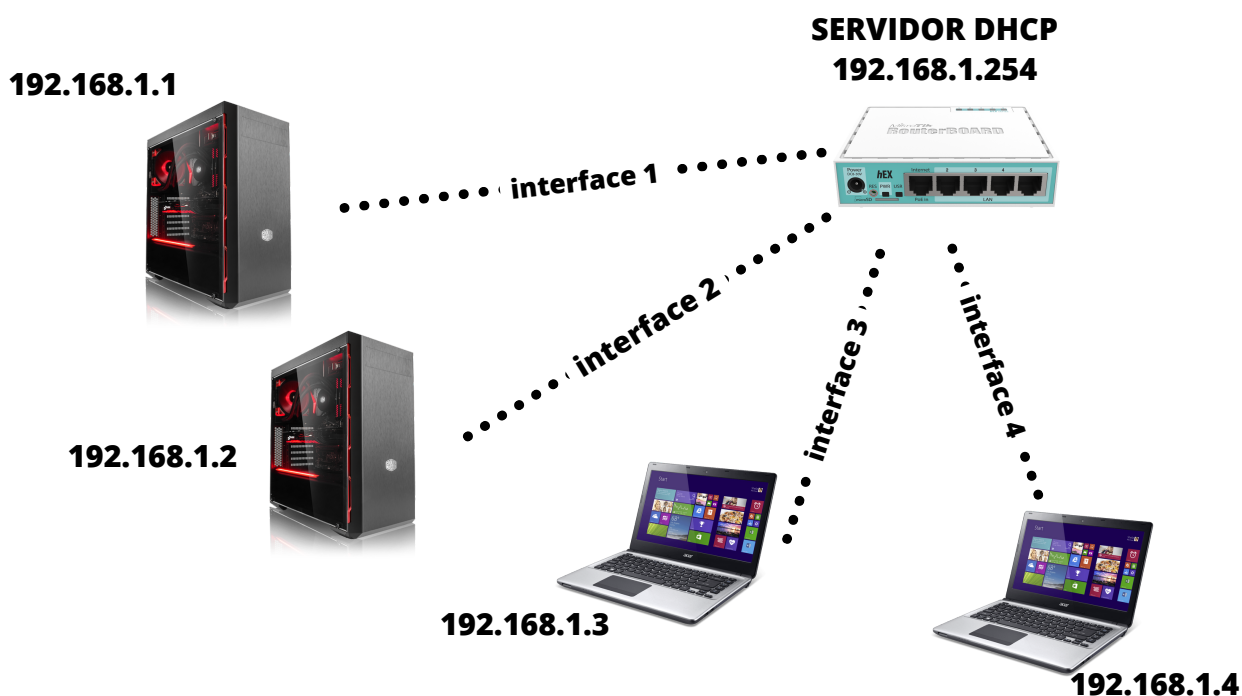
Puedes revisar los parámetros de red escribiendo en tu terminal de linux:

ifconfig



Sigamos el ejemplo que tenemos abajo. Si la computadora 192.168.1.4 quiere comunicarse con la computadora 192.168.1.1, la computadora 192.168.1.4 se comunicará primero con el servidor DHCP (192.168.1.254) porque es la puerta de enlace a la red, él reenviará la comunicación a la interface conectada a la computadora 192.168.1.1. De la misma manera, la computadora 192.168.1.1 al enviar la información solicitada por la computadora 192.168.1.4, enviará ese paquete de información al servidor DHCP quién a su vez lo enviará a la computadora 192.168.1.4

Por ello el servidor DHCP de una red es fundamental para que los paquetes de información puedan llegar a destino con éxito.



*El camino que toman los paquetes para llegar de su origen a destino, se le conoce como **ruta**. Es el servidor DHCP quién conoce todas las rutas que existen dentro de una red que administra.*

PAQUETES DE DATOS

En una red de computadoras, la información viaja encapsulada en paquetes de datos. Estos paquetes de datos contienen el número IP tanto del emisor como del receptor de dicho paquete de datos.

El paquete de datos en el protocolo de internet (TCP/IP) se compone de un encabezado con las direcciones de quien envía y recibe, y un cuerpo, o carga útil, con los datos que se van a transferir.

TABLAS Y RUTAS

Es importante conocer que el servidor DHCP crea una base de datos con los números IP y las interfaces donde se ubican estos números IP. Esta información es la que organiza el tráfico dentro de una red, conocemos a esta base de datos con el nombre de tabla de rutas. Las rutas son tan importantes dentro de una red, que el enrutador obtiene su nombre de ellas.

Cada vez que un paquete llega al servidor DHCP, la tabla de rutas le dirá hacia dónde tiene que dirigir ese paquete. La tabla de rutas se construye durante el direccionamiento IP y sin esta información el servidor DHCP no sabría hacia dónde enviar el tráfico de la red.

IP	Interface
192.168.1.1	eth1
192.168.1.2	eth2
192.168.1.3	eth3
192.168.1.4	eth4

En esta tabla de rutas podemos ver nuestra red ejemplo . Por lo general los equipos de red reemplazan la palabra interface por la abreviación eth1, eth2, eth3, como vemos aquí.

En una tabla de rutas podemos asignar más de un número IP a cada interface; incluso podemos asignar un rango de IPs completo a una interface. Esta capacidad de dirigir el tráfico hacia otros rangos de IPs distintos y por ende otras redes, es lo que permite interconectar distintas redes de computadoras.

IP	Interface
192.168.1.0/24	eth1
192.168.2.0/24	eth2
192.168.3.0/24	eth3
192.168.4.0/24	eth4

En esta segunda tabla de rutas podemos ver que cada interface tiene asociado un rango de IP distinto. Así el enrutador ya conoce a que red corresponde enviar cada paquete.

TCP/IP

Son las siglas de Transmission Control Protocol/Internet Protocol (Protocolo de control de transmisión/Protocolo de Internet). TCP/IP es un conjunto de reglas estandarizadas que permiten a los equipos comunicarse en una red como Internet.

MÁSCARA DE RED

Una IP siempre irá acompañada por una máscara de red, para que puedas identificarte correctamente en una red. La máscara de red es un parámetro que se utiliza para delimitar el rango o tamaño de una red. El rango de una red hace referencia a cuáles segmentos de dirección IP estarán disponibles para que el servidor DHCP entregue direcciones.

Imagina que en casa, te conectas a tu enrutador con tres dispositivos. La IP del primero es 192.168.1.2, la del segundo 192.168.1.3 y la del tercero 192.168.1.4. Como puedes ver, los tres primeros segmentos de las IPs son iguales mientras que el último cambia. Lo que hace la máscara de red es identificar esa parte fija de la IP y la parte variable.

A efectos prácticos, la máscara de red se trata de otro número IP, pero cuya numeración casi siempre va a estar compuesta por ceros y el número 255. Entonces, por ejemplo, por una parte puedes tener una IP que puede ser 192.168.1.1, y con una máscara de red que sea :

255.255.255.0

El 255 indica que ese segmento de IP no varía, y el 0 indica que el segmento sí es variable. Por lo tanto, si tienes una máscara que es 255.255.255.0, quiere decir que en esa red los tres primeros bloques de números de la IP nunca cambian, y sólo se asignan IPs variando los números del último segmento.

192.168.1.1

En este caso, tendremos un total de 255 direcciones disponibles, que van desde 192.168.1.1 hasta 192.168.1.255. La primera dirección IP de una red, en este caso 192.168.1.0 siempre se reserva para identificar a la red misma.

Toda red debe delimitar su rango, es decir, señalar cuáles segmentos de IP estarán disponible para que el servidor DHCP reparta direcciones, esto define entre otras cosas, la cantidad de dispositivos que pueden formar parte de la red.

Teniendo en cuenta esto, podemos poner otro ejemplo para que quede más claro aún. Si partimos de una dirección IP 192.168.0.0 y una máscara **255.255.0.0** significa que la red irá desde la dirección **192.168.0.0** hasta la **192.168.255.255**. Es decir, tendremos disponibles una red con un total de hasta 65025 equipos.

Entonces podemos ver que una dirección IP está compuesta por dos partes, una fija y otra móvil. La parte fija de una dirección IP se le conoce como identificador de red, y a la parte móvil, identificador de host o cliente.

Para hacer la vida más fácil (o más difícil depende de donde se mire), se suele usar otra forma para explicitar la máscara de red. Como mencionamos anteriormente para identificar una red reservamos la primera dirección IP del rango, esta IP acompañada de un **/8, /16 o /24**, es también una representación válida de una máscara de red. Veamos por ejemplo...

192.0.0.0/8

Aquí estamos señalando una red con un rango enorme que contiene las direcciones desde la 192.0.0.0 a la 192.255.255.255 (¡alrededor de 24 millones de direcciones!).

192.168.0.0/16

Un rango más pequeño, y sólo contiene las direcciones IP de la 192.168.0.0 a la 192.168.255.255.

192.168.1.0/24

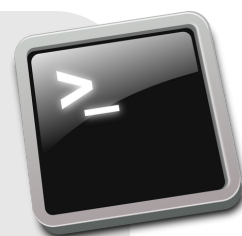
Es un rango aún más pequeño, y sólo contiene las direcciones 192.168.1.0 a 192.168.1.255.

Entonces, podemos hacer la siguiente tabla de equivalencia entre ambas formas de expresar lo mismo:

/24	—————→	255.255.255.0
/16	—————→	255.255.0.0
/8	—————→	255.0.0.0

ACCEDER A LAS CONFIGURACIONES DE RED

Escríbe en tu terminal linux **ifconfig** y aparecerán tu IP (inet) , Máscara de red (netmask) y Puerta de Enlace (bradcast).



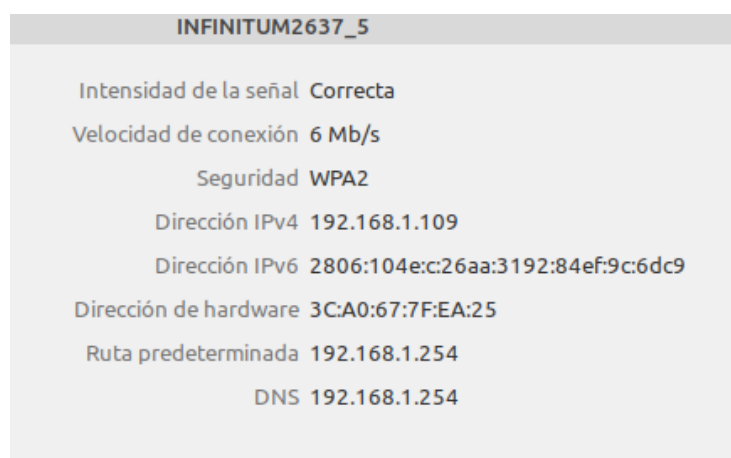
SERVIDOR DE NOMBRES DE DOMINIO (DNS)

El servidor DHCP es el servidor más importante dentro de una red, pero no es el único; para que una red pueda ser utilizada por personas requiere de un servidor de nombres de dominio (DNS).

Desde lo inicios de la computación en red se hizo evidente que recordar direcciones IP para acceder a los distintos dispositivos en red sería una tarea difícil para el ser humano. Por ello se creó el Domain Name System (sistema de nombres de dominio) que sirve para resolver nombres en las redes, es decir, para llegar a un dispositivo ya no se necesita una dirección IP, sino que basta conocer un dominio (nombre o palabra) asociado a esa IP para acceder a la comunicación.

La labor del servidor de nombres de dominio o servidor DNS, es almacenar una lista de palabras que corresponden a números IP específicos, de tal manera que no sea necesario recordar un número para acceder a otra computadora en red. El nombre de dominio equivale a una dirección IP.

Tu utilizas los servidores DNS constantemente, ya que google.com, facebook.com, la web del banco, la de tu organización, tienen asignada una IP. Por ejemplo, cuando descargaste este manual a través de Internet no escribiste la IP de la computadora que aloja la web, sino que escribiste el dominio asociado a la IP, en este caso: <https://laboratoriodemedios.org>



Cuando nos conectamos a una red, el servidor DHCP además de asignarle una IP al equipo recién conectado, también le informa cuál es la IP de la máquina registrada como Servidor DNS en la red. Esa información la podemos comprobar en las configuraciones de red de nuestro equipo.

Para navegar en algún sitio web colocamos su dominio en la barra de direcciones del navegador y damos enter. Lo que sucede en ese momento es que la computadora se comunica con la IP que tiene registrada como servidor DNS y le pregunta a cuál IP corresponde el dominio que queremos visitar; el servidor DNS revisa la información que tiene almacenada y responde con la IP correspondiente al dominio, así nuestra computadora ahora conoce el número IP correspondiente de la computadora con la cual queremos comunicarnos.

Si tienes a la mano una computadora linux con conexión a internet, ingresa a la terminal y escribes: ping facebook.com y podrás conocer el número ip de la red social.

```
chasqui@kipulap:~$ ping facebook.com
PING facebook.com (31.13.70.36) 56(84) bytes of data.
64 bytes from edge-star-mini-shv-01-lax3.facebook.com (31.13.70.36): icmp_seq=1 ttl=58 time=55.7 ms
64 bytes from edge-star-mini-shv-01-lax3.facebook.com (31.13.70.36): icmp_seq=2 ttl=58 time=52.4 ms
64 bytes from edge-star-mini-shv-01-lax3.facebook.com (31.13.70.36): icmp_seq=3 ttl=58 time=54.5 ms
64 bytes from edge-star-mini-shv-01-lax3.facebook.com (31.13.70.36): icmp_seq=4 ttl=58 time=51.4 ms
64 bytes from edge-star-mini-shv-01-lax3.facebook.com (31.13.70.36): icmp_seq=5 ttl=58 time=52.2 ms
```

PING

El comando ping tiene su origen en los **submarinos** y sus **sonares**, que envían una señal sonora para detectar si hay algún cuerpo en el agua. Si esta vuelve, significa que hay algún cuerpo o barrera en la trayectoria de la señal emitida por el sonár. El mecanismo del comando ping es similar al que utiliza el sonár: se puede ver si hay conectividad entre dos computadoras y el tiempo que tardan en llegar los paquetes en función del tiempo de respuesta.

En la terminal linux escribe ping seguido de un número IP o un nombre de dominio. Si existe la capacidad de que los paquetes de datos vayan y vuelvan del destino, el ping será satisfactorio. Cuando no haya comunicación se presume que uno de los equipos está apagado o desconectado de la red.



SERVIDOR DE SERVICIOS

Hasta el momento hemos visto servidores que permiten que la comunicación exista entre las computadoras conectadas en red... pero ¿dónde están la información que consultamos en línea, las fotos, las páginas web, los videos que vemos en línea?, la respuesta es: en los servidores de servicios.

Los servidores de servicios son computadoras conectadas a la red que almacenan información y la tienen disponible para que otras computadoras accedan a ellas. Por ejemplo, Facebook, Netflix o tu página web preferida, son información alojada en servidores de servicios.

Cualquier computadora conectada a una red con el software apropiado instalado puede funcionar como un servidor de servicios, incluso la mismísima computadora desde donde nos lees en este momento. Los servidores son computadoras que permiten el acceso remoto a los archivos que almacenan y a los servicios que brindan.

Un servidor de servicios atiende y responde a las peticiones que le hacen otras computadoras. Las computadoras que le hacen peticiones, serán los "clientes" del servidor. Estos "servicios" son los recursos que usamos y conocemos comúnmente en Internet. Alojamiento Web, Correo, Redes Sociales, Video bajo demanda, Mensajería, VideoLlamados, etc.

SERVIDORES

Para obtener más información acerca de los tipos de servidores y su función puedes escanear o dar clic en el siguiente código QR.



Instalar el software para alojar un servicio de streaming tipo netflix, o un servidor para alojar páginas web, es muy simple y actualmente gracias al software libre existen muchas opciones de instalación automatizada que no requieren conocimientos previos. En la actualidad montar tu propio servidor es una opción viable ante las grandes empresas de internet.

Cuando visitamos un sitio web o revisamos nuestros correos, en realidad nuestra computadora se está conectando a otra computadora que se encuentra físicamente en algún lugar del planeta con una dirección de IP asignada. De ella obtenemos la información almacenada en su **disco duro**. Esta información puede ser una página web, un video, un correo electrónico o cualquier otro tipo de datos.

Los servicios llamados "nube", no son algo etéreo. Por ejemplo, cuando "subes" una foto a la "nube" desde el celular para poder verla en la computadora personal, lo que realmente estamos haciendo es transferir esa información al disco duro de una computadora de una empresa privada, prendida las 24 horas y conectada a Internet desde algún punto del planeta. Al iniciar nuestra cuenta de "nube" en la computadora personal, lo que sucede es que automáticamente se conecta con la computadora del servicio de nube y descarga la foto en cuestión.

¿QUIÉNES SON LOS DUEÑOS DE LOS SERVIDORES DE SERVICIOS?

Según la Comisión Económica para Latinoamérica y el Caribe (Cepal), nuestra región es la más dependiente de los EE.UU. en términos del tráfico de Internet. El 80% de la información electrónica de la región pasa por algún nodo administrado directa o indirectamente por Estados Unidos.

Cuando navegas en Facebook, realmente estás accediendo a los discos duros propiedad de Facebook Inc. y ellos a través de tu IP saben exactamente quién eres. De igual manera, (si estas leyendo este documento online) el servidor del Laboratorio Popular de Medios Libres usa también tu dirección de IP para mandarte los paquetes que contienen la información que estás leyendo en este instante, la diferencia es que nosotras no almacenamos tus datos ni los vendemos a terceras personas.



Como existen grandes servidores, también podemos construir nuestros servidores propios o caseros.

SERVIDORES AUTÓNOMOS

También existen los servidores autónomos, gestionados por personas o colectivos cuya sostenibilidad no depende del comercio con los datos privados de sus usuarias. Los servidores autónomos promueven una internet con redes y servicios digitales donde se respete la privacidad y el acceso a la información, el conocimiento y la producción de contenidos. Puedes encontrar una lista de ellos en el código QR.



H. EQUIPOS DE RED

Como vimos anteriormente, una red de comunicación digital está conformada por computadoras conectadas entre si, pero vimos también que existen computadoras con modificaciones para brindar mejor funciones dentro de una red, estamos hablando de los enrutadores, switches, módems y firewalls.

A continuación revisaremos el hardware necesario para montar una red de manera más detenida:

ENRUTADOR

El enrutador es un dispositivo dedicado a la tarea de administrar el tráfico de que circula por una red de computadoras. Además todo enrutador tiene la capacidad de participar de dos redes al mismo tiempo.

Un enrutador es una computadora, tiene un procesador o CPU, memoria RAM, disco duro e incluso un sistema operativo, que en estos casos se les conoce como Firmware. Lo que distingue a un enrutador de una computadora tradicional es su tarjeta de red. Un enrutador debe tener como mínimo dos tarjetas de red, pues en la gran mayoría de los casos será el enrutador el encargado de dar conexión a internet, vía cable o Wi-Fi, a los distintos clientes de la red.

Otra función principal de un enrutador es crear una red entregando direcciones IP a cualquier dispositivo que se conecte a él, es decir un enrutador siempre cuenta con un servidor DHCP en funcionamiento.

Existen una gran variedad de enrutadores, los hay desde muy pequeños y baratos hasta grandes y costosos, bonitos y estéticos para que combinen con una decoración moderna o rudos y a prueba de golpes de rayo. Existen enrutadores muy simples y los hay con una gran variedad de capacidades, todo depende de las necesidades que se intenten cubrir con el equipo.



SWITCH O CONMUTADOR



Los switches son piezas de construcción clave para cualquier red. Un switch permite interconectar varios o muchos dispositivos entre sí dentro de una red. Básicamente un switch es un concentrador de conexiones, toma muchos cables y los une en una sola conexión.

La función básica de un switch es la de unir o conectar computadoras en red. Es importante tener claro que un switch **NO proporciona direcciones IP** ni conectividad con otras redes. Para ello es necesario un enrutador.

Los puertos son las bocas donde se conectan cables que permiten la conexión de los dispositivos. El número de puertos es una de las características básicas de los switches. Aquí existe un abanico bastante amplio, desde los pequeños switches de 4 puertos hasta switches troncales que admiten varios cientos de puertos con unas prestaciones y características muy avanzadas.

PUNTO DE ACCESO INALÁMBRICO



En realidad los switches no son los únicos elementos encargados de la interconexión de dispositivos en una red local. Los switches realizan esta función para medios cableados, pero cuando la interconexión se realiza de forma inalámbrica, el dispositivo encargado de ello se denomina Punto de acceso inalámbrico.

Cada punto de acceso genera una pequeña red inalámbrica para que distintos dispositivos se conecten a ella. Cuentan como mínimo con dos tarjetas de red, una que dialoga a través de la radiofrecuencia utilizando el protocolo Wi-Fi y otra tarjeta de red que dialoga a través de cable ethernet. Gracias a éstas características un punto de acceso es capaz de concentrar varias o muchos dispositivos wi-fi y transferir todo ese tráfico aéreo a un cable ethernet, para llevar todas esas conexiones hasta un enrutador a través de un cable.

CORTAFUEGOS O FIREWALL



Un firewall de hardware, como el dispositivo de la imagen, tiene un aspecto muy similar a un enrutador o switch

El cortafuegos o firewall en inglés, es un sistema de seguridad para bloquear accesos no autorizados a una red o computadora mientras sigue permitiendo la comunicación con otros accesos autorizados.

Los cortafuegos pueden ser de dos tipos, pueden ser software, de hardware o una combinación de ambos. Esto quiere decir que pueden ser aplicaciones que instales en tu computadora o, en dispositivos diseñados específicamente para controlar el tráfico.

En un firewall se establecen criterios de seguridad y a partir de ello **analiza y filtra todas las comunicaciones que entran o salen de la red** que no cumplan con estos criterios, dejando pasar al resto.

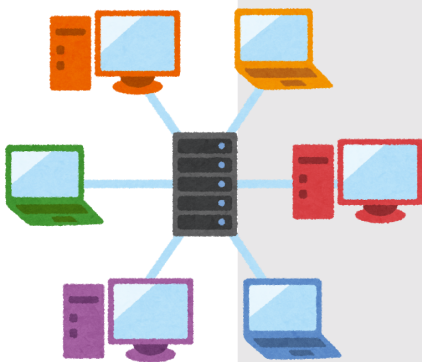
Al poder analizar el tráfico saliente y entrante, también pueden llegar a detectar si hay algún malware comunicándose con la red, monitorizando el uso de la red, o filtrando el tráfico.

Además, los cortafuegos son muy utilizados para restringir el acceso de usuario a páginas web en específico, por ejemplo, para que el navegador de las computadoras de una empresa pueda conectarse a Internet, pero bloqueando el acceso a las redes sociales.

¿UN EQUIPO DE RED PARA CADA FUNCIÓN?

Los equipos de red suelen cumplir más de una función en específico. Es muy extraño encontrar un equipo que cumpla solo una función. Por eso es que es difícil clasificarlos de manera determinante.

La mejor manera para poder clasificar o seleccionar un equipo de red es revisar qué capacidades tiene, en función de las necesidades que tenemos para nuestra red.



MÓDEM

El estándar de las redes de computadoras, admite básicamente dos tipos de medios de transmisión cableados: el cable de par trenzado, más conocido como cable de red y el cable de fibra óptica.

El conector y la tecnología utilizada para cada tipo lógicamente es diferente, así que el módem se encarga de traducir las señales que viajan por la fibra óptica en datos que pueden viajar por un cable de red. Por esa labor es fácil reconocer un módem, puesto que dispondrá de puertos de cable de red (conector RJ-45) y puertos de fibra óptica (el conector más frecuente aunque no el único es el de tipo SC) disponibles en su hardware.

Los módems son muy utilizados por las grandes empresas de telecomunicaciones, ya que históricamente les ha permitido brindar acceso a Internet a través de la red de telefonía, gracias a que este dispositivo es capaz de convertir las señales digitales en analógicas, proceso llamado “modulación”, y también es capaz de convertir las señales analógicas en digitales, a cuyo proceso se le llama “demodulación”, de ahí su nombre MÓDEM.

Actualmente grandes empresas privadas han creado una gran red de fibra óptica, incluso se han instalado enormes cables en el lecho marino, con la cuál pueden transportar grandes cantidades de datos a una gran velocidad, lo que les permite interconectar regiones, países y continentes, pero por un tema de costos y ventajas, las redes locales a las cuales nos conectamos, se construyen con cables de red o emisiones Wi-Fi, de ahí el uso de los módems.



Podemos reconocer un módem fácilmente porque tendrá una conexión de fibra óptica como también de ethernet o wi-fi



FIBRA ÓPTICA

La fibra óptica es la tecnología usada para transmitir información en forma de pulsos de luz mediante hilos de fibra de vidrio o plástico y permiten transmitir más datos a través de distancias más largas y de forma más rápida que otros medios

I. ¿CÓMO FUNCIONA UNA RED?

ELEMENTOS MÍNIMOS

Ahora que conocemos los componentes que forman parte y permiten el funcionamiento de una red de computadoras, podemos comenzar a imaginar una red y analizar cómo funciona por dentro.

Vamos a hacer un pequeño ejercicio construyendo algunas redes de manera gráfica. En este primer ejemplo construiremos una red muy básica pero con todos los elementos necesarios para que funcione correctamente. En el esquema 1 contamos con un Enrutador, un servidor DNS, un Servidor de Servicios y dos clientes en una **topología de estrella** utilizando cableado para comunicar a las tarjetas de red de los dispositivos:

SERVIDOR DNS



SERVIDOR DE SERVICIOS



ENRUTADOR



CLIENTE

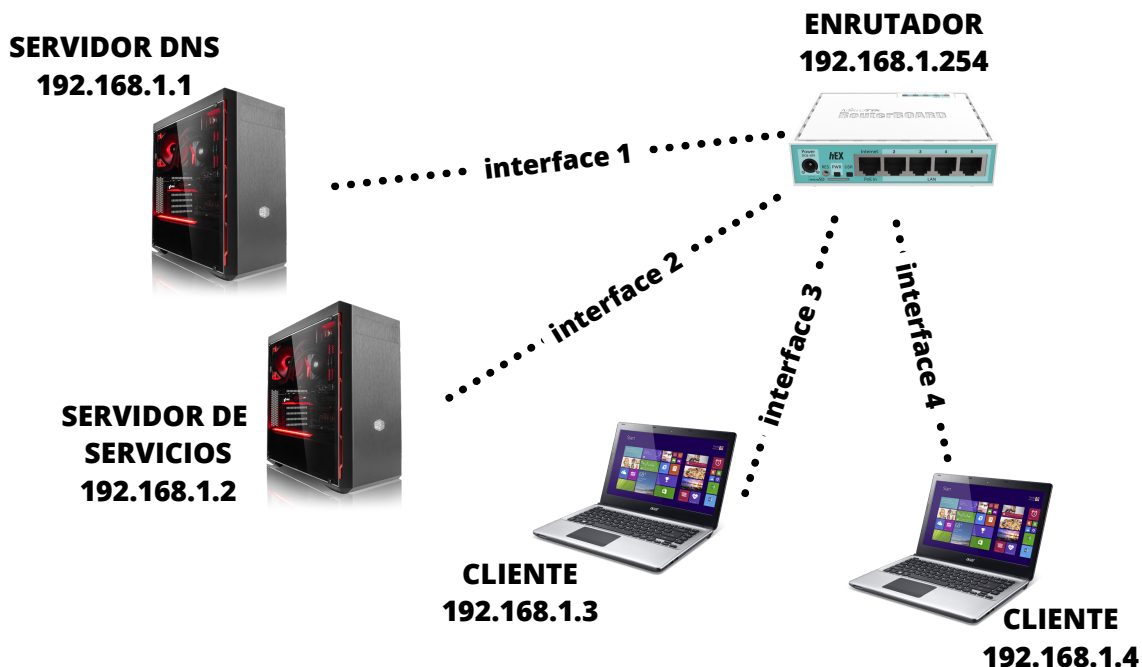


CLIENTE



DIRECCIONAMIENTO IP

Lo primero que sucederá con nuestra red cuando encendamos y conectemos los equipos es el direccionamiento IP. El enrutador asignará direcciones IP a todos los dispositivos a cambio de sus direcciones MAC; al asignar las direcciones IP ahora el enrutador conoce en que interface se encuentra conectado cada equipo y crea una base de datos (o tabla) con esa información. En el esquema 2 hemos identificado las interfaces e IPs con los números 1, 2, 3 y 4.



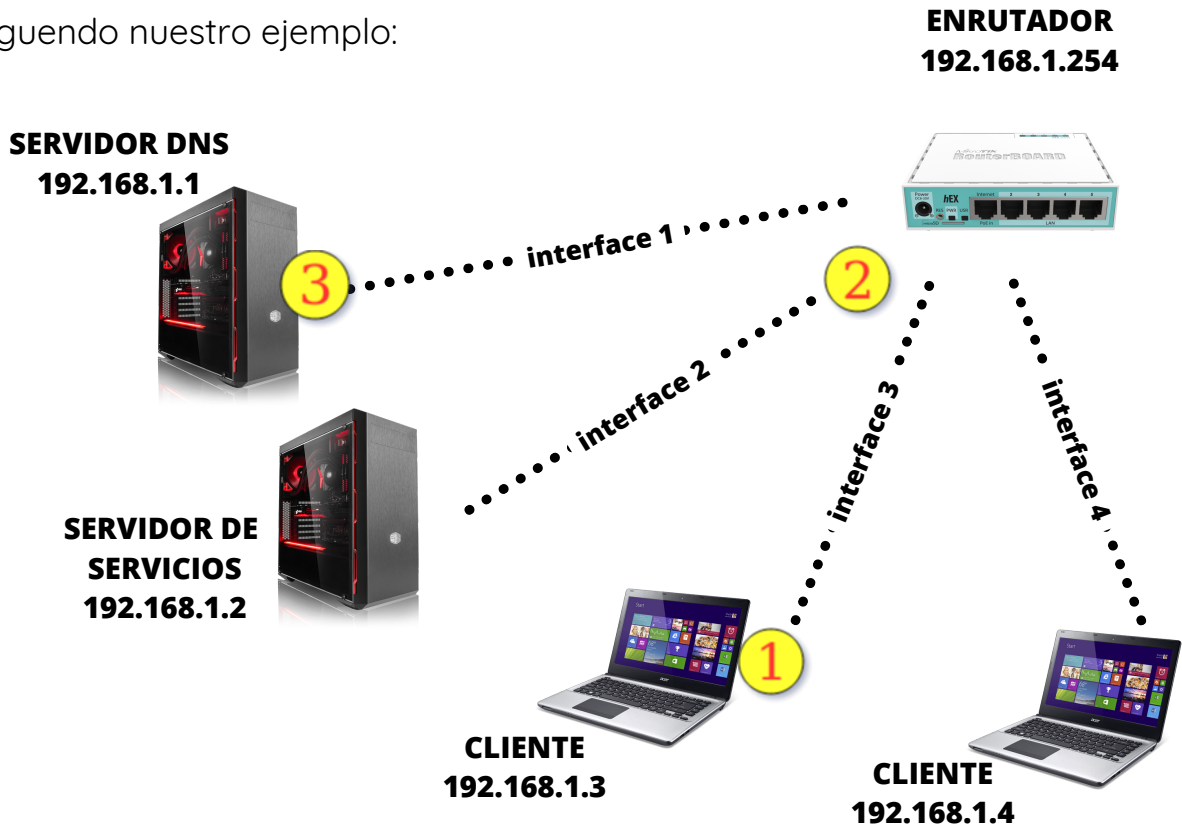
Ahora imaginemos por un momento que el servidor de servicios con la IP 192.168.1.2 es una plataforma de video streaming, y la computadora cliente 192.168.1.3 quiere acceder a ese servicio.

Primero, vamos a revisar la información que aparece en las **configuraciones de red** de la computadora cliente. Los datos desplegados en esa ventana es toda la data respecto a la red que el enrutador entregó a la computadora cliente durante el direccionamiento IP.

INFINITUM2637_5	
Intensidad de la señal	Correcta
Velocidad de conexión	6 Mb/s
Seguridad	WPA2
Dirección IPv4	192.168.1.3
Dirección IPv6	2806:104e:c26aa:3192:84ef:9c:6dc9
Dirección de hardware	3C:A0:67:7F:EA:25
Ruta predeterminada	192.168.1.254
DNS	192.168.1.1

Entonces, para comunicarse con el servidor de servicios, la usuaria escribirá el dominio de la plataforma de videos en su navegador, por ejemplo videos.net. Lo primero que debe hacer la computadora cliente es averiguar a qué número IP corresponde el dominio videos.net, para ello hará una consulta al servidor DNS de la red.

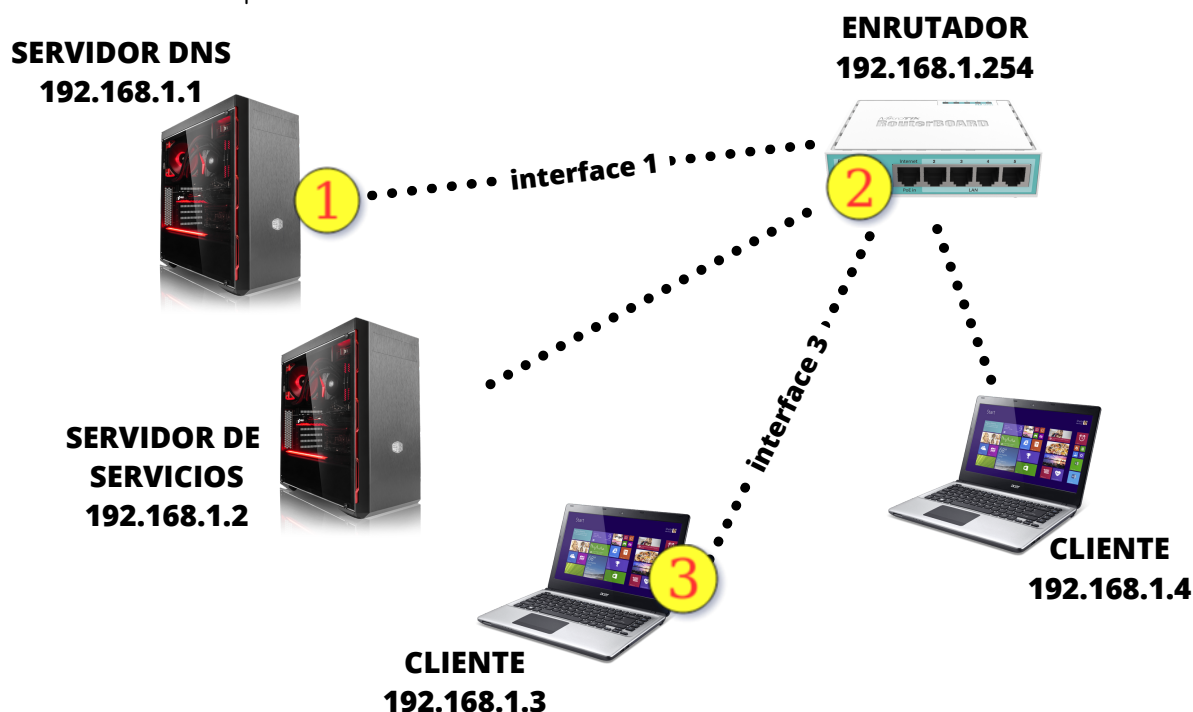
Siguiendo nuestro ejemplo:



- 1 En ese momento la computadora 192.168.1.3 enviará paquetes de datos a la puerta de enlace de la red 192.168.1.254, es decir el enrutador, con destino al servidor DNS 192.168.1.1
- 2 El enrutador, tomará esos paquetes y los redirigirá de acuerdo a la tabla de rutas, en este caso hacia la interface 1.
- 3 En este punto, el Servidor DNS recibe desde la puerta de enlace paquetes de datos del cliente 192.168.1.3 con una solicitud de información respecto al dominio videos.net

Todos los paquetes de datos en una red de computadoras vienen firmados con la IP de origen y la IP de destino; gracias a este protocolo el servidor DNS conoce a quién responder. Es muy similar al sistema de correos tradicional, donde cada carta que enviamos (paquete de datos) lleva una dirección de destino y una dirección del remitente (IPs).

Siguendo nuestro ejemplo, ahora el servidor DNS va a responder con la información solicitada a quién la solicitó, para ello se repite el proceso pero en la dirección opuesta:

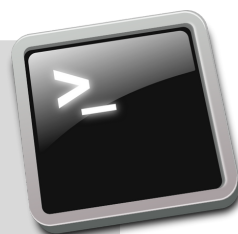


- 1 En ese momento el servidor DNS 192.168.1.1 enviará paquetes de datos a la puerta de enlace de la red 192.168.1.254, es decir el enrutador, con destino al cliente 192.168.1.3
- 2 El enrutador, tomará esos paquetes y como conoce la ruta (interface) de la IP de destino, los redirigirá a la interface correspondiente, en este caso la interface 3.
- 3 En este punto, el cliente recibe desde la puerta de enlace paquetes de datos del Servidor DNS con la información solicitada, en este caso, el número IP correspondiente al dominio videos.net (192.168.1.2)

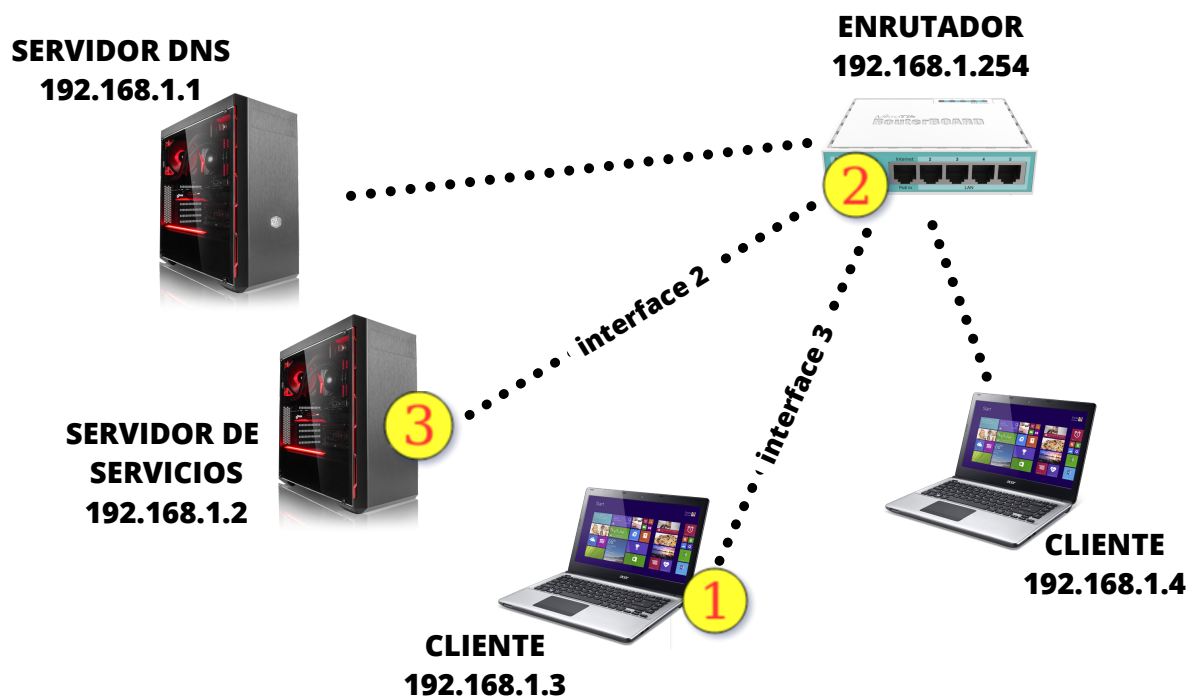
Ahora sí!, nuestra computadora ya conoce a qué IP corresponde videos.net y procederá a comunicarse con ella para conseguir ese último capítulo de la telenovela que todas hablan. Para ello, básicamente vamos a repetir el proceso que acabamos de realizar.

¿QUÉ SON LAS RUTAS?

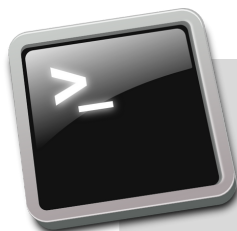
Las interfaces que toman los paquetes para llegar de su origen a destino a través de la red, se le conoce como ruta. En linux puedes consultar las rutas de una IP o DNS escribiendo: **tracert ejemplo.org**



Continuemos con el ejemplo. Ahora la computadora cliente establecerá conexión con el servidor de videos para tener acceso al material audiovisual.



- 1 El cliente 192.168.1.3 enviará paquetes de datos a la puerta de enlace de la red 192.168.1.254, es decir el enrutador, con destino a la plataforma de videos identificada con la IP 192.168.1.2 solicitando el video en cuestión.
- 2 El enrutador, tomará esos paquetes y como conoce la ruta (interface) de la IP de destino, los redirigirá a la interface correspondiente, en este caso la interface 2.
- 3 En este punto, el servidor de videos recibe desde la puerta de enlace paquetes de datos del cliente 192.168.1.3 solicitando el último capítulo de la telenovela de moda



CONOCE TU HARDWARE DE RED

Escribe en tu terminal **lspci** para obtener información breve y detallada sobre los distintos dispositivos con que cuenta tu computadora. Fíjate en Network y Ethernet Adapter

Finalmente, siguiendo nuestro ejemplo, corresponde al servidor responder al cliente y el proceso se repite nuevamente a la inversa:

4

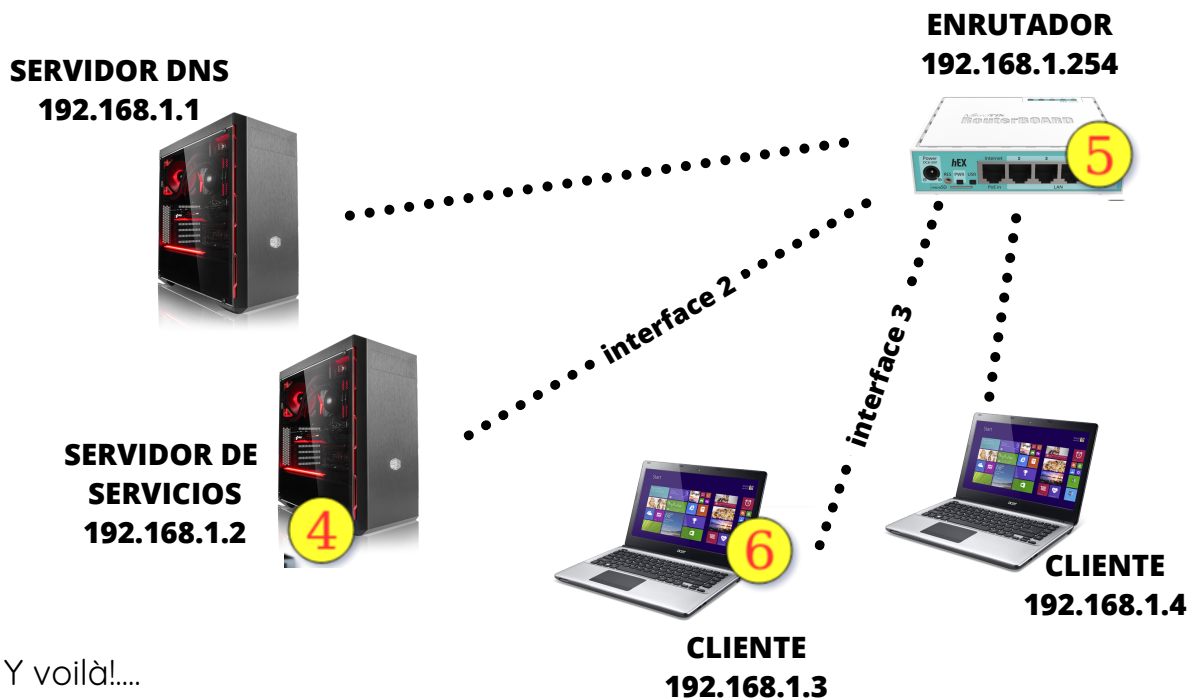
El servidor 192.168.1.2 enviará paquetes de datos que contienen la telenovela a la puerta de enlace de la red 192.168.1.254, es decir el enrutador, con destino al cliente identificado con la IP 192.168.1.3

5

El enrutador, tomará esos paquetes y como conoce la ruta (interface) de la IP de destino, los redirigirá a la interface correspondiente, en este caso la interface 3.

6

En este punto, el cliente recibe desde la puerta de enlace paquetes de datos que provienen del servidor 192.168.1.2 con el último capítulo de la telenovela de moda... a disfrutar!!!



Y voilà!...

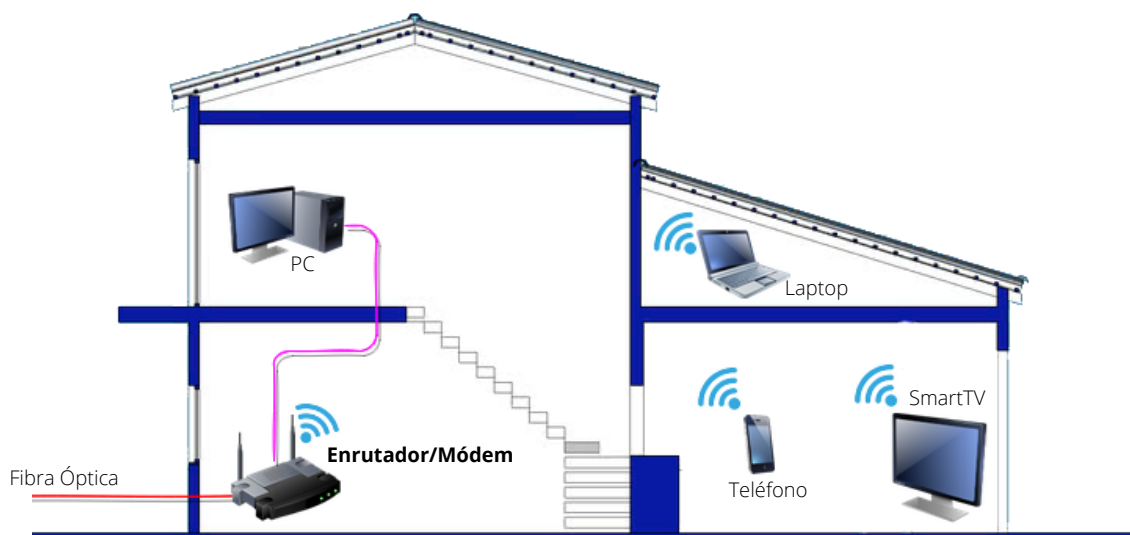
Lo que tenemos ante nosotras es lo que se conoce como una **red de área local o LAN** (Local Area Network, en inglés). Es decir una red de computadoras como tal, funcionando correctamente. La única diferencia, es que todo esto sucede en fracciones de segundo, esto que nos tomó a nosotras humanas un momento, para las computadoras y gracias al lenguaje binario todas estas acciones son casi instantáneas.

RED LAN

Una red LAN puede abarcar un área reducida de una casa, una oficina, un edificio empresarial completo o todo un pueblo. Las redes LAN son la unidad básica de toda red y también de Internet, porque en realidad internet son muchas redes LAN interconectadas, pero no nos adelantemos.

Revisemos ahora algo muy familiar, una pequeña red LAN de casa, tal como podemos encontrarla en muchos hogares actualmente. Para ello nos valdremos de un equipo multifuncional, que cumplirá varios roles al mismo tiempo en la red.

En el ejemplo que estamos revisando, llamamos **enrutador/módem** a un hardware que en realidad cumple prácticamente todas las funciones necesarias para correr una red, no solo trabaja como un servidor DHCP.



En la imagen vemos que el "enrutador" cumple con las siguientes funciones:

- 1) **Hardware Concentrador:** Gracias a que tiene interfaces Wi-Fi y Ethernet, pueden conectarse a él inalámbricamente un teléfono, una laptop y una smarttv. Por cable ethernet tenemos una computadora de escritorio (PC) conectada.
- 2) **Módem:** Recibe la conexión de alta velocidad de fibra óptica y la convierte a ethernet o Wi-Fi.
- 3) **Puerta de Enlace:** Posee un Servidor DHCP y es el encargado de realizar el direccionamiento IP de la red.
- 4) **Servidor DNS:** El equipo asume también esta tarea en este tipo de redes.
- 5) **Punto de Acceso Inalámbrico:** Posee una tarjeta de red inalámbrica con la que difunde una red para que distintos dispositivos se conecten.

¡Pero falta algo! ¡en esta red LAN no hay servidores de servicios!....

Así es, para que una red LAN funcione como tal no es necesario contar con un servidor de servicios. Entonces si una red LAN no tiene servicios, ¿para qué sirve?

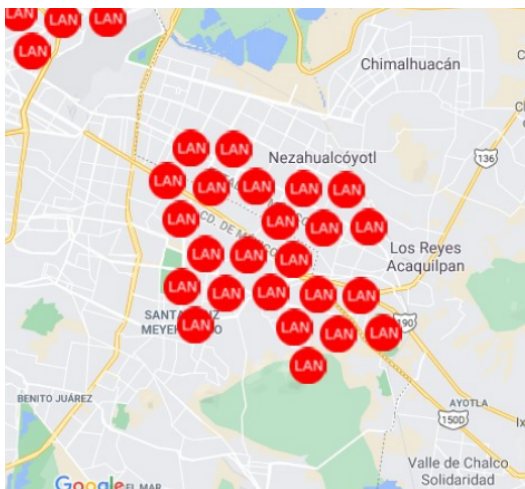
Las redes LAN de casa nos sirven para conectarnos a otros servidores de servicios que están muy lejos, en otras redes LAN de otros países, esto es lo que conocemos como **INTERNET**.

Detengámonos un momento y recordemos que una de las características principales de un enrutador es su capacidad de participar de dos redes al mismo tiempo, es decir crear y administrar una red y simultáneamente ser **cliente** de otra red distinta.

RED WAN

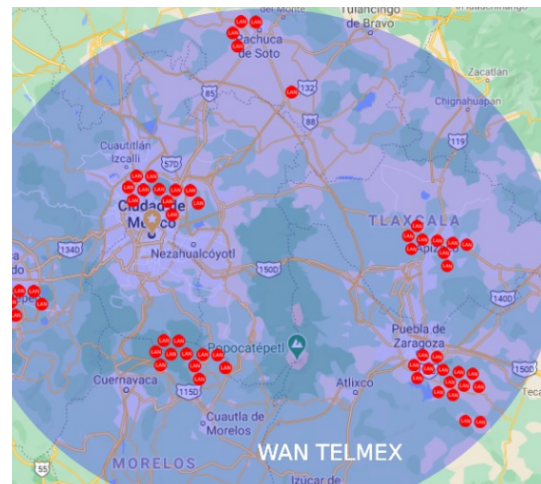
Esta red a la que se conecta el enrutador, y de la cual no es más que un simple cliente, se le conoce como una WAN (del inglés Wide Area Network, o red de área amplia). En una red WAN existe un servidor DHCP, Servidores DNS, Máscara de Red y todas las mismas características de una red LAN; la diferencia, es que **TODO**s los clientes de una red WAN son enrutadores que a su vez administran pequeñas redes LAN.

Las redes WAN son administradas y gestionadas por los ISP (del inglés Internet Service Provider, o Proveedor de Servicios de Internet). Los ISP es el nombre técnico con que se conoce a las empresas de telecomunicaciones que venden los servicios de internet en los distintos países y territorios. Por lo general cada ISP cuenta con su propia infraestructura de red que les permite brindar este servicio.



Muchas redes LAN conforman una red WAN. Por lo general las redes WAN están bajo la administración de una empresa privada (ISP)

Toda conexión de casa o comercial es una red LAN. En una ciudad hay tantas redes LAN como casas, edificios y fábricas cuentan con internet contratado.



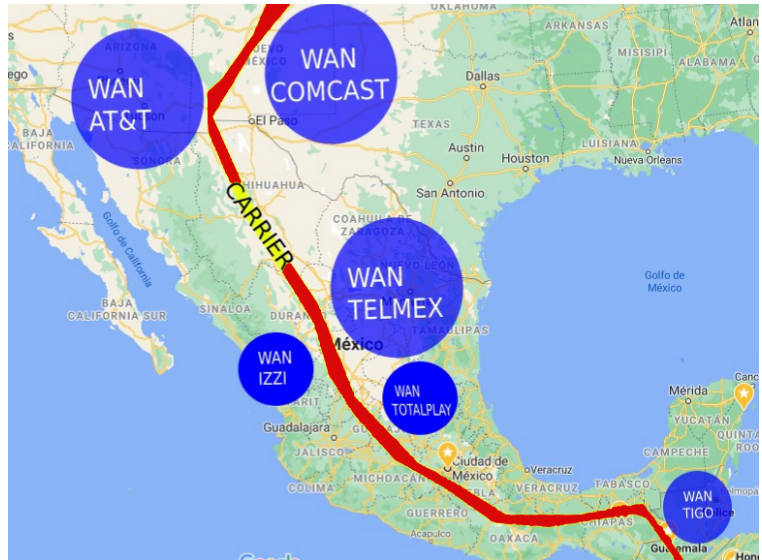
ISP

El ISP (siglas en inglés de Internet Service Provider), es el Proveedor de Servicios de Internet, es decir, la **empresa** que vende a los usuarios la conexión a Internet.

Entonces nuestra red LAN de casa, está conectada a una red WAN que es gestionada y administrada por el ISP que hemos contratado. Esta característica permite interconectar dos redes a través del enrutador, que actúa como un puente entre ambas.

RED GAN

Las redes WAN a su vez se conectan a una red GAN (Global Area Network, Red de Área Global en castellano) que es una red administrada y gestionada por los CARRIERS, grandes empresas internacionales de comunicaciones, que interconectan países y continentes con cables submarinos.



Los CARRIERS trabajan de manera coordinada de tal manera que a cada ISP se le entrega un rango de direcciones IP concreto para que reparta a sus clientes. Si un ISP quiere brindar acceso a sus usuarios al Internet global están obligadas a contratar el servicio de un CARRIER.

Hasta hace unos años, toda la internet estaba corriendo sobre los cables de teléfono (ADSL), una infraestructura que jamás fue pensada para redes de computadora. Actualmente las redes GAN están construidas con fibra óptica y ya en la mayoría de los países de latinoamerica los ISP están invirtiendo dinero para que sus redes WAN también cuenten con esta tecnología. Es importante señalar que las redes de computadoras funcionan de la misma forma sin importar si corren sobre fibra óptica o cables ethernet.

ENMASCARAMIENTO

Ha sido un trabajo arduo y ya casi llegamos al final... pero aún nos falta un último concepto para poder comprender cómo funcionan las redes de computadoras y el internet, nos referimos al Enmascaramiento o NAT (del inglés Network Address Translation).

Sabemos que en el protocolo TCP/IP, la información viaja encapsulada en paquetes de datos, y cada paquete de datos lleva una firma. Esa firma hace referencia a los números IP del dispositivo que inicia la comunicación y el destinatario de la misma. Si lo imaginamos es muy similar a cuando en una carta uno escribe el destinatario y el remitente.

Como acabamos de mencionar, un enrutador tiene la capacidad de participar en varias redes de manera simultánea, ya sea como cliente o puerta de enlace. Esto permite que dos redes puedan conectarse y que los enrutadores intercambien paquetes entre redes que asignan direcciones IP o rangos de red incompatibles.

Cada vez que estos paquetes de datos pasan por un enrutador con destino a una red distinta de la que se originan, el enrutador realiza el enmascaramiento. El enrutador reemplaza la dirección IP de origen por la propia, de tal manera que esos paquetes sean válidos en la nueva red. Por así decirlo el enrutador, le "presta" su IP a tu comunicación para que sea válida. Una vez que los paquetes enmascarados vuelven, el enrutador sabe de dónde se originaron y los envía correctamente.

Internet en sus inicios no fue pensado para ser una red tan extensa, por ese motivo el protocolo IPv4 solo puede entregar 4.294.967.296 direcciones únicas, pero el hecho es que el número de máquinas conectadas a Internet aumentó exponencialmente y las direcciones IP se agotaban. Por ello surgió el enmascarado o NAT.

Gracias a este "parche", las grandes empresas sólo utilizarían una dirección IP y no tantas como máquinas hubiese en dicha empresa. También se utiliza para conectar redes domésticas a Internet.

WLAN

WLAN son las siglas de Wireless Local Area Network, es decir, red de área local Inalámbrica. Una Lan inalámbrica se comporta de manera similar a una red LAN cableada. La diferencia está en que no hay cables si no conexiones de radiofrecuencia.

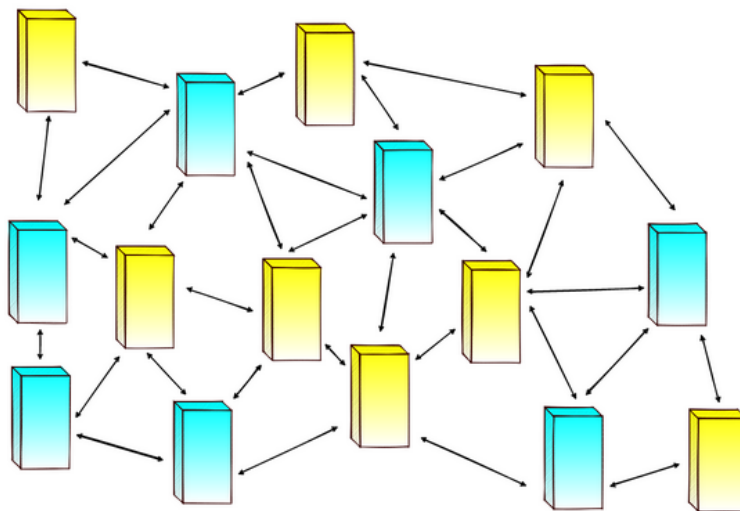
INTERNET

Pero dónde y qué es internet. Para responder esa pregunta, nos vamos a imaginar por un momento que queremos visitar Google.com

Para navegar en algún sitio web colocamos su dominio en la barra de direcciones del navegador y damos enter. Lo que sucede en ese momento es que la computadora se comunica con la IP que tiene registrada como servidor DNS y le pregunta a cuál IP corresponde el dominio que queremos visitar; el servidor DNS revisa la información que tiene almacenada y responde con la IP correspondiente al dominio.

Por lo general en una red LAN de casa, es el mismo enrutador el que aparece como servidor DNS de la red, en realidad no es que nuestro enrutador posea un listado con todas las direcciones web de internet, si no que cuando recibe una consulta DNS, el enrutador consulta a su vez a alguno de los servidores DNS que existen en la red WAN y que mantiene el ISP o alguno de los que existen en la red GAN.

Una vez obtenida la dirección IP correspondiente a Google.com, nuestra computadora cliente comenzará a enviar paquetes de datos hacia esa dirección IP.



Internet es un entramado de computadoras, todo Internet son computadoras, Google, Facebook o Netflix, también son computadoras con una dirección de IP asignada.

¿Simple no?

Internet son millones de computadoras interconectadas entre sí alrededor del mundo. Cuando visitamos un sitio web o revisamos nuestros correos, en realidad nuestra computadora se está conectando a otra computadora que se encuentra físicamente en algún lugar del planeta con una dirección de IP asignada. De ella obtenemos la información almacenada en su disco duro. Esta información puede ser una página web, un video, un correo electrónico o cualquier otro tipo de datos.

Cuando navegas en Facebook, Google, Netflix o Amazon, realmente estás accediendo a los discos duros propiedad de esas empresas, y con ello mucha de tu información personal queda bajo su resguardo. En plataformas como Youtube al subir videos, es esta empresa la que se hace dueña de ese material ya que en el contrato de usuario al crear una cuenta en sus servidores así lo estipula. Por ello es fundamental para fortalecer nuestras libertades que existan alternativas a las grandes empresas de comunicación digital. Tu comunidad organizada podría ser una de esas alternativas.

SERVIDORES DNS

Su ISP le asignará servidores DNS cada vez que se conecte a Internet, pero es posible acceder a otros servidor DNS que existen en internet. Existen servidores DNS públicos y privados, y cada uno de ellos tienen características distintas. Puedes acceder a un listado de ellos, con el código QR



K. RECAPITULEMOS

Elementos básicos de una red de computadoras

Comúnmente una red informática contiene los siguientes elementos:

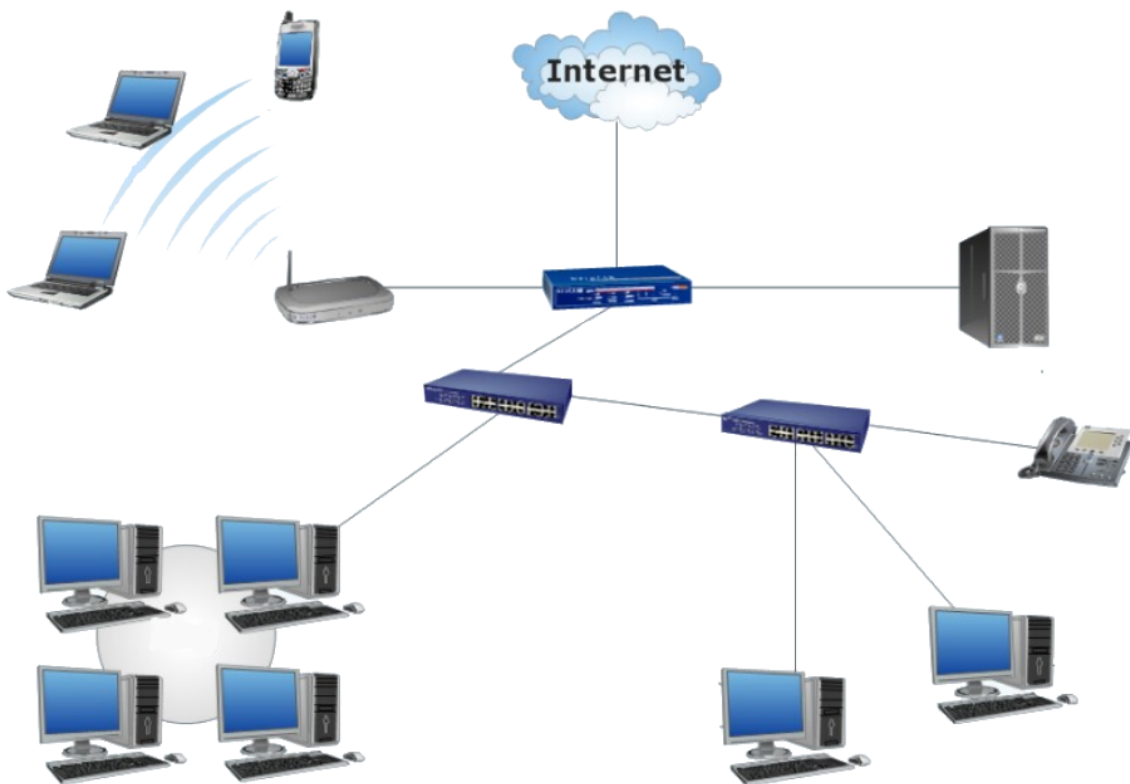
- **Servidor.** Los servidores son los encargados de procesar el flujo de datos de la red, atendiendo a todas las demás computadoras conectadas (es decir, “sirviéndolos”) y centralizando el control de la red en sí misma. Existen varios tipos de servidores, los principales son:
 - Servidor DHCP
 - Servidor DNS
 - Servidor de Servicios
- **Clientes o estaciones de trabajo.** Estas son las computadoras que forman parte de la red y pero no brindan servicio alguno, su función es solicitar los recursos disponibles en la red.
- **Medios de transmisión.** Se refiere al cableado, a las ondas electromagnéticas del Wi-Fi, o al medio físico que permita la transmisión de la información de la red, sea cual sea.
- **Elementos de hardware.** Todas las piezas tecnológicas que habilitan el establecimiento físico de una red, o sea, que la permiten. Hablamos de tarjetas de red, módems y enrutadores, o antenas repetidoras que extienden la conexión inalámbricamente.
- **Elementos de software.** Similarmente, se requiere de programas para administrar y poner en funcionamiento el hardware de comunicaciones de cada estación de trabajo. Esto incluye el sistema operativo de los enrutadores (Firmware), como también el software que gestiona las redes, como el Firewall, DHCP y los protocolos Ethernet, TCP/IP y Wi-Fi.

EJERCICIO

El esquema a continuación representa a una red LAN de una oficina. Cuenta con:

- 1 enrutador
- 1 servidor de servicios
- 2 switch
- 1 punto de acceso inalámbrico
- 10 clientes

¿Podrías reconocer cuál equipo es cuál? escribe sus nombres sobre la imagen.



L. LECTURA COMPLEMENTARIA

Texto original de **COMPPA**. Sembrando Voces: Manual Teórico Avanzado, revísalo completo en el código QR



Hoy en día el manejo de dispositivos digitales como teléfonos, computadoras o la conexión a Internet es parte cotidiana de nuestras actividades, nos facilitan la elaboración y publicación de contenidos, al igual que la difusión de información de manera inmediata. Internet nos permite acceder de manera rápida a canciones y producciones radiofónicas, encontrar noticias de otros medios de comunicación e interactuar a través de chats y redes sociales.

Internet es una “red de redes” que enlaza computadoras en todo el mundo. Si vemos Internet de esta manera, como una infraestructura y un conjunto de páginas web y aplicaciones, no podemos decir que es un bien común, porque esta infraestructura está gestionada y controlada por empresas y gobiernos. Internet es una red de conexiones, como carreteras de datos que se cruzan y conectan en ciertos puntos. Los nodos de conexión clave por los cuales pasa la mayoría del tráfico de datos son los servidores raíces de internet.

“Según la Comisión Económica para Latinoamérica y el Caribe (Cepal), nuestra región es la más dependiente de los EE.UU. en términos del tráfico de Internet. El 80% de la información electrónica de la región pasa por algún nodo administrado directa o indirectamente por Estados Unidos, fundamentalmente por el llamado “NAP de las Américas”, en Miami -el doble que Asia y cuatro veces el porcentaje de Europa-, y se calcula que entre un 70 y 80% de los datos que intercambian internamente los países latinoamericanos y caribeños también van a ciudades estadounidenses; donde se ubican 10 de los 13 servidores raíces que conforman el código maestro de Internet”.

Elizalde, Rosa Miriam. Colonialismo 2.0 en América Latina y el Caribe: ¿Qué hacer?

"Sin embargo, lo que construye Internet no es únicamente su materialidad, sino sus habitantes. Pensar internet como un bien común significa que es producto de una comunidad que genera valor gracias a sus interacciones, a su capacidad de creación colectiva y a los lazos afectivos que teje: algo que construimos entre todas y de lo que nadie puede apropiarse. Por esta razón, hoy que Internet se encuentra amenazada por el control de las corporaciones y los Estados, debemos defender nuestro derecho a una red descentralizada, libre, abierta y neutral a la que todo ser humano tenga acceso, sin restricciones. Debemos defender Internet como un espacio para ejercer nuestras libertades. Internet no debe ser el espacio para el control de los individuos y del territorio, como ocurre en la actualidad. No es posible hablar de democracia si Internet no es libre.

"Sursiendo. "Entrevista a Paola Ricaurte" en ¿Es Internet un bien común?

Internet se ha vuelto un campo de batalla en la guerra de la información. Por un lado causa una sensación de democratización porque todos podemos ser comunicadorxs, pero también genera poderosas herramientas de manipulación. Las redes sociales son espacios donde se construye realidades paralelas. Hay empresas que se especializan en abrir páginas web o perfiles falsos en las redes sociales para difundir mensajes en favor de los gobiernos, o en contra de los movimientos sociales. En 2019 Facebook cerró 181 cuentas y 1488 páginas en Honduras que eran fraudulentas, dedicándose a comentar y amplificar mensajes positivos sobre el presidente Juan Orlando Hernández. El poder de dirigir mensajes específicos a un público seleccionado, convencerlo y manipularlo, hizo de Internet una de las herramientas más importantes en la manipulación de la opinión pública.

EL EXTRACTIVISMO DE DATOS

Una de las bases para esta manipulación es la recopilación masiva de datos sobre nosotrxs. Empresas como Google o Facebook son de las que más ganan en el mundo, aunque no cobran por usar sus servicios. ¿De dónde viene el dinero? ¿Cuál es el producto que venden?

Nosotrxs somos el producto que venden, más en detalle, nuestros datos personales y nuestra privacidad. Cada vez que usamos sus servicios estas empresas guardan la información que publicamos o que buscamos, de dónde nos conectamos y a qué hora. Saben qué música y qué comida nos gusta, dónde pasamos nuestro tiempo libre, con cuáles de nuestrxs amigxs nos comunicamos más y sobre qué temas.

LA SELECCIÓN DE INFORMACIÓN

La información que vemos en los anuncios en el Internet no es casual, hay programas (algoritmos) que usan la información sobre nosotros para seleccionar los productos e informaciones que nos pueden interesar. Por ejemplo, si buscamos varias veces ofertas de zapatos es muy probable que, con el tiempo, se nos aparezcan más anuncios de zapatos. Si en Youtube escuchamos sólo música de marimba, el mismo algoritmo nos propondrá más música de marimba.

¿Y por qué ver información y ofertas que nos interesan sería malo? Tendremos que entender que no únicamente se trata de vendernos zapatos. Nuestros datos se usan para estudiar y analizar nuestros comportamientos, qué es lo que nos interesa y nos gusta. Con base en estos datos recopilados se elaboran mensajes y campañas que responden específicamente a nuestros intereses. Cada vez más se están afinando los algoritmos y la recopilación de datos, estos son utilizados por empresas multinacionales, gobiernos, servicios de inteligencia o partidos políticos, no sólo para vendernos zapatos sino también para campañas políticas o ataques en contra de movimientos sociales.

Recordemos que las informaciones y sus marcos influyen en cómo percibimos el mundo en que vivimos. Si los algoritmos eligen la información que se nos presenta con base en lo que nos gusta, poco a poco viviremos en una burbuja de la realidad. Sólo veremos las cosas con las cuales nos sentimos cómodos y compartiremos opiniones con quienes piensan igual o semejante a nosotros. Con nuestros datos, no solamente se puede definir cuáles productos de consumo ofrecernos para que nos agraden más, sino también se pueden elegir las opiniones políticas para que estas sean perfectamente ajustadas a nuestro gusto. Esta práctica no es nefasta sólo porque nos roba nuestra privacidad, sino también porque nos quita la posibilidad de conocer, reflexionar y razonar con personas que tienen diferentes opiniones. Confrontarnos con saberes distintos es fundamental para el aprendizaje y el desarrollo humano, así como para una sociedad democrática, incluyente y participativa.



Queremos agradecer a todas quienes compartieron sus conocimientos a lo largo del camino andado, quienes con amor y paciencia nos abrieron sus experiencias y aprendizajes en el hacer de la comunicación comunitaria para la defensa del territorio.

A la comunidad de San Francisco Xochiteopan, a Estéreo Lluvia y Cultural Survival por la confianza para navegar con nosotras aventurosas aguas desconocidas.

a Fauno y toda la raza de SUTTY, a RadiosLibres.net y la comunidad de Libera Tu Radio, a Juan Manuel Ledón y Jessica y a todas las que nos apoyaron en los momentos difíciles.

GRACIAS



**NO ODIAS A LOS MEDIOS,
SIÉMBRALOS LIBRES**

Ante la creciente centralización, privatización y uso no consentido de nuestra data personal en internet, creemos fundamental comenzar a cuestionarnos la propiedad de las plataformas e infraestructuras que actualmente sostienen nuestras comunicaciones digitales. Para ello ponemos a disposición este segundo cuadernillo de la Biblioteca Popular de Cultura Libre, dónde se compilan en un lenguaje sencillo conocimientos sobre redes de computadoras.

