

En este módulo se verá:

1. Medios guiados y no guiados.
2. Cables de par trenzado.
3. Ancho de banda y velocidad de transmisión.
4. Segmentos como los *backbone*.
5. Ancho de banda por segmento de red.

Medios

Los **medios** o “**medios de transmisión**” son las vías físicas por donde se transportan las tramas, según el modelo OSI corresponde a la capa 1 (física).

Lo que se vuelca al medio, es decir, lo que el medio transporta son **señales físicas** y según el tipo de señal los medios se pueden clasificar en dos grandes grupos:

Medios de transmisión guiados o alámbricos.

Medios de transmisión no guiados o inalámbricos.

Las tecnologías actuales de transmisión usan ondas electromagnéticas, pulsos eléctricos o pulsos de luz.

En el caso de los **medios guiados** los datos se conducen a través de cables o “alambres” en el caso de pulsos eléctricos y cables de fibra que guían los pulsos de luz.

En los **medios inalámbricos**, se utiliza el aire como medio de transmisión, a través de radiofrecuencias, microondas y luz (infrarrojos, láser); por ejemplo: puerto IrDA (*Infrared Data Association*), Bluetooth o Wi-Fi.

Según el sentido de la transmisión, existen tres tipos diferentes de medios de transmisión:

Simplex.

Semi-duplex (half-duplex).

Duplex o duplex completo (full-duplex).

Otra característica importante de cualquier medio de transmisión es el ancho de banda que es la cantidad de información que puede transportar y la velocidad de transmisión.

Señalización

La información se representa generando señales mediante la variación de voltaje, intensidad lumínica u ondas de radio que se vuelcan en un medio que pueda transportar o conducir dicha señal.

En dispositivos electrónicos (televisores, relojes, teléfonos, computadoras, etc) se utiliza el sistema binario para representar información, es decir bits, que pueden ser 1 y 0 y estos valores se representan físicamente con pulsos eléctricos:

3 Voltios = 0

5 Voltios = 1

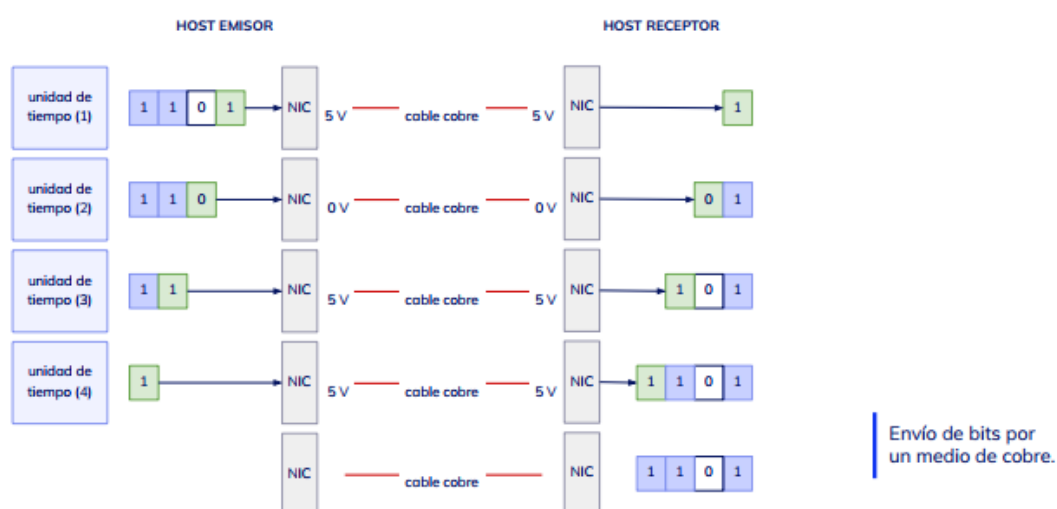
Este ejemplo no es totalmente representativo, en determinados contextos se representa el 0 con 0 Voltios y el 1 con voltajes mayores a 2, además que estamos excluyendo las ondas de radio y los pulsos lumínicos.

Enviando bits

En redes es la **interfaz de red** la que se encarga de tomar una trama (secuencia de bits) y generar el tipo de señal correspondiente para representar los bits de dicha trama.

Pongamos el siguiente ejemplo, imaginemos una trama de 4 bits, en una unidad de tiempo (1) se envía una corriente eléctrica por un cable de cobre, luego en otra unidad de tiempo (2) no se envía nada, en la siguiente unidad (3) se envía una señal eléctrica y lo mismo en la última unidad (4), por cada bit en 1 se envían 5 voltios por el cable, cuando el bit está en 0 no se envía ninguna señal, es decir 0 voltios.

Esta intermitencia se conoce como “**pulso**”. Un buen ejemplo de ello es el código morse, una secuencia de pulsos y pausas representan letras del alfabeto, en este caso un pulso sostenido por una cantidad dada de tiempo representa un bit en 1, la ausencia sostenida por una unidad de tiempo representa un 0, la interfaz de red receptora interpreta los bits del mismo modo, detecta el estado “encendido” o “apagado” del pin receptor por unidades de tiempo y construye la trama en función de estos estados.



Señales digitales

Las **señales digitales** son señales discretas que tienen **valores finitos** y en sistemas binarios los valores son “**Up**” (1 binario) y “**Down**” (0 binario).

También se los llama estados de encendido y apagado. La representación gráfica de una señal digital se muestra de la siguiente manera:



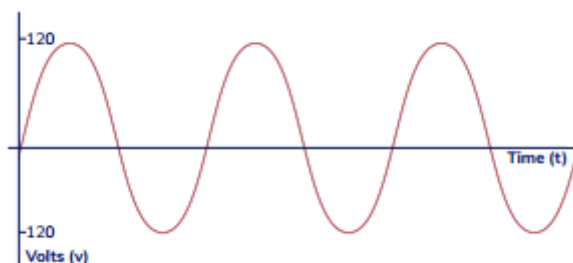
Lo que representa la gráfica de la slide anterior es una **onda cuadrada** que varía entre **dos puntos** y no toma ningún otro valor intermedio.

Una señal binaria que sólo puede tomar un valor de 1 o 0 es un ejemplo perfecto de señales digitales. En este caso son pulsos eléctricos, pero bajo el mismo principio podríamos representar la misma información con pulsos lumínicos, la intensidad medida de la luz recibida se puede interpretar como un estado *Up* o *Down*, o encendido o apagado que representa los 1 y 0 respectivamente en el sistema binario.

Señales analógicas

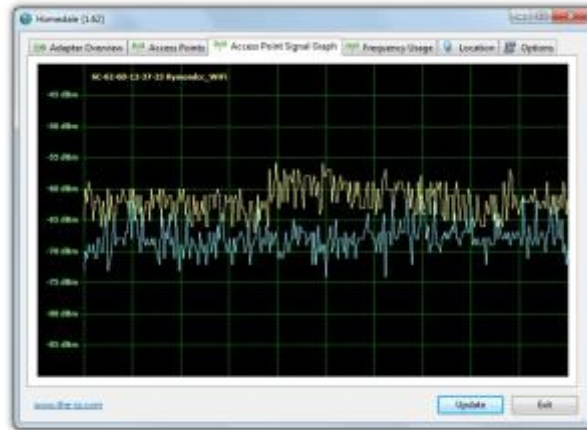
En las **señales analógicas** las variaciones de voltaje, onda electromagnética, intensidad lumínica o cualquier otro fenómeno físico medible tienen **valores distintos** de forma continua entre sus puntos más altos y más bajos.

En el caso de las señales digitales se representan como ondas cuadradas, en este caso se definen como **ondas senoidales**.



Las ondas que se generan cuando se arroja una piedra al agua, la voz humana y las ondas de radio se describen como señales de onda senoidal, pero hablando estrictamente en el ámbito de redes, encontramos que la información se transmite no mediante pulsos sino en forma de señales analógicas en el caso de la transmisión inalámbrica por ondas de radio, es decir, WiFi.

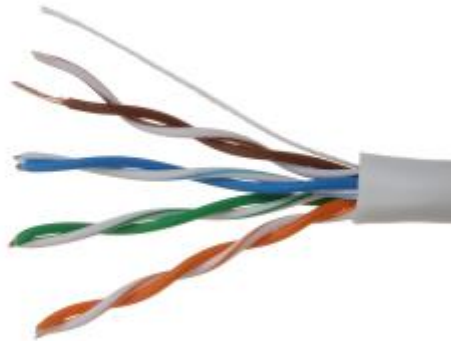
Si bien en la gráfica anterior muestra una señal continua y predecible, en la realidad estas señales varían en función de la información que se quiere representar, por ejemplo, la siguiente imagen muestra una gráfica de las señales enviadas y recibidas en un dispositivo inalámbrico.



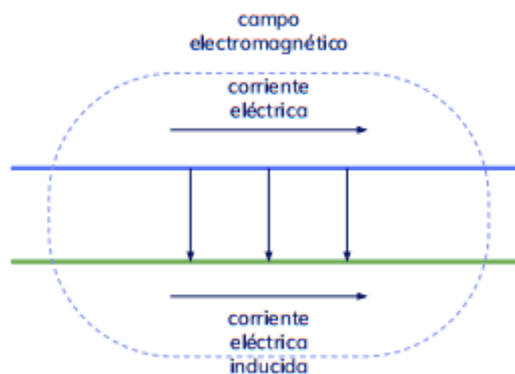
Cable de par trenzado UTP

El **cable de par trenzado** es el tipo de cable más utilizado en redes LAN y está tipificado en el estándar Ethernet.

Se trata de pares de hilos trenzados de manera **helicoidal**, estos hilos están hechos de aleaciones de **cobre** o **aluminio** y **conducen corrientes eléctricas**.



Cuando pasa una corriente eléctrica por un conductor se genera un campo electromagnético, este campo puede inducir una corriente en otros conductores que estén dentro del área de interferencia, de hecho este fenómeno se denomina “**inducción**” y es el principio de funcionamiento de los transformadores eléctricos.



En el caso de los medios de cobre para transmisión de datos esto representa un problema, los hilos conducen electricidad y pueden interferir las señales de los hilos circundantes provocando ruidos y la corrupción de la información.

Cuando se entrelazan los alambres de forma helicoidal, las ondas de los campos electromagnéticos se cancelan, por lo que la interferencia producida por los mismos es reducida lo que permite una mejor transmisión de datos.

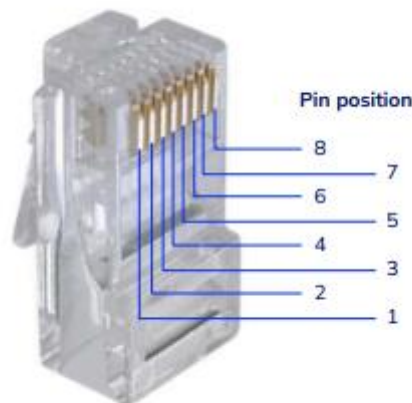
El cable de par trenzado utilizado en redes de datos es el **cable UTP** que se caracteriza por tener **4 pares de cables** señalizados bajo un **código de colores estandarizados**.

De estos 4 pares un par se utiliza para el envío de datos y otro par para la recepción de datos, quedando dos pares libres para otros usos.

Conectores en cables UTP

RJ45 es una interfaz física comúnmente utilizada para conectar redes de computadoras con cableado estructurado. Posee ocho pines o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado (UTP).

Es utilizada comúnmente con estándares como **TIA/EIA-568-B** o **TIA/EIA-568-A**, que define la disposición de los pines o wiring pinout según el código de colores bajo las normas TIA/EIA-568-B o TIA/EIA-568-A.



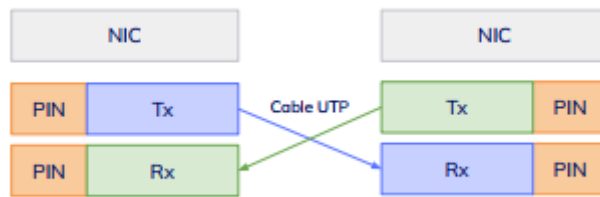
Normas y códigos de colores

Cuando hablamos de vías de comunicación tenemos que identificar los **roles** de estas vías o canales. Un canal es para el envío de datos mientras que el otro canal es para la recepción y en sistemas electrónicos se denominan de la siguiente manera:

Rx: receiver o receptor de señales.

Tx: transmitter o transmisor de señales.

En el cable de par trenzado se usan un par para enviar señales (Tx) y otro par para recibir señales (Rx), tanto en la interfaz de red como en los pines del conector existe una relación con los pares para enviar y recibir señales.



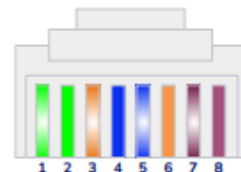
El pin de emisión de señal de una interfaz de red se vincula con el pin de recepción de señal de la interfaz de red de destino, el conexionado de los pines se realiza bajo las normas TIA/EIA-568-B y TIA/EIA-568-A.

Esta disposición en canales para enviar y recibir señales de manera bidireccional y en simultáneo es lo que se conoce como comunicación Full Duplex.

En tecnologías obsoletas, como las topologías físicas de bus con cable coaxial o topologías con cable de par trenzado y hubs la comunicación era Half Duplex, de todos modos aún se utiliza la comunicación Half Duplex, por ejemplo, la conexión del módem de un cliente a la red del ISP se hace mediante cables de coaxiales que solo tienen un canal de comunicación, es decir, un solo hilo de cobre.

Norma TIA/EIA-568-A

PIN	COLOR	PAR	FUNCION
1	Blanco Verde	3	RD +
2	Verde	3	RD -
3	Blanco Naranja	2	TD +
4	Azul	1	Ninguna
5	Blanco Azul	1	Ninguna
6	Naranja	2	TD -
7	Blanco Marrón	4	Ninguna
8	Marrón	4	Ninguna

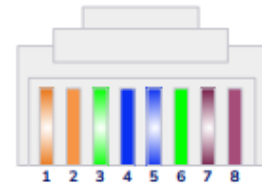


TD: Transmisión de Datos

RD: Recepción de Datos

Norma TIA/EIA-568-B

PIN	COLOR	PAR	FUNCION
1	Blanco Naranja	3	TD +
2	Naranja	3	TD -
3	Blanco Verde	2	RD +
4	Azul	1	Ninguna
5	Blanco Azul	1	Ninguna
6	Verde	2	RD -
7	Blanco Marrón	4	Ninguna
8	Marrón	4	Ninguna



TD: Transmisión de Datos

RD: Recepción de Datos

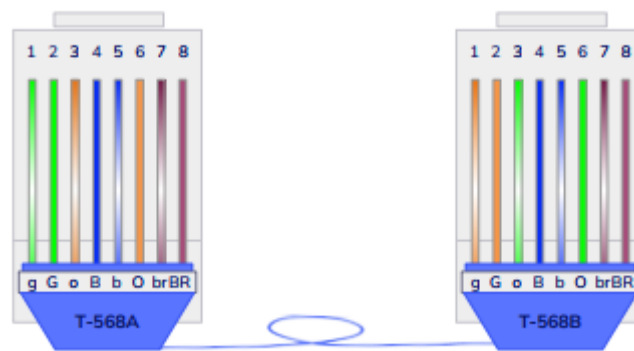
Armado de cables: recto y cruzado

Cuando se arma un cable o se compra ya armado se indica el tipo de armado según la norma usada.

Cable recto: usa la misma norma en ambos extremos, ya sea A o B.



Cable cruzado o crossover: usa normas distintas en cada extremo.



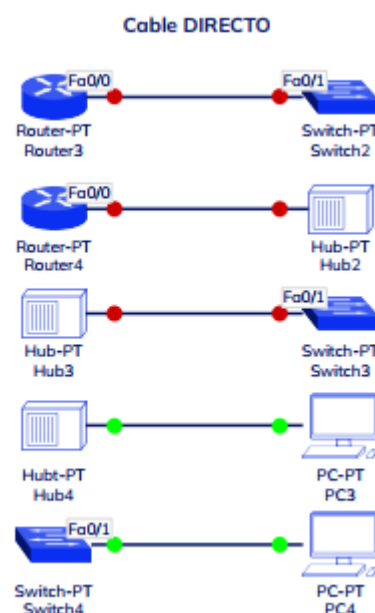
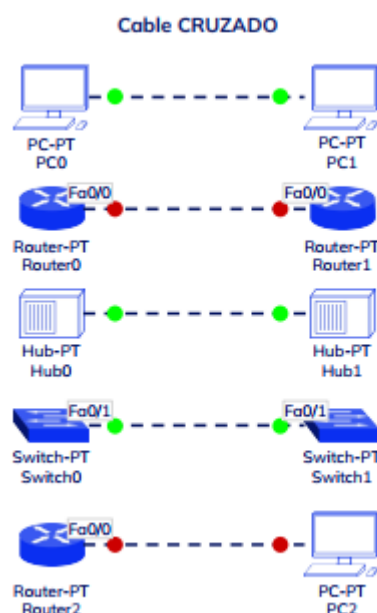
Determinación del tipo de cable

La pregunta es *¿cuándo usar un cable cruzado y un cable recto?* La regla dice que para **dispositivos de igual capa lleva cable cruzado, mientras que dispositivos de capas distintas lleva cable recto**. Veamos esta relación mediante una tabla:

Tipo de cable	Dispositivo A	Capa	Dispositivo B	Capa
Recto	NIC	3	SWITCH	2
Cruzado	Router	3	PC (nic)	3
Recto	SWITCH	2	PC (nic)	3

Veremos un ejemplo del uso de distintos tipos de cables según dispositivos.

Recordemos que estamos hablando de estándar Ethernet, no importa si es una pc, una impresora o un router, todos usan NICs, por lo tanto son dispositivos de capa 3, mientras que un switch es de capa 2 y el ya obsoleto hub es de capa 1 según el modelo OSI.



Categorías de cable UTP y velocidades

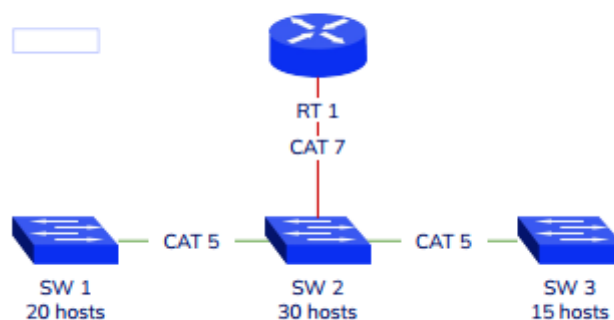
El estándar Ethernet define las tecnologías y las velocidades de transmisión, en el caso del cable UTP existen categorías que definen un ancho de banda y/o velocidad de transferencia para el cable, cada categoría mejora estos aspectos respecto a la categoría anterior.

Categoría	Velocidad	Frecuencia	Velocidad de de descarga
ETHERNET CAT 5	100 Mbps	100 MHz	15,5 MB/s
ETHERNET CAT 5E	1.000 Mbps	100 MHz	150,5 MB/s
ETHERNET CAT 6	1.000 Mbps	250 MHz	150,5 MB/s
ETHERNET CAT 6A	10.000 Mbps	500 MHz	1.250 MB/s ó 1,25 GB/s
ETHERNET CAT 7	10.000 Mbps	600 MHz	1,25 GB/s
ETHERNET CAT 7A	10.000 Mbps	1.000 MHz	1,25 GB/s
ETHERNET CAT 8	40.000 Mbps	2.000 MHz	5 GB/s

Es importante definir la **categoría** de cable a usar según los segmentos de red, *backbones*, conexión de host al switch, etc.

Pongamos un ejemplo:

se pueden usar categorías de menor velocidad para conectar los hosts al switch, pero es necesario usar cables de mayor categoría para conectar los switches a otros switches o routers ya que estos serán los *backbones* y llevarán la carga de datos de todo el segmento de red.



La elección de de **la categoría está relacionada al coste de implementación de la red**, los cables de mayor categoría son más costosos, sería óptimo cablear toda la red con cables de la máxima categoría, pero eso sería innecesariamente caro.

También es importante mencionar que no siempre se pueden cumplir las expectativas en relación a un segmento de red y la categoría de cable usada para el *backbone*, sencillamente no alcanza, es entonces donde la segmentación y las topologías físicas

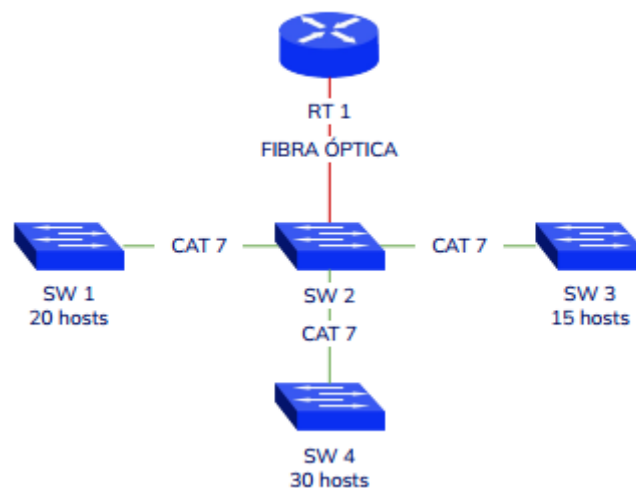
juegan un papel fundamental, segmentos chicos es igual a volúmenes de datos pequeños.

Por otra parte, hablando específicamente de *backbones*, se usan otros tipos de medios, como cables de fibra que tienen un ancho de banda mucho mayor en comparación con los cables de cobre.

Este es un switch con puertos para conexiones RJ45 y puerto para conexiones de fibra óptica.



Con él se podrían conectar segmentos de red para hosts con conexiones con cables UTP mientras que dispone de un puerto para el *backbone* de fibra.



Cables STP y FTP

Básicamente son los mismos cables que el UTP, tienen las mismas categorías y normas de conexión y usan conectores RJ45, pero incorporan otras tecnologías que permiten su uso en circunstancias particulares.

Cable STP

Shielded twisted pair (STP) o cable de par trenzado apantallado o blindado. Contiene pares trenzados rodeados cada par de una cubierta protectora hecha de aluminio. Es un tipo de cable más costoso y difícil de instalar, además usa un tipo de conector RJ45.

Esta solución sirve para **prevenir posibles interferencias y ruido externo**. Esta pantalla debe disponer de una interconexión con la toma de tierra que tenga continuidad hasta el terminal en cuestión que haga uso del cable STP.



Conector RJ45
para cable STP.

Cable FTP

Siglas de “**Foiled Twisted Pair**” o **cable de par trenzado apantallado**. En este caso tenemos un cable cuyos pares trenzados están separados entre ellos por un sistema básico basado en plástico o material no conductor. En este caso el apantallamiento no es individual, sino global que envuelve a todo el grupo de pares trenzados, y está construido de aluminio.

No cuenta con tan buenas prestaciones como los cables STP, pero si mejoran a los UTP en cuanto a distancia y aislamiento. Son muy utilizados y utilizan el conector RJ45, y el propósito de la pantalla es el mismo que en los cables STP, además utilizan conectores con recubrimiento metálico y puesta a tierra.



Cable coaxial

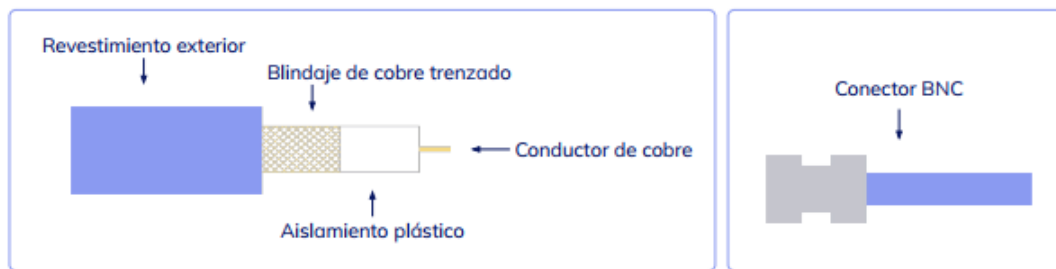
El **cable coaxial** consiste en un conductor de cobre rodeado de una capa aislante flexible. El conductor central también puede ser hecho de aluminio para una fabricación más económica, sobre el material aislante existe una malla de cobre tejida que actúa como el segundo hilo del circuito y como un blindaje para el conductor interno, así también esta capa reduce la cantidad de interferencias electromagnéticas externas.

Características:

Velocidad y tasa de transferencia de 10 a 100Mbps.

Costo económico.

Longitud máxima del cable : 500 Metros.



Estructura de un cable coaxial



Diseño de cable coaxial



Diseño y tipo de conectores

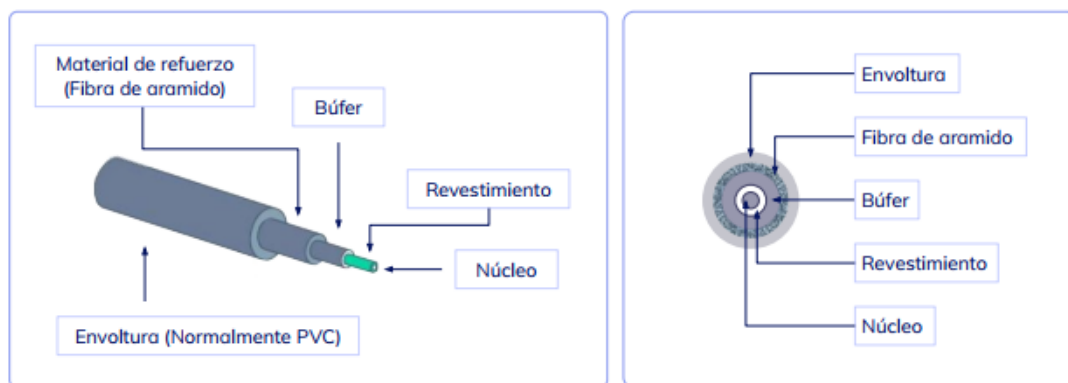
Cable de fibra óptica

El **cableado de fibra óptica** utiliza fibras de plástico o de vidrio para guiar los impulsos de luz desde el origen hacia el destino. Los bits se codifican en la fibra como **impulsos de luz**.

El cableado de fibra óptica puede generar velocidades muy superiores de ancho de banda para transmitir datos sin procesar. La mayoría de los estándares actuales de transmisión aún necesitan analizar el ancho de banda potencial de este medio.

Los cables de fibra óptica consisten en un revestimiento exterior de PVC y un conjunto de materiales de refuerzo que rodean la fibra óptica y su revestimiento. El revestimiento rodea la fibra de plástico o de vidrio y está diseñado para prevenir la pérdida de luz de la fibra.

Se requieren **dos fibras** para realizar una operación **full duplex** ya que la luz sólo puede viajar en una dirección a través de la fibra óptica. Los láseres o diodos de emisión de luz (LED) generan impulsos de luz que se utilizan para representar los datos transmitidos como bits en los medios.



Estructura de un cable de fibra óptica.

Fibra multimodo y monomodo

La **fibra óptica monomodo** transporta un sólo rayo de luz, generalmente emitido desde un láser.

Este tipo de fibra puede transmitir impulsos ópticos en distancias muy largas, ya que la luz del láser es unidireccional y viaja a través del centro de la fibra.

La **fibra óptica multimodo** a menudo utiliza emisores LED que no generan una única ola de luz coherente, la luz de un LED ingresa a la fibra multimodo en diferentes ángulos.

Los tendidos extensos de fibra pueden generar impulsos poco claros al recibirlos en el extremo receptor ya que la luz que ingresa a la fibra en diferentes ángulos requiere de distintos períodos de tiempo para viajar a través de la fibra. Este efecto, denominado dispersión modal, limita la longitud de los segmentos de fibra multimodo.



Monomodo	Multimodo
Núcleo pequeño.	Núcleo mayor que el del cable monomodo (50 micrones o mayor).
Menor dispersión.	Permite mayor dispersión y, por lo tanto, pérdida de señal.
Ideal para aplicaciones de larga distancia (hasta 100 km, 62,14 mi.).	Adecuado para aplicaciones de larga distancia pero para menores distancias que el monomodo (hasta ~2 km, 6.560 pies).
Usa láseres como fuente de luz y es comúnmente utilizado con backbones de campus, para distancias de varios miles de metros.	Usa LED como fuente de luz y es comúnmente utilizado en redes LAN o para distancias de unos doscientos metros dentro de redes de campus.

Conectores de fibra óptica

Punta Recta (ST) (comercializado por AT&T): un conector muy común estilo Bayonet, ampliamente utilizado con fibra multimodo.

Conector suscriptor (SC): conector que utiliza un mecanismo de doble efecto para asegurar la inserción positiva. Este tipo de conector se utiliza ampliamente con fibra monomodo.

Conector Lucent (LC): un conector pequeño que está adquiriendo popularidad en su uso con fibra monomodo; también admite la fibra multimodo.



Conector ST
El conector de punta recta (ST) es ampliamente usado con la fibra multimodo.



Conector SC
El conector suscriptor (SC) es ampliamente usado con la fibra monomodo.



Monomodo (LC)
Conector Lucent (LC) monomodo



Multimodo (LC)
Conector LC multimodo



Multimodo dúplex (LC)
Conector (LC) multimodo duplex

Medios de transmisión no guiados o inalámbricos

Los medios inalámbricos **transportan señales electromagnéticas** mediante frecuencias de microondas y radiofrecuencias que representan los dígitos binarios de las comunicaciones de datos. Como medio de red, el sistema inalámbrico no se limita a conductores o canaletas, como en el caso de los medios de fibra o de cobre.

El **wifi** es una tecnología que permite la interconexión inalámbrica de dispositivos electrónicos.

Los dispositivos habilitados con wifi (teléfonos, ordenadores personales, televisores, videoconsolas, reproductores multimedia, etc) pueden conectarse entre sí o a Internet a través de un punto de acceso de red inalámbrica.

Estándares

IEEE 802.11a : opera en una banda de frecuencia de 5 GHz y ofrece velocidades de hasta 54 Mbps. Posee un área de cobertura menor y es menos efectiva al penetrar estructuras edilicias ya que opera en frecuencias superiores.

Los dispositivos que operan conforme a este estándar no son interoperables con los estándares 802.11b y 802.11g descritos a continuación.

IEEE 802.11b : opera en una banda de frecuencia de 2.4 GHz y ofrece velocidades de hasta 11 Mbps. Los dispositivos que implementan este estándar tienen un mayor alcance y pueden penetrar mejor las estructuras edilicias que los dispositivos basados en 802.11a.

IEEE 802.11g : opera en una frecuencia de banda de 2.4 GHz y ofrece velocidades de hasta 54 Mbps. Los dispositivos que implementan este estándar operan en la misma radiofrecuencia y tienen un alcance de hasta 802.11b pero con un ancho de banda de 802.11a.

IEEE 802.11n : el estándar IEEE 802.11n se encuentra actualmente en desarrollo. El estándar propuesto define la frecuencia de 2.4 Ghz o 5 Ghz. La velocidad típica de transmisión de datos que se espera es de 100 Mbps a 210 Mbps con un alcance de distancia de hasta 70 metros.

Acceso al medio

Las interfaces de red inalámbricas vuelcan señales al medio (el aire) mediante el uso de **antenas**, estas tienen la capacidad de **conducir** las señales electromagnéticas y al mismo tiempo de **emitirlas**.

La capacidad de una antena de recolectar señales se mide en ganancia, la unidad de medida es el **DBi**, cuanto más ganancia tenga una antena mejor se aprovecha el ancho de banda del estándar utilizado.

No debe confundirse ganancia con potencia, este término se refiere al “volumen” de señales evocadas al medio, poniendo un ejemplo, la diferencia entre hablar y gritar.

Tipos de antenas

Existen distintos tipos de antenas para usos particulares.

Antenas omnidireccionales

Este tipo de antena pueden captar y enviar señales en todas direcciones.



Antena direccional

Este tipo de antenas se utilizan para establecer enlaces de punto a punto y a largas distancias, ya que concentra toda la energía hacia un foco, como si de una linterna se tratase.



Enlace punto a punto con antenas direccionales.

Dispositivos inalámbricos

Existen una gran cantidad de estos dispositivos según el tipo de tecnología y solución ofrecida, pero hablaremos de dos tipos en particular:

Access Point: es el dispositivo al que se conectan las interfaces inalámbricas de los dispositivos de usuario, podríamos entenderlo como un “switch” inalámbrico.

Adaptadores WiFi: como cualquier interfaz de red, pero utiliza un medio inalámbrico para enviar y recibir señales.

Adaptadores y puntos de acceso de una WLAN



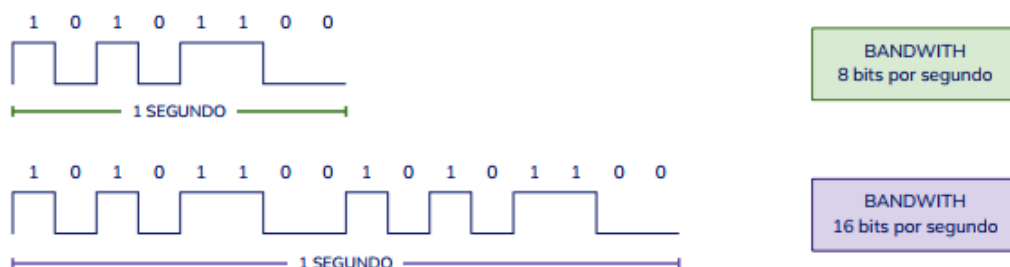
Ancho de banda

Por definición el ancho de banda es la **cantidad máxima de información** (bits) que se puede enviar a través de un medio un momento dado.

Pensemos en un caño de agua, cuanto más grande sea el diámetro del caño más cantidad de agua pasará por un período determinado. Por ejemplo un segundo, si el caño tiene un menor diámetro pasará menor cantidad de agua en el mismo tiempo.

Entonces, el ancho de banda es la **cantidad de bits que pasan por un medio en un momento dado** y esto se determina por las características físicas del medio y de los dispositivos de red.

Se puede graficar el concepto de ancho de banda del mismo modo que graficamos las señales, partamos usando señales digitales.



En un caso el ancho de banda permite el paso de un **máximo de 8 bits por segundo**, mientras que en el otro en la misma cantidad de tiempo se transporta el **doble**, es decir, **16 bits**, por lo tanto una conexión puede transportar el doble de información que la otra.

El ancho de banda **no determina** la velocidad de transferencia pero ambos conceptos están relacionados, como se detallará más adelante.

Medición de ancho de banda

En *networking* las mediciones de ancho de banda, velocidades, tasa de transferencia, etc. se hacen en **bits por segundo**, que es lo que se transporta por un medio, la unidad es el bit por segundo '**bps**'.

Es importante no confundir bits con bytes, que es una unidad de información compuesta por 8 bits:

1 byte = 8 bits

Un bit por sí mismo sólo representa 2 valores, pero un conjunto de ellos permiten representar otro tipo de valor o dato:

8 bits = 1 byte = números decimales de 0 a 256. Dirección IP = 32 bits = 4 bytes.

Los **bytes componen la información que**, por ejemplo, **hacen a un archivo**, ya sea de imagen, de audio, un documento de texto, etc.

El **bit** es la **unidad mínima** de información, lo que **compone los bytes**.

Un bit se representa con la letra 'b' mientras que un byte con 'B'.

En la siguiente tabla se muestran las unidades de bits y su representación en bytes:

Unidad	Cantidad de bits por segundo	Bytes
1 bps	1 bps	
1 Kbps	1.000 bps	125B
1 Mbps	1.000.000 bps	125KB
1 Gbps	1.000.000.000 bps	125MB

Pongamos el ejemplo de una conexión de 1Gbps, en condiciones ideales tomaría 1 segundo en transmitir un archivo de 125MB.

La **conversión de bits a bytes**, para tener una noción real del volumen de datos a transmitir en función del tamaño de archivos, se realiza así:

cantidad de bits / 8

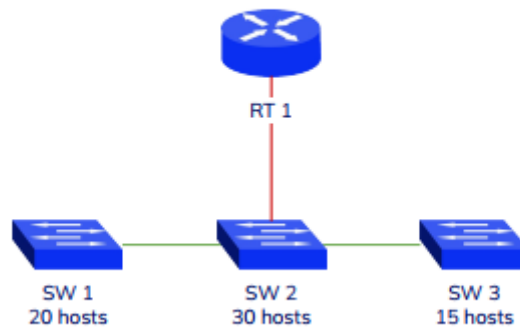
8b / 8 = 1B 1000 b / 8 = 125B

***1.000.000.000b / 8 = 125.000.000B / 1.000.000 = 125MB**

***Dividimos el resultado por 1.000.000 para convertir de B a MB**

Ancho de banda, segmentos de red y backbone

El ancho de banda determina la cantidad de información que puede pasar por un medio en 1 segundo y es fundamental para **determinar el tipo de conexiones** entre segmentos de red.



En el ejemplo de la slide anterior, la conexión entre SW 1 y SW 2 debe transportar toda la información enviada y recibida por los hosts de SW 1. El ancho de banda de la conexión y dispositivos de red deben tolerar tal volumen de datos. De igual manera sucede con SW 3.

La conexión entre SW 2 y RT 1 debe tolerar todo el volumen de datos enviados y recibidos por los segmentos SW 1, SW 2 y SW 3, por lo tanto el ancho de banda de esa conexión debe ser mayor.

Los **backbones** o **conexiones troncales** son aquellas que interconectan los segmentos de red y por donde pasa el mayor volumen de datos, los *backbones* suelen tener un ancho de banda mucho mayor.

Definir el volumen de datos y el ancho de banda es **clave** para el correcto funcionamiento de la red. Enviar un volumen de datos mayor a lo que el medio puede transportar provoca latencias, pérdida de paquetes, intermitencias e inestabilidad en las conexiones a nivel de capa 4 (protocolos de transporte).

Estimando el ancho de banda

El **estimado de ancho de banda** para un segmento de red lo podemos establecer teniendo en cuenta el tipo y cantidad de información que un host necesita enviar y recibir:

Servicios de streaming (Zoom, Youtube, Meet).

Acceso a archivos en red, tamaño promedio de los ficheros.

Cantidad de servicios a los que se accede fuera del segmento de red.

Envío de correo electrónico.

Etc.

Luego de establecer el estimado del ancho de banda necesario para un **host** se multiplica por la cantidad de hosts dentro del segmento físico. Como resultado, el *backbone* que conecta el segmento físico con el siguiente debe tener el ancho de banda necesario para abastecer a todos los hosts.

Otro aspecto a tener en cuenta es el estimado de ancho de banda para las **conexiones a internet**. A nivel global se estima y se contrata en consecuencia, y en general los anchos de banda provistos por los ISP no suelen ser grandes en comparación con los anchos de banda en conexiones *backbone*. En muchos casos se suelen utilizar varias conexiones de internet y se jerarquiza el tipo de tráfico por conexión para garantizar una transferencia de información fluida.

Cabe aclarar que, generalmente, es poco probable que todos los hosts de un segmento de red estén enviando y recibiendo información utilizando la totalidad del ancho de banda por hosts al mismo tiempo, de hecho, el ancho de banda nunca es totalmente aprovechado como veremos más adelante.

Velocidad de transmisión

El ancho de banda es la cantidad de información que recibes cada segundo, mientras que la **velocidad** es **cuán rápido esa información se recibe o descarga**. Este término se puede definir como la **velocidad a la que se transmite la información**.

Cuando un usuario adquiere un paquete con una empresa prestadora de servicios de internet, recibe, por ejemplo, 10 mbps, 30 mbps, 100 mbps, etc. Y esto se refiere a la **cantidad de datos que podemos descargar o subir a la red**.

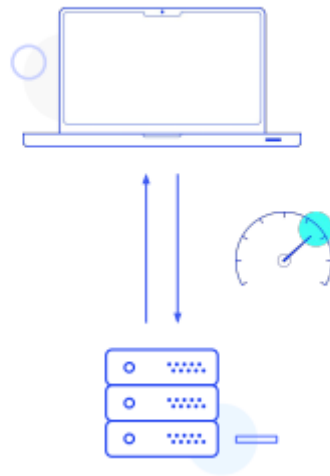
Como recomendación, lo indicado es que para que la velocidad pueda existir será necesario tener un ancho de banda igual o superior a la velocidad contratada en el paquete de servicio.

En el caso de una LAN, es obvio, cuanto mayor ancho de banda entre conexiones de host a conmutador, y conexiones de *backbone* mayor velocidad, pero la velocidad no depende de forma exclusiva del ancho de banda, y esto se debe a varios factores.

Latencia

Debe saber que es el **tiempo total** que transcurre desde que envía una información, hasta que la misma llega a un receptor. Su valor de medición se hace en milisegundos, también se conoce como **ping** y está presente en actividades que realiza cotidianamente como jugar en línea o hacer videollamadas.

El protocolo de capa 3 del modelo OSI que nos permite medir la latencia es el protocolo ICMP, y el programa '**ping**' es el más utilizado para no solo hacer estas mediciones sino también corroborar que efectivamente un paquete sale de un hosts llega a destino y regresa al origen.



Latencia, velocidad y ancho de banda

La **velocidad de conexión** influye en la latencia una vez que pasamos de un rango predeterminado.

Poniéndolo en un ejemplo, si tenemos una conexión a Internet de 1 Mbps y la comparamos con una conexión de 100 Mbps, dependiendo del tamaño del paquete se notará una mejora grande en la velocidad. Otros factores que importan a la hora de hablar de latencia son el estar conectado a internet por Wi-fi o un cable, si tiene servicio de fibra óptica o qué tanta distancia hay entre su ordenador y un router, etc.

La velocidad está influida por el tipo y calidad del medio, aunque un enlace wifi promete un ancho de banda 54Mbps la distancia entre emisor y receptor, obstáculos, interferencias y pérdida de paquetes harán que un conjunto de datos tarde más en enviarse o recibirse aumentando la latencia, y esto es independiente del ancho de banda.

Pero no solo esos son los factores que influyen en la velocidad:

De transmisión: es el tiempo que tarda el paquete en arribar hasta el siguiente nodo u otro destino final.

De propagación: es el tiempo que tarda un bit en propagarse desde un punto cualquiera de origen hasta llegar a uno de destino. Su velocidad depende del medio físico por el que se transporte y siempre es menor o igual a la velocidad de la luz.

El **ancho de banda** de las conexiones entre nodos intermediarios.

De procesamiento: se define en el tiempo que tardan los routers en examinar la cabecera y a su vez, la respuesta en determinar a dónde hay que enviar cualquier paquete haciendo una previa comprobación de sus tablas de enrutamiento.

De cola: tiempo de espera del paquete para poder ser transmitido a través de un enlace físico. Cabe anotar que no podemos saber previamente si va a haber un retardo de cola o no, ya que este cambia en tiempo real.

Tasa de transferencia

Una **tasa de transferencia de datos (DTR)** es la velocidad a la que se pueden transmitir los datos entre dispositivos. Esto a veces se denomina **rendimiento**.

La tasa de transferencia de un dispositivo a menudo se expresa en **kilobits** o **megabits** por segundo, abreviados como kbps y mbps respectivamente.



Calcular la velocidad de transferencia, el tiempo y los datos

Se calcula la **velocidad de transferencia** dividiendo la cantidad de datos entre el tiempo de transferencia.

Reemplaza la cantidad de datos (D) y el tiempo de transferencia (T) en la ecuación **$V = D / T$** para encontrar la tasa o velocidad (V).

Por ejemplo, se transfiere 25 MB en 2 minutos. Lo primero que debes hacer es convertir los 2 minutos a segundos multiplicando 2 por 60, que da como resultado 120. Entonces:

$$V = 25\text{MB} / 120\text{s}$$

$$V = 0,208 \text{ MB/s}$$

Pero como dijimos anteriormente, las velocidades y ancho de banda no se mide en bytes, sino en bits, entonces debemos convertir el valor de V que están en bytes a bits:

$$0,208 \text{ MB/s} * 8 = 1,208 \text{ Mbps}$$

Esta es la velocidad de transferencia real, es lo que tardó un fichero de 25 MB en llegar de un host a otro.

Conclusión

La velocidad es relativa a un conjunto de factores, el ancho de banda no define la velocidad de transferencia, pero mejores tecnologías y medios permiten **reducir la brecha** entre velocidad y ancho de banda.

En términos prácticos debemos considerar el ancho de banda para garantizar el paso de un volumen de datos dado entre segmentos de red, si el ancho de banda es inferior al volumen de datos se producen los cuellos de botella, aumento de latencia e inestabilidad en conexiones a nivel de capa 4 y superiores.

Para finalizar pongamos un ejemplo: hoy día una conexión promedio de internet está en 100Mbps, al descargar un fichero de algún servicio de alojamiento de archivos en internet vemos que la velocidad de descarga está en 5Mbps

¿Por qué no descargó a 100Mbps?

Latencia producida por distancias, procesamiento de paquetes, saltos entre nodos.

Ancho de banda de conexiones intermedias entre el servidor y el host del cliente.

El ancho de banda propio del servidor donde está alojado el fichero, en este punto estos servicios limitan la velocidad de transferencia por archivo ya que el ancho de banda total del que disponen debe abastecer a cientos y tal vez miles de usuarios que están descargando archivos al mismo tiempo.

Sentido de transmisión

El término **Duplex** hace referencia, por sí solo, a la capacidad de enviar y recibir datos.

El Duplex se usa a menudo cuando se habla de conversaciones por teléfono o equipos informáticos. Este por tanto es el sistema que permite mantener **comunicaciones bidireccionales**, algo que resulta básico hoy en día, al poder recibir y enviar mensajes de forma simultánea.

La posibilidad de poder transmitir en modo Duplex está condicionada por diferentes niveles. Uno de esos niveles es el medio físico para poder transmitir en ambos sentidos, también el sistema de transmisión para poder enviar y recibir a la vez y por último el protocolo o norma de comunicación que utilice.

Full Duplex

Este término describe la **transmisión y recepción de datos simultáneas a través de un canal**.

Un dispositivo **Full Duplex** es capaz de realizar transmisiones de datos de red **bidireccionales al mismo tiempo**. No va a tener que esperar y verificar si se está emitiendo en un sentido.

Para que la comunicación sea Full Duplex es necesario que existan **dos canales o vías** de comunicación, un canal para enviar información y otro para recibir información, esta tecnología supone una mejora crucial en términos de velocidades de transferencia, ya que duplica el uso del ancho de banda de un medio físico.

Half Duplex

Por otra parte tenemos la opción de **Half Duplex**. Este tipo de dispositivos solo pueden transmitir en **una dirección a la vez**.

De este modo, los datos pueden moverse en dos direcciones, pero **no al mismo tiempo**. Por tanto la comunicación es **bidireccional, pero una a la vez**. El uso del medio se hace por turnos, mientras uno envía tramas al medio, el resto escucha, luego cuando el canal está desocupado otro dispositivo de red puede usar el medio.

Ciertamente este modelo ofrece un rendimiento inferior respecto al Full Duplex por lo que mencionamos. Un ejemplo de modo de uso sería un *walkie-talkie*. Los dos pueden hablar, pero no al mismo tiempo. Uno tiene que esperar a que termine el otro. No podrían establecer una comunicación al mismo tiempo, en ambos sentidos, como sí podríamos lograr con un teléfono móvil.

Servicios de Red

Identificación de hosts en la red: Servicio WINS y NETBIOS

En el caso de las redes con hosts que ejecutan windows existen dos tipos de servicios que se encargan de anunciar al host e identificar un host en la red, veamos:

NetBIOS: este servicio identifica un host bajo un nombre, es decir el **nombre de host**.

WINS: Windows Internet Naming Service (WINS) es un servidor de nombres de Microsoft para NetBIOS, que mantiene una tabla con la correspondencia entre direcciones IP y nombres NetBIOS de ordenadores. Esta lista permite localizar rápidamente a otro ordenador de la red.

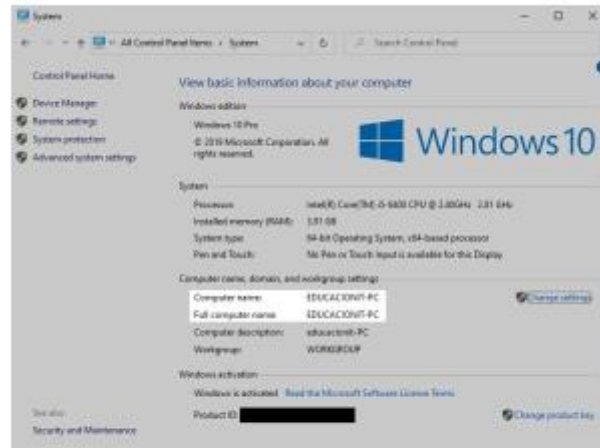
Los servicios de “anuncio de servicios” (carpetas e impresoras compartidas, etc.) y “nombres de hosts” informaran a todos los equipos de la red que sean compatibles el nombre propio y su dirección IP. El resto de los hosts mediante el servicio WINS tomarán nota del nombre de host y la dirección IP que le corresponde a cada equipo que se anuncie. Luego podemos referirnos a cualquier host por su IP o nombre de host.

Muchas veces no existe compatibilidad entre sistemas operativos distintos, como el caso de linux y windows, pero en general dispositivos como impresoras de red trabajan con NetBIOS y WINS, es por eso que desde windows podemos visualizar una impresora por su nombre.

Nombre de host

En una red de computadoras no solo se identifican los dispositivos a partir de una dirección IP, además de la dirección los dispositivos se identifican bajo un nombre que debe ser único dentro de la red, entonces podemos “contactar” un host mediante su IP o su nombre.

El **nombre de host** se determina en el momento de instalación de un sistema operativo, en smartphones normalmente el nombre ya viene predefinido (marca y modelo), en el caso de las impresoras sucede lo mismo y en general es posible cambiar el nombre de host en cualquier momento.

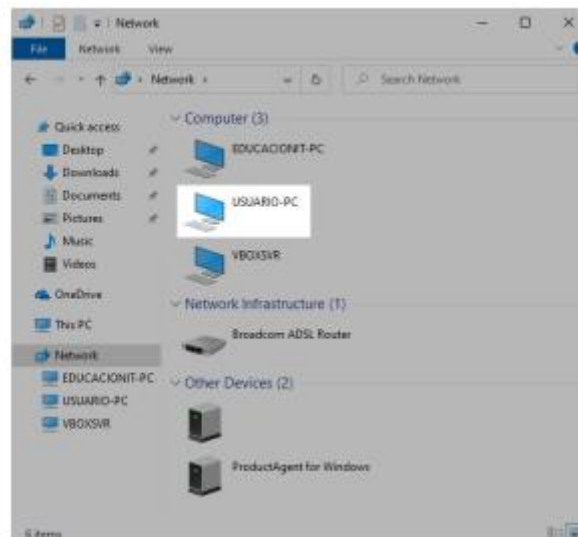


Nombre del host determinado en la etapa de instalación del SO.

Hosts y servicios descubiertos

Hosts en la red

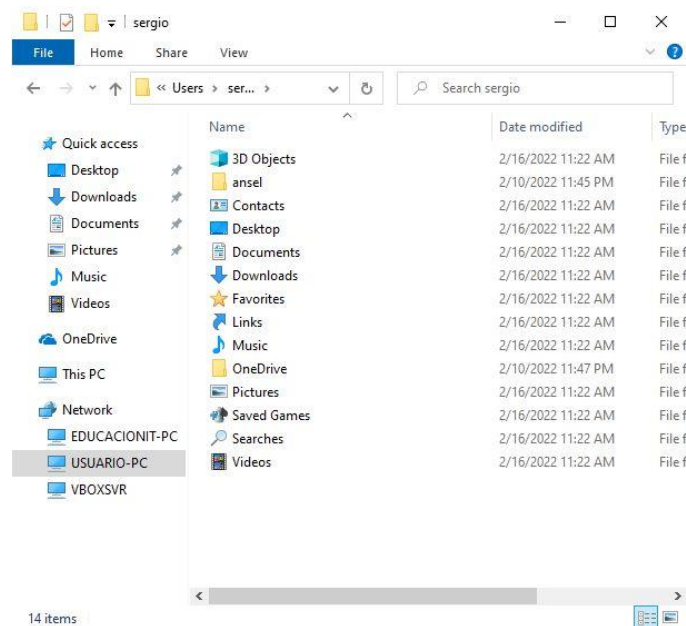
En windows desde el navegador de archivos podemos ir a la sección red y ver los dispositivos anunciados a los que podemos acceder.



Host “USUARIO-PC” anunciado en la red.

Recursos compartidos

Ver los servicios de red que comparten los hosts descubiertos.



El host “USUARIO-PC” tiene compartido su directorio personal.

Herramienta PING

Utilizar la herramienta ping para probar la conexión usando el nombre de host.

```

C:\Users\educacionit>ping -4 USUARIO-PC

Pinging USUARIO-PC [192.168.1.34] with 32 bytes of data:
Reply from 192.168.1.34: bytes=32 time=5ms TTL=128
Reply from 192.168.1.34: bytes=32 time=7ms TTL=128
Reply from 192.168.1.34: bytes=32 time=2ms TTL=128
Reply from 192.168.1.34: bytes=32 time=9ms TTL=128

Ping statistics for 192.168.1.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 9ms, Average = 5ms

C:\Users\educacionit>
  
```

Se indica el nombre del host como parámetro, el servicio WINS traduce el nombre en una IP.

Fichero ‘hosts’

Se utiliza para **registrar los nombres de hosts** y las **direcciones IP** que les corresponden.

Normalmente no tenemos ninguna necesidad de modificar este archivo, los registros se actualizarán de forma dinámica a partir de los servicios NetBIOS y WINS.

Cabe mencionar que este fichero se utiliza en multitud de sistemas operativos y firmwares de dispositivos de red y tienen la misma estructura:

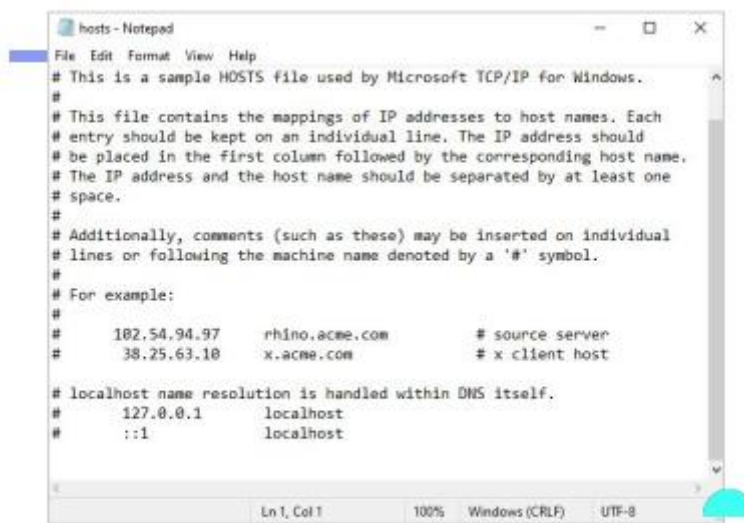
<dirección ip> <nombre de host>

192.168.1.56 contabilidad

...

En windows lo podemos encontrar en

“C:\Windows\System32\drivers\etc\hosts”.



```
File Edit Format View Help
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name,
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10      x.acme.com           # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
```

Contenido del fichero "hosts" de windows

Servicio DNS

El **Sistema de Nombres de Dominio** o **DNS** se encarga de traducir nombres “amigables” para los usuarios en direcciones IP:

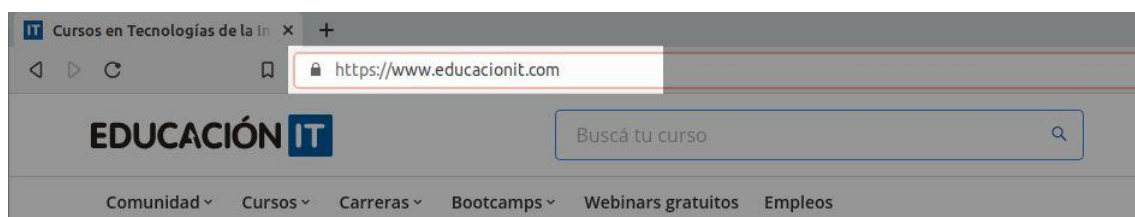
educacionit.com has address **54.207.106.237**

Cuando introducimos en el navegador una url esta se compone de varias partes:

Protocolo de aplicación:

HTTP/HTTPS/FTP/FTPS

Dominio: educacionit.com



Normalmente solo ponemos el nombre del sitio al que queremos acceder, la misma aplicación junto con el servidor determinarán el protocolo a utilizar.

Cuando introducimos una URL o el dominio en un navegador, en este caso “educacionit.com” estamos solicitando el contenido web a un servidor que aloja dicha web, veamos el proceso bajo el modelo de capas TCP/IP:

Capa de aplicación: el usuario introduce el nombre del sitio “educacionit.com”, la aplicación genera un mensaje que es la solicitud de acceso a dicho sitio. El mensaje se estructura bajo el protocolo de aplicación que corresponda (HTTP o HTTPS).

Capa de transporte: el mensaje se segmenta bajo el protocolo de transporte TCP, se establece la conexión de puerto a puerto (80 para http, 443 para https).

Capa de internetworking: se generan los paquetes de datos y se agrega la dirección IP de destino “54.207.106.237”, el servidor donde se aloja el sitio.

Capa de acceso a la red: se generan las tramas a partir de los paquetes de datos, estas tramas serán dirigidas al dispositivo de red que pueda llevar dicho paquete al destino, normalmente el *gateway*.

Analizando el proceso...

¿De dónde sale la dirección IP del servidor si solo indicamos el nombre del sitio “educacionit.com”?

En internet existe una red de miles de servidores DNS, estos servidores llevan registros de los nombres de dominios, subdominios, nombres de servidores de correo, etc. y las direcciones IP asociadas a estos tipos de registros. Cuando introducimos un dominio en un programa cliente este debe averiguar cuál es la dirección IP asociada a dicho dominio y lo hará consultando a un servidor DNS que pueda resolver la solicitud, una vez obtenida la IP se podrán enviar los mensajes al servidor correspondiente.

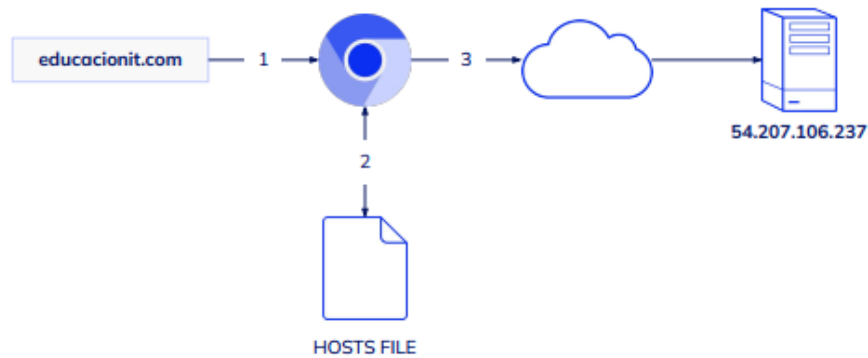
Es algo similar a lo que sucede con el nombre de host y el fichero “hosts”, pero a una escala mucho mayor, la red DNS es el sistema que nos permite conectar con cualquier host de internet a partir de un dominio registrado y propagado.

Funcionamiento

La resolución de un nombre de dominio es un proceso que puede ser complejo.

Es importante saber que las aplicaciones van a intentar obtener una dirección IP de dos maneras, por un lado buscará registros en el **fichero hosts** y, si no lo encuentra, recurrirá a un **servidor DNS**.

Fichero hosts



1. Se introduce el nombre de dominio en el navegador web.
2. Se busca un registro que relacione el nombre “educacionit.com” con una dirección IP.
3. Si este se encuentra en el fichero hosts se envía el paquete a la dirección IP asociada al registro.

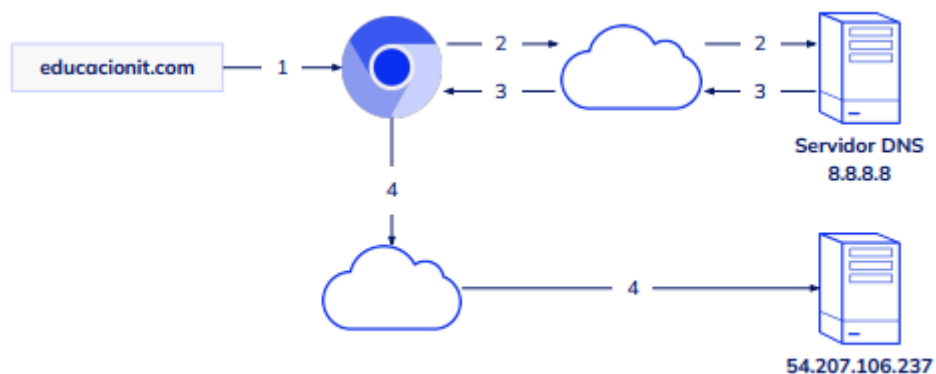
Es poco probable que en el fichero hosts exista un registro de dominios de internet.

Como vimos anteriormente en este fichero registramos direcciones de hosts dentro de la LAN en situaciones específicas, pero describiendo

el proceso de resolución de nombre esto es lo que sucede primero.

Consulta DNS

El fichero hosts, como era de esperar, no contiene ningún registro, entonces se intentará averiguar la dirección IP consultando a un servidor DNS.

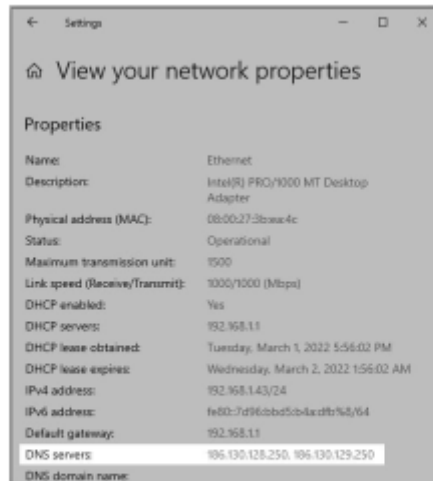


1. Se introduce el nombre de dominio en el navegador web.
2. Se envía una petición de resolución de nombre de dominio a un servidor DNS de internet.

3. El servidor DNS responde con la dirección IP asociada al dominio que se intenta resolver.

4. Se envía la solicitud a la dirección IP devuelta por el servidor DNS.

Para que un host pueda resolver nombres de dominio necesita tener configurado un servidor DNS y tener acceso a él.



Servidores DNS configurados en el host
186.130.128.250 y 186.130.129.250.

Tipos de servidores DNS

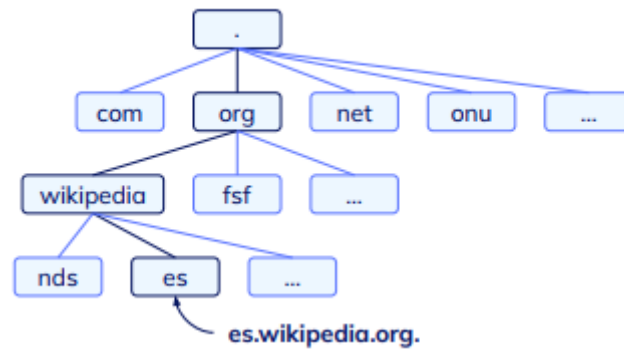
La red de servidores DNS de internet es compleja, cada servidor tiene un rol en particular, dentro de una organización de escala global, pero estos servidores no solo existen en internet, sino también en redes LAN, WAN y MAN.

Vamos a explorar la funcionalidad de los servidores DNS según su rol.

Servidores de Nombres Dominio

Estos servidores **guardan los registros de todos los nombres de dominios que existen en internet**, y tienen una **arquitectura jerárquica**, cada nivel sabe quien puede resolver un nombre completo.

Por ejemplo, cuando se pide “educacionit.com” los servidores que administran los “.com” indican quién puede saber el dominio completo “educacionit.com”.



Servidores de Resolución de nombres de dominio

Estos son los servidores que se encargan de resolver una petición, son los servidores que se configuran en el host.



1. Se introduce el nombre de dominio en el navegador web.
2. Se envía una petición de resolución de nombre de dominio a un servidor DNS de resolución de nombre de dominio de internet.
3. El servidor de resolución realiza la búsqueda en servidores de nombres de dominio.
4. El servidor de nombres de dominio devuelve al resolutor la información recabada.
5. El servidor de resolución de nombres entrega la dirección IP asociada al dominio que se intenta resolver.

Dentro de la infraestructura de red son los servidores de resolución los que nos van a permitir acceder al contenido web o cualquier otro servicio de red a partir de un nombre.

Dentro de una LAN se pueden colocar servidores DNS que pueden gestionar nombres de dominio que solo existen dentro de la LAN, por ejemplo “servidor-nas.intranet”.

DNS CACHE

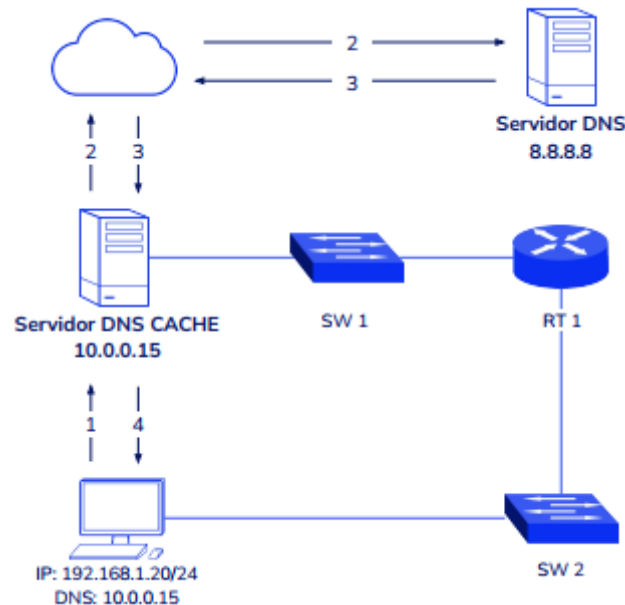
Los servidores pueden estar dentro de una LAN o ser accesibles desde internet, vamos a poner el foco a **servidores DNS dentro de una LAN**.

El propósito de tener un servidor DNS en una LAN es **evitar el uso de internet**.

Imaginemos que cada host de la red haga las peticiones a un servidor de internet por cada sitio al que accede, estaríamos utilizando el ancho de banda de la conexión a internet, cuantos más hosts y más peticiones más ancho de banda es necesario y esto se suma a el resto del tráfico que pasa por dicha conexión.

En un red con salida a internet lo que se busca es minimizar el tráfico, todo aquello que se pueda resolver de manera local evita el tráfico hacia la red pública y se economiza el ancho de banda, y por otra parte tenemos el beneficio de los tiempos de respuesta, es **más rápido realizar una consulta a un servidor local que a uno de internet.**

Bajo esta premisa entran en juego los **servidores DNS Caché, que actúan como servidores de resolución de nombres de dominio** y por cada consulta **guarda en una caché las respuestas**, en consultas posteriores para el mismo dominio no los buscara en internet, sino que responderá con lo que tenga registrado en la caché.



1. El host 192.168.1.20 envía un solicitud de resolución al servidor DNS Caché local.
2. El servidor 10.0.0.15 realiza la resolución con un servidor de internet.
3. El servidor de internet devuelve toda la información solicitada.
4. El servidor DNS Caché local entrega al host la dirección IP del dominio a consultar.

En el futuro cuando el host realice la misma consulta el servidor DNS Caché responderá con lo que tenga almacenado sin recurrir al servidor de internet. Esta información queda guardada un tiempo predefinido, luego se vuelve a repetir el proceso.

Servidores de resolución públicos y privados

Los servidores DNS de internet pueden ser públicos o privados, esto básicamente define quiénes pueden usar un servidor DNS.

Servidores públicos

Son los servidores de internet que **cualquiera puede usar** tanto en la propia computadora como para todos los hosts y servidores dentro de una red LAN, estos servidores forman parte del conglomerado DNS.

A la derecha vemos una lista de servidores DNS públicos.

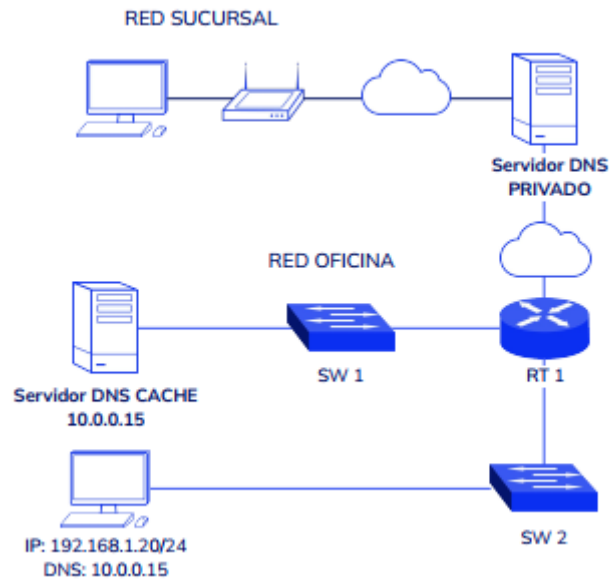
- DNS de Google primaria: 8.8.8.8
- DNS de Google secundaria: 8.8.4.4
- DNS de OpenDNS primaria: 208.67.222.222
- DNS de OpenDNS secundaria: 208.67.220.220
- DNS de Cloudflare primaria: 1.1.1.1
- DNS de Cloudflare secundaria: 1.0.0.1
- DNS de Comodo Secure DNS primaria: 8.26.56.26
- DNS de Comodo Secure DNS secundaria: 8.20.247.20
- DNS de Quad9 primaria: 9.9.9.9
- DNS de Quad9 secundaria: 149.112.112.112
- DNS de DNS.Watch primaria: 84.200.69.80
- DNS de DNS.Watch secundaria: 84.200.70.40
- DNS de AdGuard DNS primaria: 176.103.130.130
- DNS de AdGuard DNS secundaria: 176.103.130.131
- DNS de Dyn primaria: 216.146.35.35
- DNS de Dyn secundaria: 216.146.36.36

Servidores privados

Hay varios aspectos con respecto a estos servidores. Por un lado si disponemos de un servidor dentro de la LAN técnicamente estamos hablando de un servidor privado, que además puede gestionar dominios internos como “servidor-nas.intranet”. Pero en un sentido más concreto un **servidor DNS privado solo admite solicitudes de clientes predefinidos**.

Por ejemplo, normalmente en la red hogareña los servidores DNS son provistos por el ISP, pero esos servidores no pueden ser usados por cualquiera, solo los clientes del ISP. Del mismo modo hay servicios DNS de pago que ofrecen muchas características orientadas a la seguridad, dominios privados, caché, velocidad, etc. En este tipo de servicios son admitidos los clientes que abonan una factura mensual, anual, etc. Los **servidores públicos también son servidores privados**, pero asociamos lo público a lo gratuito, los mismos servicios listados anteriormente tienen paquetes de servicios pagos.

Un último ejemplo de servidor privado es aquel que podemos instalar y configurar pero no dentro de la LAN, sino mediante la contratación de una VPS donde el administrador de sistemas instalará y configurará el servicio DNS para responder consultas a cualquier host admitido aun fuera de la red LAN.



Servicio DHCP

El **protocolo de configuración dinámica de host (DHCP)** es un protocolo de red de tipo cliente/servidor mediante el cual un servidor DHCP asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo en una red para que puedan comunicarse con otras redes IP.

Hasta el momento hemos visto como configurar distintos aspectos de red de un host:

IP

Máscara

Gateway

DNS

Siendo que la IP y la Máscara son los elementos fundamentales para que un host sea parte de una red, el resto son configuraciones importantes pero no estrictamente necesarias, si el host no precisa resolver nombres de internet, no lleva DNS; si no tiene comunicación con otras redes, no precisa de *Gateway*.

En una red puede resultar complejo y costoso tener que establecer de manera manual la configuración de red de cada host.

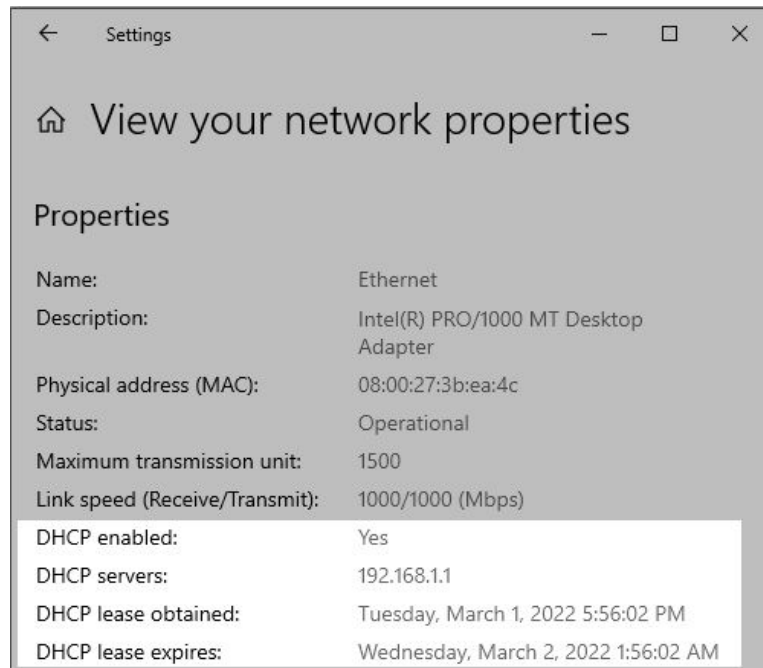
Para evitar esto el servicio **DHCP** es el que se encarga de **asignar un conjunto de parámetros a cada host en la red de manera automática**, siendo la IP y la Máscara las configuraciones esenciales, pero también puede asignar DNS y *Gateway* entre otros aspectos más avanzados. Los servidores DHCP son más comunes de lo que se piensa, de hecho **cada vez que conectamos un dispositivo móvil a una red wifi es el servidor DHCP de la red la que determinará la configuración de red del dispositivo.**

Prácticamente todos los routers hogareños, modems provistos por el ISP, routers orientados a pequeñas empresas disponen de un servicio DHCP.

Funcionamiento

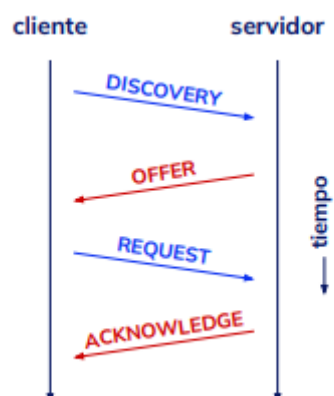
Cuando un host se enciende y se carga el sistema operativo, el cliente DHCP va a solicitar a un servidor DHCP la configuración de red, siempre y cuando el host este configurado de esa forma:

Según la imagen está activado el cliente DHCP por lo que la configuración de red es automática, el servidor DHCP es el 192.168.1.1 el “leasing” es la entrega de una dirección IP pero esta dirección no es siempre la misma para el mismo host, esta cambia cada ‘X’ cantidad de tiempo, es algo que está determinado en el servidor DHCP, pasado ese tiempo la dirección se renueva.



Obtención de IP

Cuando el host solicita una dirección se realizan una serie de pasos como se muestra aquí.



La comunicación entre cliente y servidor utiliza los puertos 67 para el servidor, 68 para el cliente y el protocolo de transporte es el UDP.

1. El cliente DHCP envía un paquete DHCPDISCOVER a la dirección 255.255.255.255 desde la dirección 0.0.0.0. Con esta denominada difusión amplia o broadcast, el cliente establece contacto con todos los integrantes de la red con el propósito de localizar servidores DHCP disponibles e informar sobre su petición. Si solo hay un servidor, entonces la configuración es extremadamente sencilla.
2. Todos los servidores DHCP que escuchan peticiones en el puerto 67 responden a la solicitud del cliente con un paquete DHCPOFFER, que contiene una dirección IP libre, la dirección MAC del cliente y la máscara de subred, así como la dirección IP y el ID del servidor.
3. El cliente DHCP escoge un paquete y contacta con el servidor correspondiente con DHCPREQUEST. El resto de los servidores también reciben este mensaje de forma que quedan informados de la elección. Con esta notificación, el cliente también solicita al servidor una confirmación de los datos que le ha ofrecido. Esta respuesta también sirve para confirmar parámetros asignados previamente.
4. Para finalizar, el servidor confirma los parámetros TCP/IP y los envía de nuevo al cliente, esta vez con el paquete DHCPACK (DHCP acknowledged o «reconocido»). Este paquete contiene otros datos (sobre servidores DNS, SMTP o POP3). El cliente DHCP guarda localmente los datos que ha recibido y se conecta con la red. Si el servidor no contara con ninguna dirección más que ofrecer o durante el proceso la IP fuera asignada a otro cliente, entonces respondería con DHCPNAK (DHCP not acknowledged o «no reconocido»).

Pool de direcciones

En una red todos los hosts van a compartir un conjunto de configuraciones:

Máscara

DNS

Gateway

Pero cada host va a diferir en la ID de Host de su dirección IP, entendamos el concepto de DHCP como una plantilla, todos reciben la misma información pero una IP única para cada host.

En el servidor DHCP se especifica un rango de direcciones a repartir, una cantidad específica, este rango se denomina pool, cuando el pool se agota ya no puede seguir asignando direcciones.

Configuración del servidor DNS router TP Link.

Como se mostró en la imagen anterior, el pool de direcciones establece que se pueden repartir IPs desde la 192.168.1.100 a la 192.168.1.199, en total 100 direcciones.

Además de las direcciones podemos configurar otros parámetros:

Gateway

Servidores DNS

Lease Time

Dominio por defecto (si hubiese un dominio de red)

Direcciones estáticas

No todos los hosts de una red obtienen direcciones dinámicas, algunos de ellos precisan tener **direcciones fijas** como es el caso de algunos hosts que ofrezcan servicios a la red externa, como por ejemplo el escritorio remoto de windows. En ese caso cuando se hace un mapeo de puertos se va a apuntar a una dirección IP que no debe cambiar nunca.

Un servidor DHCP permite la asignación de una dirección estática para un host en particular, esto se logra reservando una dirección asociándola a la MAC Address de la interfaz que va a recibir dicha dirección.

Address Reservation				
ID	MAC Address	Reserved IP Address	Status	Modify
1	08-00-27-04-70-9B	192.168.1.145	Enabled	Modify Delete
2	08-00-27-04-70-9C	192.168.1.215	Enabled	Modify Delete
<div> Add New... Enable All Disable All Delete All </div>				

Obviamente la forma de configurar el servidor va a depender del servidor en sí mismo, por ejemplo la interfaz de usuario varía de dispositivo a dispositivo y en otros casos se realiza a través de la línea de comandos, pero en todos ellos los parámetros son los mismos.

Address Reservation				
ID	MAC Address	Reserved IP Address	Status	Modify
1	08-00-27-04-70-9B	192.168.1.145	Enabled	Modify Delete
2	08-00-27-04-70-9C	192.168.1.215	Enabled	Modify Delete
<div><div>Add New...</div><div>Enable All</div><div>Disable All</div><div>Delete All</div></div>				

La forma de configurar el servidor va a depender del servidor en sí mismo, por ejemplo la interfaz de usuario varía de dispositivo a dispositivo y en otros casos se realiza a través de la línea de comandos, pero en todos ellos los parámetros son los mismos.