***Notas del Curso.***

**Bienvenidos al Curso de Redes de Internet**

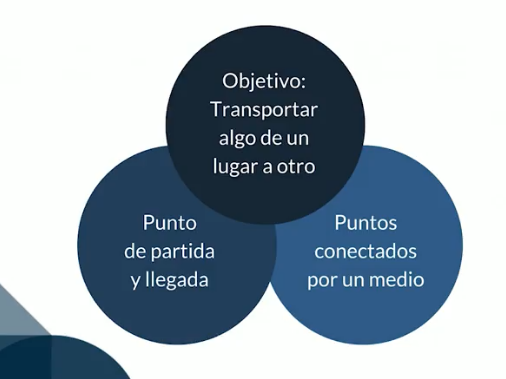
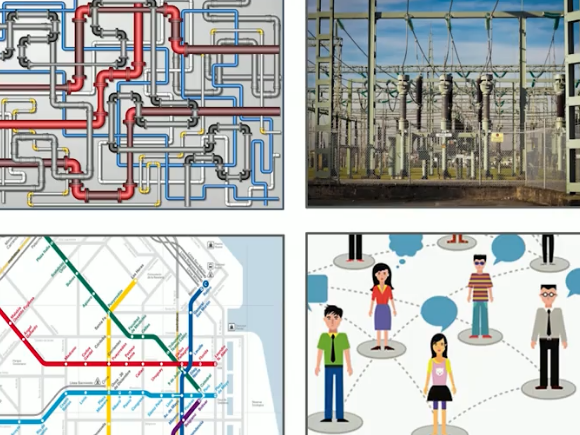
Hola bienvenidos al **Curso de Redes de Internet**

En este curso vamos a hablar sobre cómo internet ha cambiado la forma en la que nos comunicamos. Además, vamos a ver cómo la economía y la política han cambiado gracias a las redes de internet. Hoy en día podemos comunicarnos sin importar en dónde nos encontramos. En este curso vamos a ver:

* Cómo funciona la comunicación en redes
* Modelos de referencia OSI y TCP/IP
* Diseño de redes y configuración

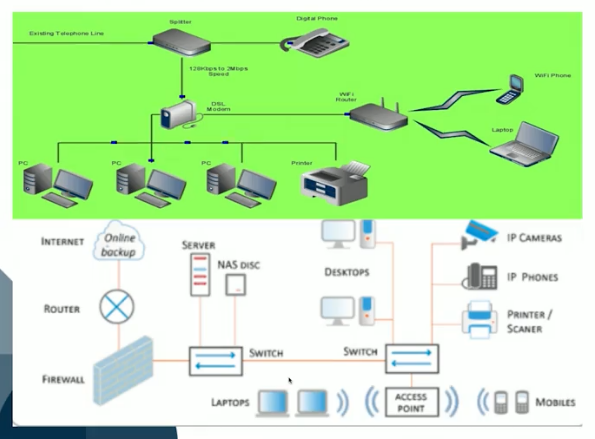
**Qué es la red, Internet, LAN, WAN y Topologías de Red**

El objetivo de una **red** es transportar un elemento de un lugar a otro.

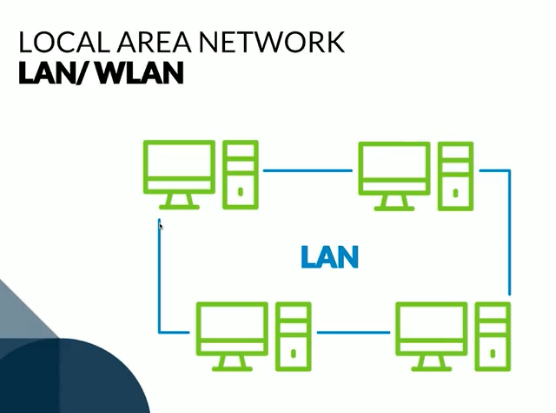


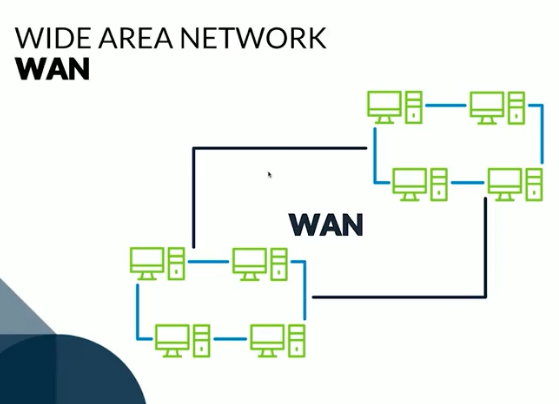
Siempre tenemos un punto de partida y un punto de llegada. Una **red informática** es un **conjunto de equipos conectados** entre sí por medio de dispositivos físicos o inalámbricos que envían y reciben impulsos eléctricos, ondas electromagnéticas, o cualquier otro medio para el transporte de datos.





Existen varios tipos de redes informáticas que son:

* **LAN(Local Area Network o Red de área local) /WLAN(Wireless Local Area Network o Red de área local Inalámbrica)** La red LAN es una red pequeña que conecta ordenadores o dispositivos en areas pequeñas como las que tenemos en la casa, o en una oficina con el fin de compartir recursos, datos o apps.
* 
* **WAN (Wide Area Network o Red de área amplia)** **Este tipo de red generalmente sirve para conectar dispositivos que se encuentran separados por un área geográfica extensa, es decir, si las redes LAN conectan computadores o dispositivos en un área “pequeña”, las redes WAN conectaran “sucursales” con sedes centrales.** Las redes WAN son redes que interconectan países o ciudades.



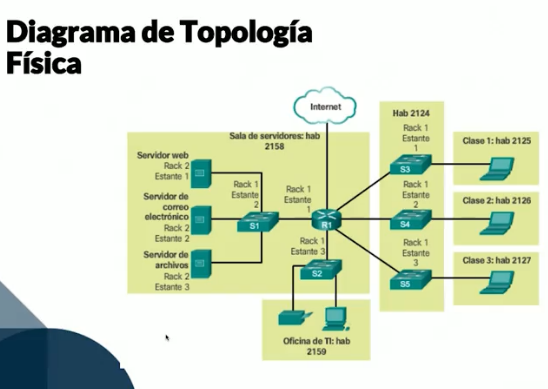
* **MAN (Metropolitan Area Network o Red de área metropolitana)** Es una infraestructura de red que abarca un área mayor a una LAN pero menor que una WAN. Las redes MAN **conecta** como **un barrio**, esto quiere decir que es mucho más pequeña.

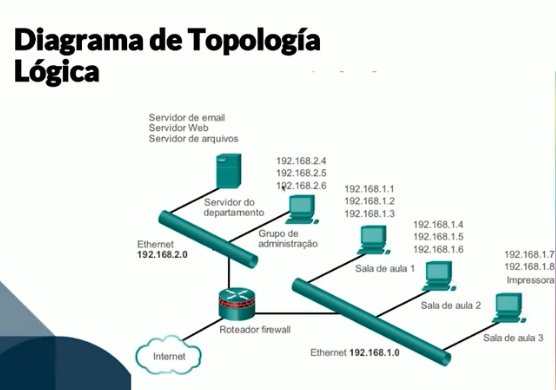
**¿Qué es internet?**

El internet es una red de redes interconectadas mundialmente. “NO existe la nube”.



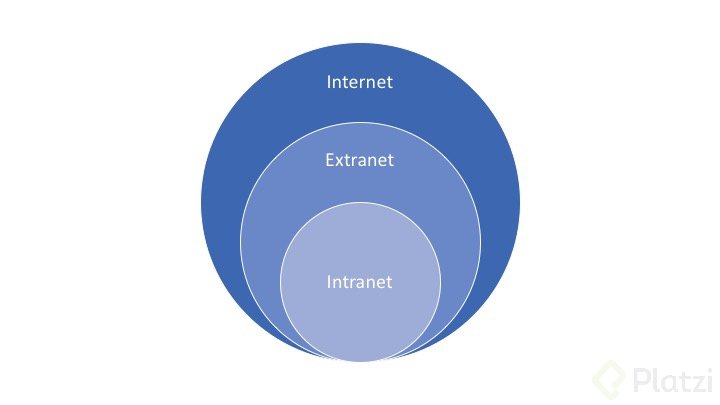
**Topología de red:** Es el mapa físico y lógico de la red.





# Intranet y Extranet.

Esta clase vamos a hablar de dos formas en las que podemos diseñar e implementar las redes de acuerdo con características de acceso que queremos dar a los usuarios.



### **Intranet**

Son aquellas redes internas en las que el acceso a la información está estrictamente limitada a personal de la compañía. Este tipo de redes se restringen con el uso de software y se usan en situaciones en las que la información a la que pueden acceder los usuarios es confidencial.

### **Extranet**

El siguiente nivel de acceso sucede cuando las compañías requieren dar acceso seguro y bajo confidencialidad a usuarios externos incluso a organizaciones diferentes a la que posee la información.

Esto puede pasar por ejemplo cuando una compañía requiere compartir documentos o información con proveedores o contratistas.

# Ejemplos de Topologías de Red y sus usos.

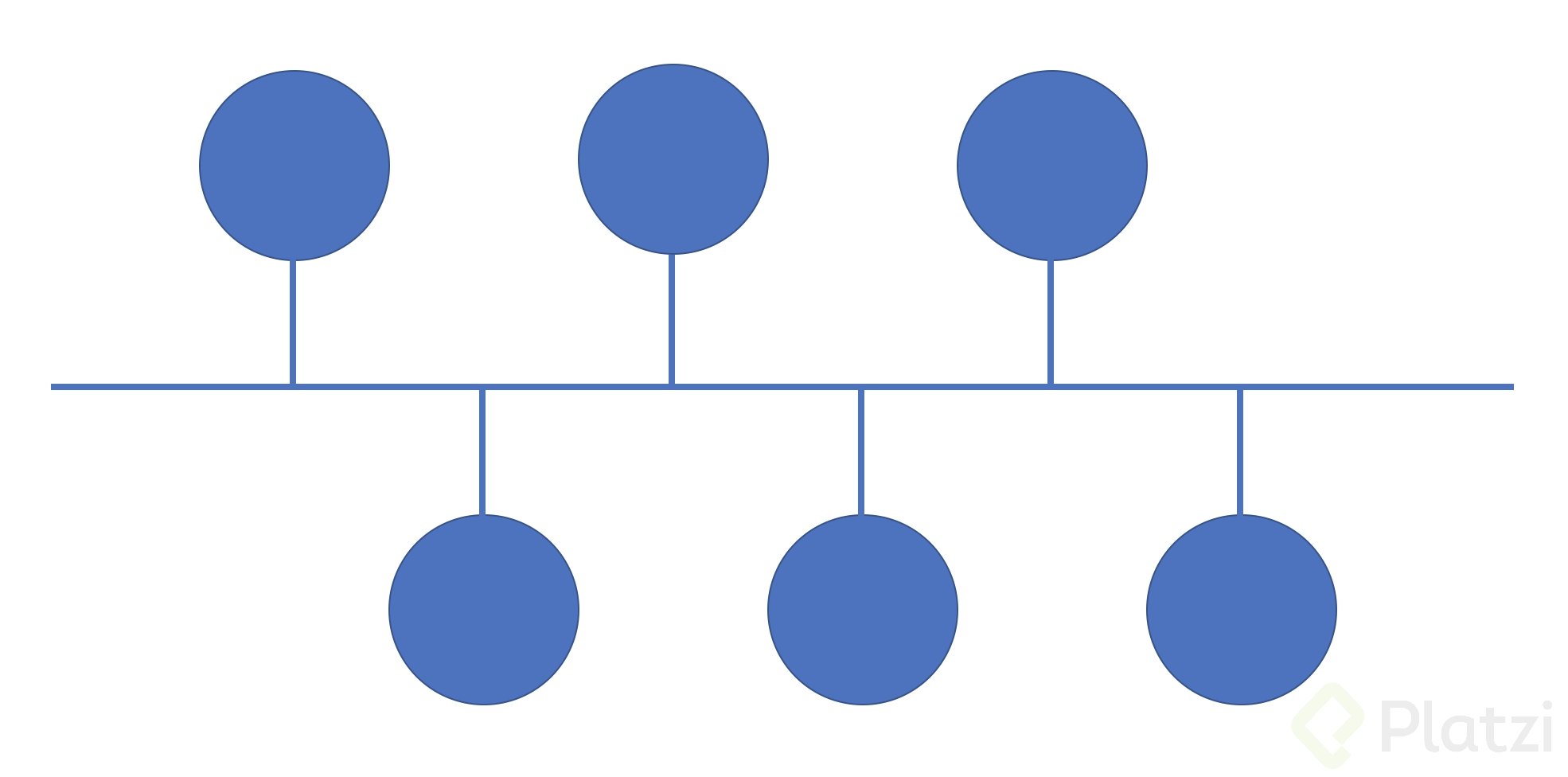
La topología de red nos permite identificar **la forma en que los nodos están conectados**. La información se envía a través de los medios y de los nodos para viajar de un lugar a otro.

Ya vimos las dos formas en que podemos mostrar estos diseños, **física** cuando queremos mostrar los equipos de red que conforman el diseño y **lógica** para mostrar el direccionamiento lógico de los dispositivos.

La topología más rápida de implementar y de ver es cuando tenemos **dos nodos conectados por un medio para enviar información** esta es llamada Punto a Punto, un punto envía información al otro.

Luego tenemos otras topologías, veamos algunas de sus características y ventajas.

### **Topología de bus.**



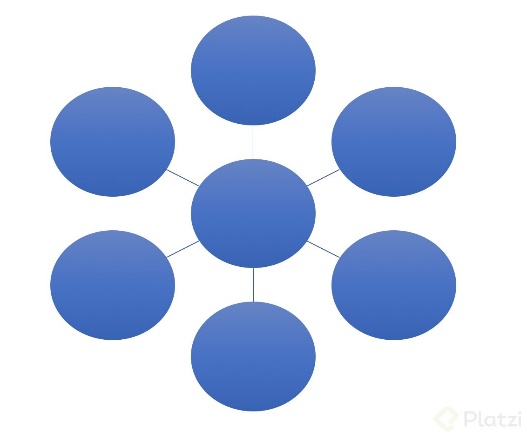
Este tipo de topología es el más usado en redes de tipo **LAN**. En esta topología los nodos están conectados a un mismo medio que transporta la información.  
La ventaja de este tipo de red es que es fácil de implementar y puede crecer rápidamente sin tener que hacer cambios bruscos a la red.  
Esto, aunque es una gran ventaja y seguro le facilita la vida al administrador de la red, presenta dos inconvenientes, uno es que el tráfico de todos los nodos puede ser visto por los otros y el segundo es que a medida que la red crezca se va a ver afectado el rendimiento.

### **Topología de anillo.**



Este tipo de topología consiste en que cada nodo tiene una única conexión de entrada y una conexión de salida. Un token de confirmación viaja a través de cada nodo avisando que se envió y fue recibida correctamente.  
Este tipo de topología aunque garantiza el envío de la información puede llegar a ser un poco lenta ya que ésta debe pasar por cada nodo intermedio antes de alcanzar su objetivo. En el caso de que uno de los nodos fallé esto puede afectar el funcionamiento de la red.

**Topología de estrella.**

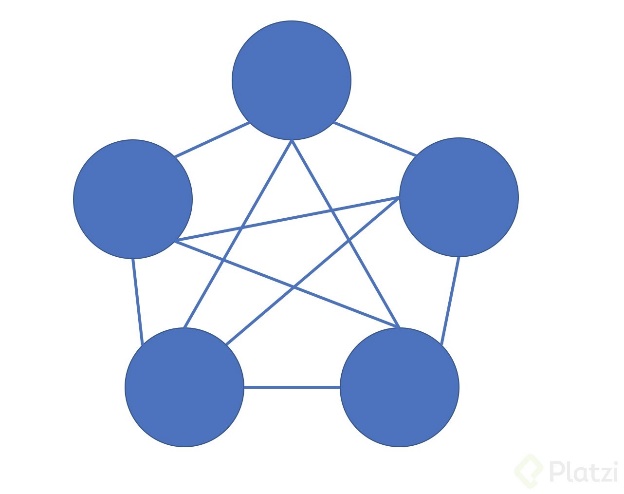


En esta topología todos los nodos están conectados a un punto central, esta implementación permite garantizar el funcionamiento de la red, de forma que si alguno de los nodos falla esto no va a afectar para nada el funcionamiento ni el rendimiento de la red.

Esta topología se usa mucho en redes LAN, por ejemplo en oficinas en las que hay un switch al que llegan todas las conexiones de los dispositivos a través de cable.

Es una topología que permite agregar nodos nuevos siempre que el dispositivo central lo permita, sin embargo en caso en que el nodo central falle toda la red dejará de funcionar.

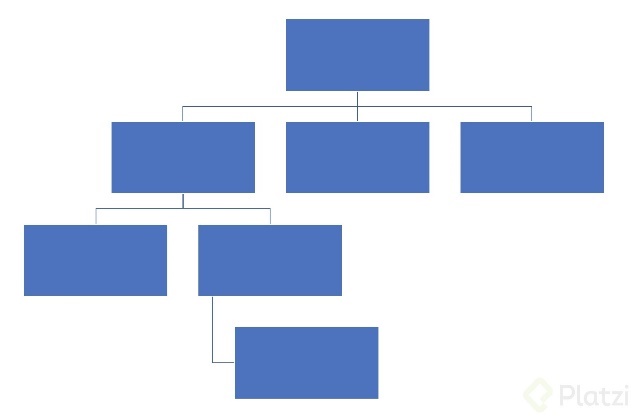
**Topología de malla.**



En las topologías de tipo malla todos los nodos están conectados entre sí, este tipo de conexión permite que cada nodo pueda actuar como servidor y como cliente.

Esta es una forma óptima de mantener la conexión entre dispositivos en una red, ya que se reduce a uno la cantidad de dispositivos por los que debe viajar la información y en caso de que un nodo de la red falle los datos pueden ser enviados por otro camino, lo que asegura disponibilidad.

**Topología de árbol.**



En esta topología contamos con varios dispositivos intermedios que permiten que otros nodos se conecten. Por ejemplo, podemos tener un punto inicial que recibe la conexión a Internet desde el *ISP* (Internet Service Provider o Proveedor de servicios de Internet), de allí viaja por el medio a un switch que distribuye a otros dispositivos que pueden ser nodos u otros dispositivos intermedios, switches, routers etc. quienes a su vez envían los datos a otros dispositivos iguales. La forma de la red se parece mucho a un árbol.

# Tecnologías de acceso a internet: Banda Ancha y velocidad de Internet.

Medidas para calcular el rendimiento de las redes:

* **Ancho de Banda**

**Capacidad** máxima de la conexión **para transferir bits**.

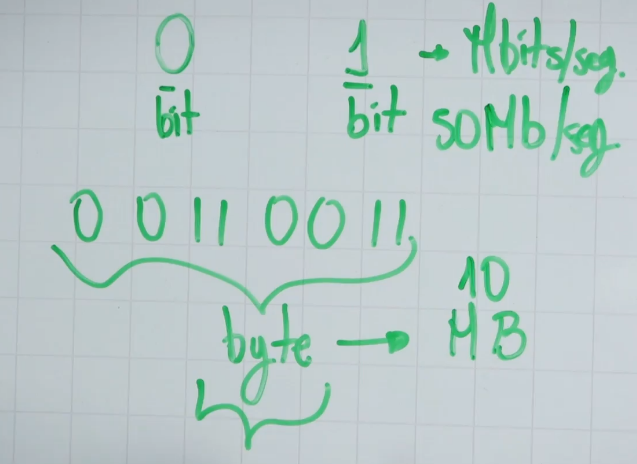
"En computación de redes, ancho de banda es la medida de datos y recursos de comunicación disponible o consumida expresados en bit/s o múltiplos de él como serían los Kbit/s,Mbit/s y Gigabit/s"

* **Velocidad de Internet**

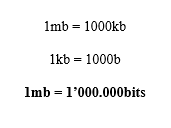
"Se define como el número de bits que se transmiten por unidad de tiempo a través de un sistema de transmisión digital o entre dos dispositivos digitales. Así pues, es la **velocidad de transferencia de datos**."

**Bit y Bytes.**

Debemos tener en cuenta que un **bit** puede ser un 0 o un 1 y que un **byte** es un conjunto de **8 bits.**



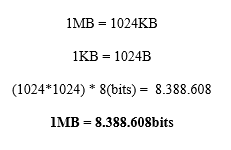
**Medidas en Bits.**

**1 Kilobit (Kb-Kbit)** = 1000 bits **(b)**  
**1 Megabit (Mb)** = 1000 Kilobits **(Kb)**

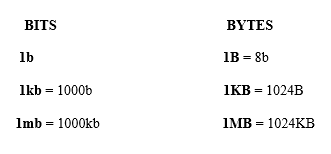
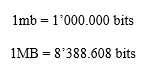
**En 1 Megabit hay 1’000.000 bits**

**Medidas en Bytes.**

**1 Byte (B)** = 8 bits **(b)** => Al byte también lo llaman octeto  
**1 Kilobyte (KB)** = 1024 Bytes **(B)**  
**1 Megabyte (MB)** = 1024 Kilobytes **(KB)**



**En 1 Megabyte hay 8’388.608 bits**



**Calcular velocidad real ofrecida por el ISP (Internet Service Provider)**

Cuando nuestro proveedor de Internet ya sea Claro/ETB nos ofrecen paquetes de velocidad lo que no sabemos es que el valor que nos dicen esta dado en mega**Bits** por lo que la velocidad real debe ser calculada en mega**Bytes.** Para ello debemos hacer la conversión correspondiente:

Teniendo en cuenta que:

Si Mi ISP me ofrece una velocidad de : 20 Mbps

De Mb -> B  
20 Mb = 2 500 000 B

De B a KB  
2 500 000 B = 2441.41 KB

De KB a MB  
2441.41 KB = 2.44141 MB

La velocidad real de transferencia de datos es de 2.44 MB/s

Para realizar un cálculo mucho más rápido solo tengo que dividir el numero ofrecido de velocidad 20 Mbps en este caso, en 8.4.

30 Mbps / 8 = 3.75 MB/s 1GB x 5min aprox.

40 Mbps / 8 = 5 MB/s 1GB x 3min aprox.

50 Mbps / 8 = 6.25 MB/s

60 Mbps / 8 = 7.5 MB/s

80 Mbps / 8 = 10 MB/s

# La Red Convergente.

Como su palabra lo indica **convergen**, en la que podemos trasmitir tanto la voz, los datos y video, por el mismo medio y ser utilizadas consecutivamente sin necesidad de una infraestructura para cada una de ellas, como era antes, además del menor coste de mantenimiento de las infraestructura.

Podemos poner como ejemplo las líneas ADSL, en las cuales conviven los tres servicios conjuntamente, por las cuales se transmite la voz por el medio de cobre, con el que convive la transmisión de datos, por los que además se transmiten los servicios de TV, como puede ser la televisión bajo demanda o streaming.

Eso es lo que podemos decir que es una red convergente. La interacción de varios servicios de comunicación por un solo medio.



**Ping o Latencia.**

Es el tiempo que tarda en transmitir un paquete dentro de la red.

# Instalación de Packet Tracer, emulador de redes.

Existe software que nos permite hacer simulación de redes, de forma que podamos probar todos los casos antes de hacer las implementaciones reales.

Para este curso vamos a estar usando Packet Tracer, este es un software que Cisco ofrece en versión de estudiante para que podamos aprender y practicar. Cisco es una de las empresas más grandes y quien manda la parada en cuanto a investigación y nuevos desarrollos en el tema de redes. Sus dispositivos son ampliamente usados en entornos empresariales y además ofrece a quien quiera aprender mucho contenido en su sitio [www.netacad.com](http://www.netacad.com).

Uno de los contenidos que te recomiendo está aquí: [Packet Tracer](https://www.netacad.com/courses/packet-tracer). Este es un curso gratuito que te va a abrir un mundo de oportunidades. Y además nos va a ayudar para que continuemos con nuestro curso de redes.

Entra al link que te dejé antes y enrólate al curso. De esta forma vamos a poder descargar e instalar Packet Tracer. [La instalación](https://www.netacad.com/courses/packet-tracer-download/) es realmente sencilla, unas vez que hayas hecho el registro en Netacad vas a encontrar en los recursos del curso el instalador para tu sistema operativo, lo descargas y sigues las indicaciones del asistente.  
Packet Tracer no está disponible para dispositivos con IOS por eso estaremos trabajando las simulaciones en Windows.

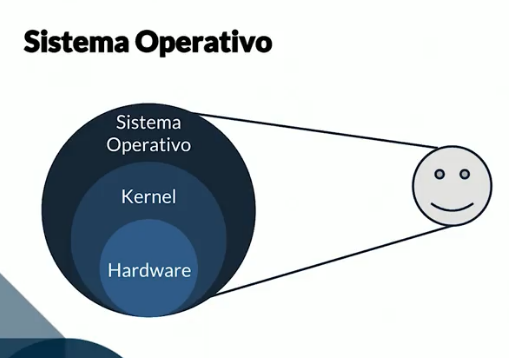
<https://www.netacad.com/courses/packet-tracer/introduction-packet-tracer>

<https://www.computernetworkingnotes.com/ccna-study-guide/download-packet-tracer-for-windows-and-linux.html>

# Métodos de acceso a los dispositivos

En este curso vamos a hacer configuraciones en algunos equipos.

Durante el curso vamos a usar imágenes como simulaciones de redes. Cisco tiene todo un programa de certificación en redes. Vamos a usar estas imágenes como los fierros que se usan a gran escala. El sistema operativo es como nosotros accedemos al kernel.



**Existen tres tipos de accesos.**

**Accesos por cable de consola:** Conectar con cable, a través de una pc. Probablemente el más seguro, pero poco práctico ya que es necesario llevar una pc al lugar físico donde está el hardware.

**Acceso por Telnet:** El protocolo Telnet, acrónimo de “Telecommunication Network”, es un protocolo de red que permite comunicarse en modo texto con otra máquina de manera que podamos controlarla de forma remota. Este protocolo se basa en la arquitectura cliente-servidor, donde el servidor será el ordenador que vamos a manejar y el cliente el ordenador desde el que vamos a controlar el servidor.

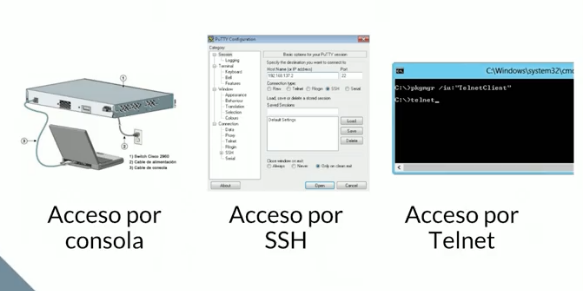
Este es un protocolo muy simple, sin embargo, cuenta con grave problema de seguridad, y es que las conexiones no son seguras, y el tráfico viaja sin cifrar.

**Accesos SSH:** Es una forma inalámbrica de conectarse, es más segura que a través de telnet, pero hay que configurar para poder ingresar. Esta se hace por primera vez a través de cable.

SSH o Secure Shell, es un protocolo de administración remota que permite a los usuarios controlar y modificar sus servidores remotos a través de Internet. El servicio se creó como un reemplazo seguro para el Telnet sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada. Proporciona un mecanismo para autenticar un usuario remoto, transferir entradas desde el cliente al host y retransmitir la salida de vuelta al cliente.

Cualquier usuario de Linux o macOS puede hacer SSH en su servidor remoto directamente desde la ventana del terminal. Los usuarios de Windows pueden aprovechar los clientes SSH como Putty. Puede ejecutar comandos shell de la misma manera que lo haría si estuviera operando físicamente el equipo remoto.

Por defecto SSH usa el puerto 22 y Telnet utiliza el puerto 23, una medida básica de seguridad es configurarlos en otros puertos que no sean los establecidos por defecto.



# Práctica: Navegación por el sistema operativo, comandos y privilegios

el primero es el Modo usuario: permite consultar toda la información relacionada al router sin poder modificarla la podemos identificar porque va tener al final un símbolo de mayor que menor que  
Router >

el segundo modo es el++ Usuario privilegiado++:se va a poder visualizar el estado de la configuración del routers o dispositivos con comando show y debugs aunado de que en este modo se habilitan las opciones copy y eraser para modificar la imagen del equipo lo identificas por un símbolo gato al final, este, accedes con el comando enable  
Router >enable  
Router #

el tercer modo es Modo de configuración global: el cual te permite usar todos los demás comandos de configuración del equipo lo identificas por la sintaxis entras a este modo usando el comando  
Router#configure terminal  
Router (config) #

para poner contraseña a modo de usuario privilegiado seria ingresar desde modo de configuración global

router(config)#enable secret platzi  
donde platzi sería la contraseña

otro forma de dar una contraseña al modo privilegiado  
es  
router(config)#enable password platzi

al ser un dispositivo de capa 2 se crea una SVI(Switch Virtual Interface)  
para darle una dirección ip al switch por lo regular este proceso se da mucho para dar una ip de managment a los switches o soportar protocolos de enrutamiento \*switches capa 3

interface vlan 1 (numero de la vlan a la cual se le va a crear la svi)  
ip address 192.168.168.1.2 255.255.255.0 (comando para ingresar una ip a una interfaz ip address seguido de la ip y de su máscara en este caso de 24)  
no shutdown (a diferencia de otros productos este comando significa que queremos levantar la interfaz o shutdown en dado caso que queremos dar de baja la interfaz)

<https://sites.google.com/site/retamarcisco/lista-de-comandos-y-funciones>

# Suites de protocolos.

Una suite de protocolos es un conjunto de protocolos que nos ayudan desde las diferentes capas y servicios de la red a garantizar que la información viaja de un lugar a otro, de forma segura y confiable, algunos de estos sirven para garantizar que la información es entregada o no como lo son TCP y UDP.

En la siguiente clase estaremos hablando de los modelos de referencia para la transmisión de datos en Internet, el modelo OSI y el modelo TCP/IP. Veremos que son similares y una de las cosas por las que esto es así es porque los protocolos que ambos usan en sus capas son protocolos abiertos, de uso libre, de forma que pueden estar implementados en cualquier dispositivo de hardware o a través de software.

A continuación listo algunos de los protocolos usados en las diferentes capas de red y su funcionamiento:

## **De la capa de Acceso a la Red (TCP/IP) / Física + Enlace de Datos (OSI)**

**ARP**

Es el protocolo que permite hacer la asignación de direcciones físicas y direcciones lógicas en el modelo OSI funciona en la capa de Enlace a Datos en la capa lógica.

**Ethernet**

Es el protocolo que nos permite definir los estándares relacionados con los medios cableados y la señalización en la capa física.

**Controladores de NIC**

Corresponde a la definición de los algoritmos que llevan las instrucciones a la máquina para recibir y enviar datos a través de la tarjeta de acceso a Internet del dispositivo.

## **Capa de Internet (TCP/IP) / Capa de Red (OSI)**

**IP**

Protocolo de Internet, es el protocolo encargado de la asignación de direcciones lógicas a los dispositivos, recibe los segmentos de la capa de transporte y los direcciona a través de la red.

**NAT**

Network Address Translation, este protocolo hace la traducción de direcciones IP privadas en direcciones IP públicas únicas globalmente.  
Es un protocolo que permite a los routers enviar mensajes a través de Internet. Cada dispositivo en la red LAN sale a Internet a través de un dispositivo llamada Router que contiene un listado de direcciones IP privadas vs direcciones IP públicas.  
Cuando un host quiere enviar un mensaje a un dispositivo externo el router determina a través de NAT a donde debe enviar.  
Con el uso de direcciones IPv6 se espera que el uso de este protocolo no sea necesario ya que es posible asignar a cada host en el mundo una dirección lógica única.

**ICMP**

Este protocolo apoya al protocolo IP proporcionando mensajes y notificaciones de error cuándo un mensaje no puede alcanzar su destino. Valida que el mensaje haya alcanzado su destino, valida también si el tiempo de vida del mensaje ya ha sido superado entre otras cosas. Su labor es únicamente informar sobre el error sin ejecutar acción alguna para resolverlo.

## **Capa de Transporte (TCP/IP) / Capa de Transporte (OSI)**

Los protocolos de esta capa son TCP y UDP, de ellos estaremos hablando más adelante en el curso.

## **Capa de Aplicación (TCP/IP) / Capa de sesión + Capa de Presentación + Capa de Aplicación (OSI)**

**DNS**

Domain Name System, es el protocolo encargado de hacer la traducción de direcciones IP (172.217.14.163) en textos que podamos leer y recordar fácilmente como [www.google.com](http://www.google.com)

**DHCP**

Es el protocolo encargado de asignar direcciones IP de forma dinámica a los dispositivos. Está pendiente de liberar las direcciones cuando estás ya no están siendo usadas.

**SMTP**  
Este es un protocolo de **envío** de correo, pongo en negrita la palabra porque este es precisamente su funcionamiento, tanto desde los hosts como desde los servidores, el protocolo SMTP es en encargado de **enviar los mensajes**.

**POP**

Junto con IMAP, POP es un protocolo encargado de la recepción de los mensajes en el dispositivo de destino. POP descarga los mensajes desde el servidor a tu pc y son eliminados del servidor. Si recibes un mensaje usando el protocolo POP ese mensaje puede ser consultado sin conexión a Internet luego de ser descargado al pc, pero si se borra de tu pc ya no hay manera de recuperarlo.

**IMAP**

El otro protocolo para recuperación de correo, en este caso los mails son revisados desde el servidor, de forma que se requiere conexión a Internet para leer los mensajes, puedes acceder a tus mails desde diferentes dispositivos y no tienes que preocuparte por la recuperación ya que el servidor realiza copias de seguridad para garantizar que el mail sigue disponible.

**FTP/TFTP**

Son protocolos para transferencia de archivos.

**HTTP/HTTPS**

Este es tal vez el protocolo que todos sabemos que es familiar, porque es el que usamos todo el tiempo siempre que estamos consultando información en internet. El protocolo HTTP es el conjunto de reglas que definen la forma en que son enviados los mensajes para el intercambio de texto a través de la red.

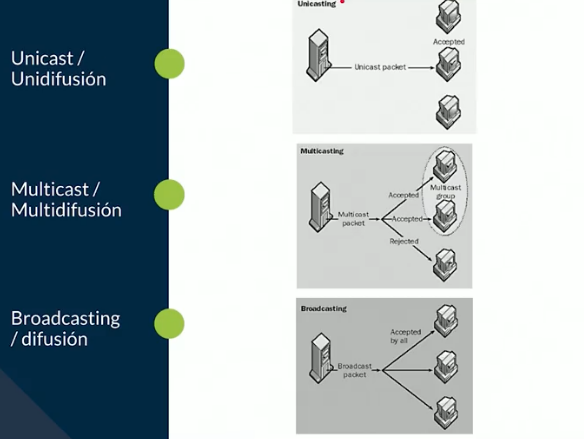
# Aspectos básicos de comunicación.

Los elementos básicos de la comunicación son: El emisor, el mensaje, el canal o el medio y el receptor. Los protocolos son las normas que nos indican establecer una comunicación que sea efectiva. Necesitamos establecer protocolos que nos ayuden a ver que la información pase por todas las capas que tiene los procesos de comunicación.



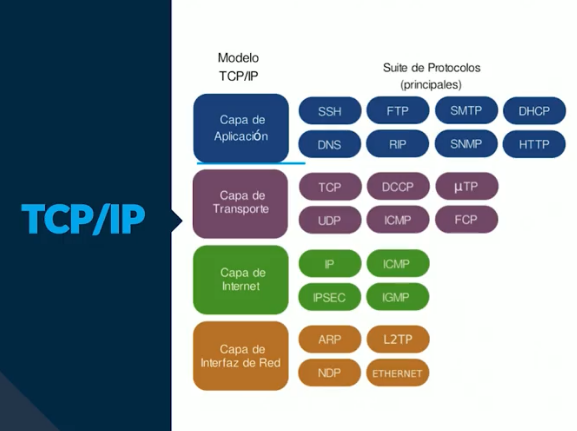
Los protocolos determinan las siguientes características:

* **Codificación del mensaje**
* **Formato y encapsulamiento del mensaje**
* **Tamaño del mensaje** : Las señales muy grandes no son transmitidos, son rechazados. El tamaño es importante y se es limitado.
* **Sincronización** : Contamos con protocolos que nos ayudan a determinar cuándo se está enviando un mensaje, cuando llego y cuando se puede enviar otro.
* **Opciones de entrega: Unicast** se le envía a un solo host, **Multicast** permite enviar a un grupo más pequeño, no a todos los host, **Broadcasting** nos envía paquetes a toda la red.



# Modelos de referencia Modelo OSI, modelo TCP/IP

Los modelos de protocolos de referencia son normas y estándares que nos ayudan a determinar las fases y los protocolos por los que la información va a viajar hasta llegar a su destino.





Si observamos ambos modelos nos podemos dar cuenta que casi siempre son las mismas capas.

**Capa Física**: Es la capa de los medios, son los cables, elementos que transmiten la información que transportan las señales y que llevan los mensajes

**Capa Enlace de datos**: Los equipos que hacen los direccionamiento. Estamos hablando de los medios físicos pero no del cableado sino de los dispositivos que nos permiten codificar y decodificar la información.

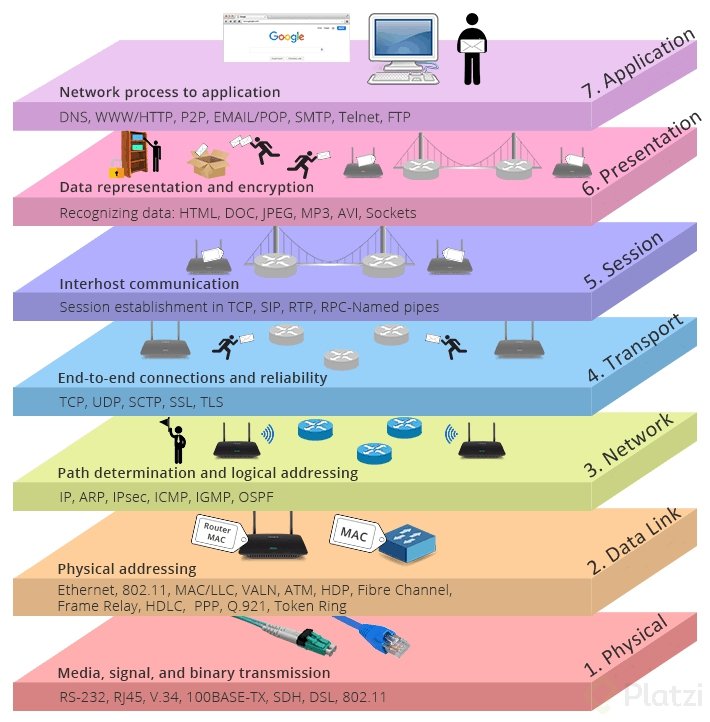
**Capa de Red**: es la capa que hace el direccionamiento lógico, el direccionamiento de IP.

**Capa de Transporte**: Nos da la conexión de extremo a extremo. Tiene los protocolos TCP (**T**ransmission **C**ontrol **P**rotocol) y UDP (**U**ser **D**atagram **P**rotocol) . Nos aseguran que el mensaje fue enviado y recibido.

**Capa de Sesión**: Es una capa que se abre y nos mantiene el flujo de información que nos permite la comunicación entre los dispositivos de red.

**Capa de Presentación**: Se refiere a la representación que tiene los archivos desde las aplicaciones.

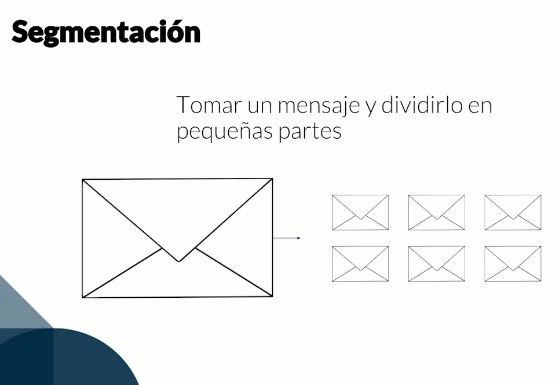
**Capa de Aplicación**: es la capa que tú ves, la que ves como usuario final



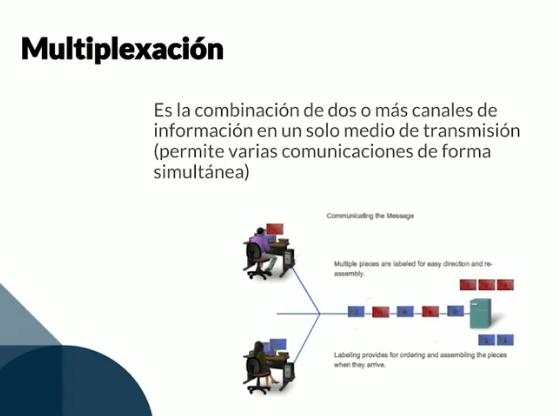
# Segmentación de los mensajes y Unidades de Datos de Protocolo PDU

Dos características que nos ayudan son el **tamaño** del mensaje y el **formato** del mensaje.

* La segmentación consiste en tomar un mensaje muy grande y dividirlo en mensajes más pequeños.



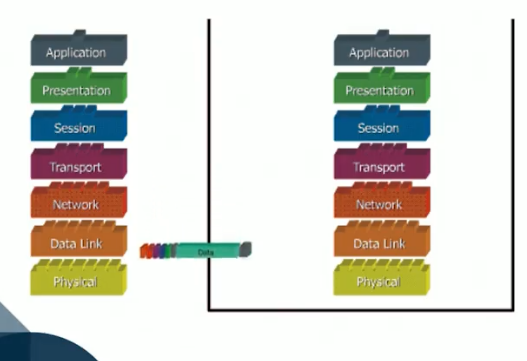
* La multiplexación es la combinación de dos o más canales de información en un solo medio de transición.



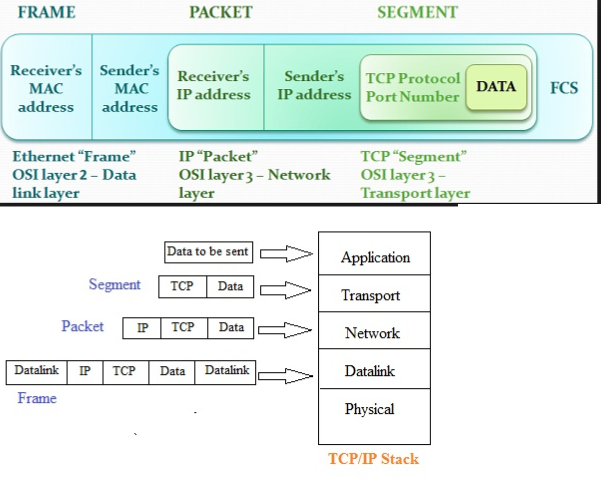
La multiplexión es compartir un canal con varias señales, es muy importante ya que es igual de caro mantener una línea con alto ancho de banda que una con bajo, por eso se pensó en la multiplexión, hay 3 formas principales de aplicarla.

* **Por división de frecuencia** : cuando se divide al ‘espectro’ en distintas bandas de frecuencia, en donde cada usuario puede usar una frecuencia distinta que no interfiera con las demás. En el mundo normal sería como que distintas personas en un bar hablan en distintos volúmenes de voz.
* **Por división de tiempo** : cuando cada usuario toma ‘turnos’ para recibir todo el ancho de banda y mandar su información. En el ejemplo de antes sería que en el bar cada persona tome su turno para hablar y las demás se queden calladas.
* **Por división de código** : En esta, cada usuario del canal usa una codificación distinta para hablar, de esta forma todos pueden usar el canal al mismo tiempo reduciendo la interferencia del canal. En los ejemplos anteriores sería que cada persona en el bar hable un idioma distinto.

**PDU** **P**rotocol **D**ata **U**nit es una unidad que nos permite identificar la información a medida que es transmitida a través de las capas de red.



La información **Data** que se está enviando, al estar recorriendo las distintas capas se le añadirán **unidades** (PDU) acorde vaya pasando entre capa y capa.



El PDU en la capa de **enlace a datos** se llama **Trama/Frame**

El PDU en la capa de **red** sería un **Paquete**

El PDU en la capa de **transporte** es un **Segmento**.

En la capa **física** (es decir los cables) ya estamos hablando de **bits.**

**(000100100110110101)**

# Practica: Wireshark para ver el tráfico de red.

# <https://www.wireshark.org/>

# 

# El switch y el AP

Recordemos que la capa Física y de medios de red es la que se encarga de hacer conexión entre dispositivos usando interfaces y direcciones físicas.

En esta capa contamos con varios dispositivos y vamos a ver cuáles son y sus diferencias.

### **El Switch**

Es el dispositivo que nos permite realizar conexiones físicas entre hosts, el switch se encarga de filtrar y direccionar los paquetes a través de la red de área local LAN.

El switch permite la conexión entre dispositivos a través del medio cableado.

Existe otros dispositivo que nos permite hacer la conexión de manera casi igual, es el Hub, incluso pueden verse iguales, pero yo te recomiendo no usar este dispositivo.

Mientras el switch toma los paquetes que llegan y analiza las direcciones físicas de los hosts conectados para reenviar el paquete únicamente a su destinatario el hub envía el mensaje por todos los canales, sin tener en cuenta el direccionamiento.

### **El Access Point AP**

Otro dispositivo de la capa física es el Access Point, este dispositivo es el encargado de realizar el enlace entre las redes cableadas y las redes inalámbricas. Nos permite crear redes LAN haciendo uso de las ondas de radio. **Redes Wifi**

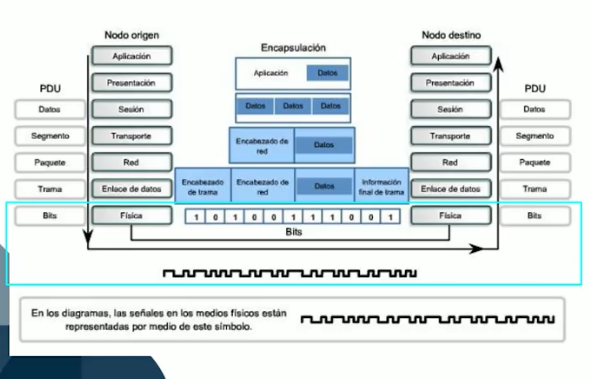
# ¿Cuál es la diferencia entre router, Access point y un modem?

Un **router** asigna una dirección IP a cada dispositivo que está dentro de la red LAN para que estas sean identificadas, y el **Access Point** crea una red inalámbrica(ejm: wi-fi) para interconectar dispositivos como los celulares que no cuentan con un puerto para conectar un cable de red.

El **modem** simplemente es un dispositivo que combina un **router** y un **A**ccess **P**oint.

# Capa Física: Elementos, funciones, transferencia de datos, ancho de banda, rendimiento

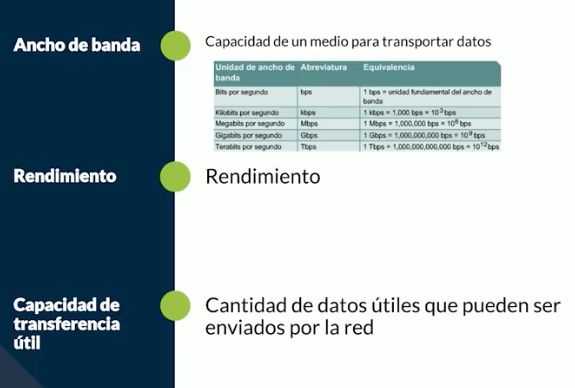
Para que logremos una conexión de red siempre depende de un cable. Aquí te muestro cómo la información está siendo transformada desde los bits hasta que toma la forma que espera el receptor.



Hay algunas organizaciones que regulan los estándares de la capa física como **TIA** y la **EIA**.



La capacidad de los medios para transportar los datos depende del ancho de banda, el rendimiento y la capacidad de transferencia útil.

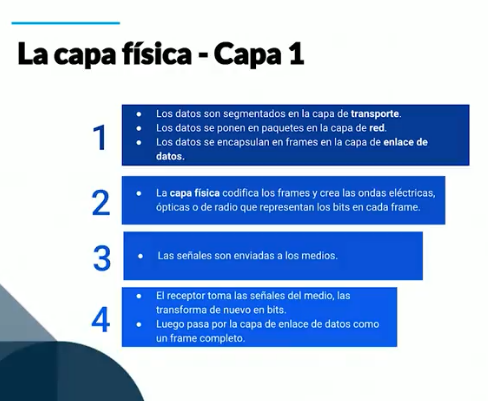


Para que haya una comunicación en red debe haber un medio, de esto se ocupa la capa física (cables u ondas de radio).

La capa física está compuesta por:

1. Cable de cobre
2. Cable de fibra óptica
3. Inalámbrico (ondas de radio)

**La Fibra Óptica** tiene poca interferencia, porque al no ser un medio que transporte electricidad, sino que envía impulsos de luz, este es inmune a las interferencias electromagnéticas (como lo puede ser un microondas, una lampara fluorescentes, una instalación eléctrica de alto voltaje)



**NIC**: Network Interface Card. Tarjeta de red se conecta a la tarjeta madre del computador, teléfono, otro y le proporciona los puertos y toda la parte física de circuitos y algoritmos que tiene.



# El cable de par trenzado.

En la clase anterior viste algunos de los elementos de la capa física y en esta lectura profundizaremos aún más en uno que es fundamental: el cable de par trenzado.

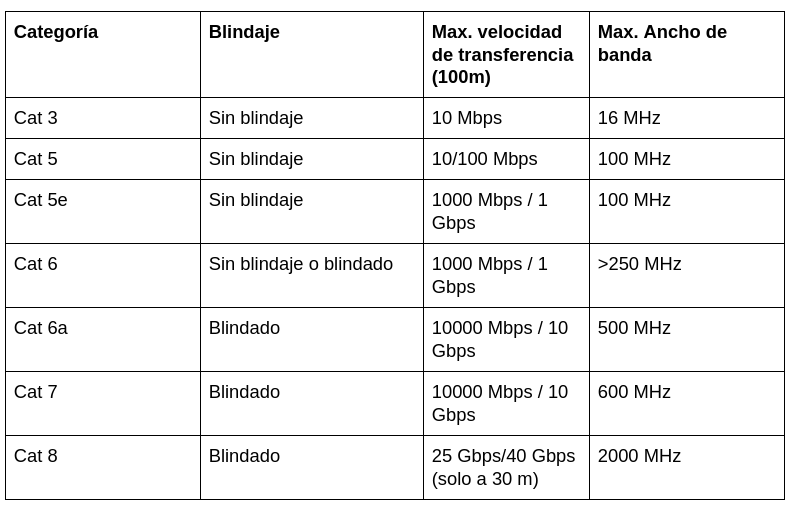
Este es el medio por el cual se transmite información entre dos dispositivos físicos de una red. Fue inventado en 1881 por Alexander Graham Bell y contiene dos conductores eléctricos que están fabricados normalmente de cobre.

Está diseñado para evitar la interferencia externa de señales y la diafonía de otros cables a su alrededor. Al ser un dispositivo físico este se ve limitado en sus propiedades de transmisión por la distancia. El rango en el cual se ve afectada la transmisión de información es de 100 metros.

# 

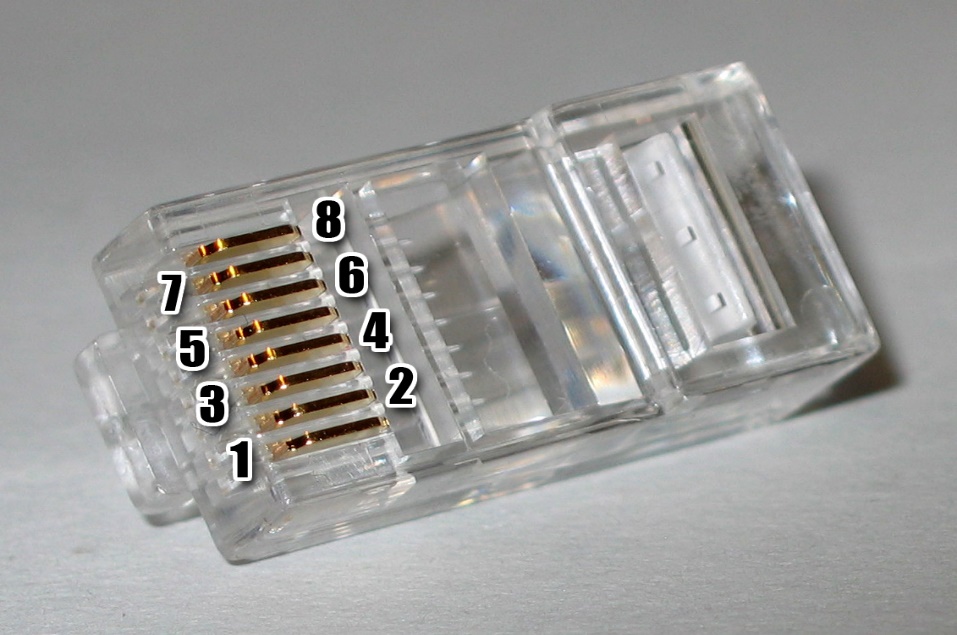
## **Categorías del cable de par trenzado**

Existen diferentes categorías de cables de par trenzado. Estas categorías están divididas principalmente en las velocidades de transferencia que pueden realizar, su ancho de banda y el blindaje que posee alrededor el cable para asegurar una mejor comunicación. Puedes ver más información en la siguiente tabla:



Las categorías que se usan normalmente para crear cables de red ethernet son de la categoría 5 a la categoría 6 por su costo y manipulación. Los cables de categorías superiores se usan en otro tipo de infraestructuras, además de que su costo es mucho más elevado.

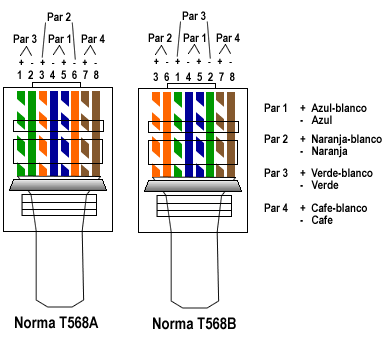
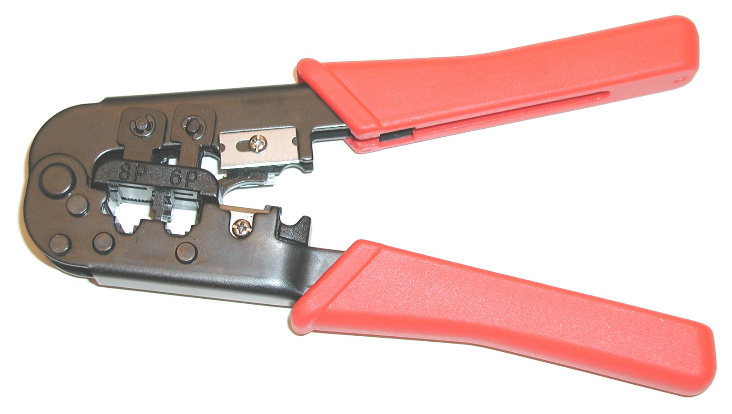
Para conectar dos dispositivos físicos en la red es necesario que al final de estos cables se inserte un conector RJ-45. Este conector cubrirá los 4 pares trenzados de cables asignando un pin a cada filamento, en total 8 pines numerados de la siguiente forma:



## 

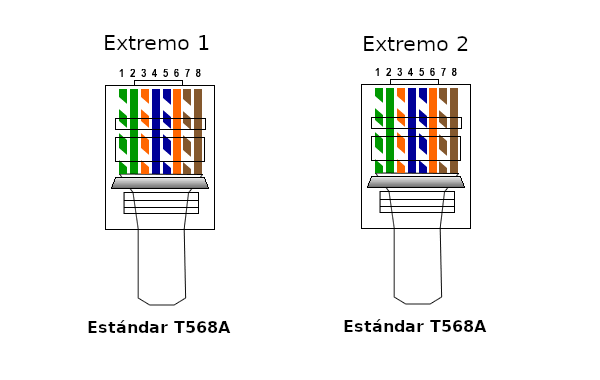
## **Crear la conexión de pines en un conector RJ-45**

# Existen diferentes estándares que se pueden seguir para configurar el orden de los cables dentro de un conector RJ-45, los más comunes son el estándar T568A y T568B, el estándar más común de usar es el T568A. La única diferencia entre estos dos estándares es la posición de los cables verdes y naranjas cómo se ve a continuación:



Una vez tienes configurados los pines dentro de tu conector, lo siguiente es sellar los cables con los pines a través de una herramienta especial llamada pinza ponchadora.

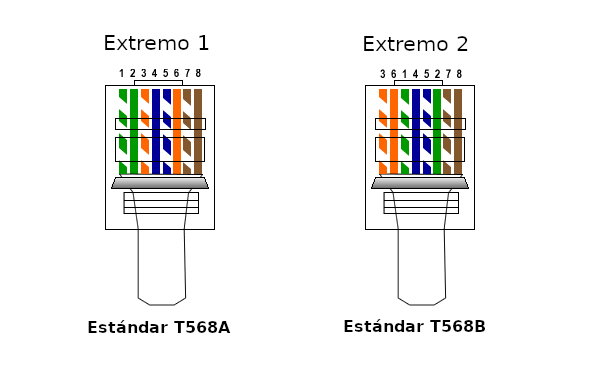
Pero esto no es todo para que nuestro cable de red funcione, para ello debemos saber si los dispositivos son del mismo tipo, por ejemplo de un PC a otro PC. Si estos son diferentes (de un PC a un router) se usa una configuración diferente en cada extremo. Dependiendo del caso usaremos un cable directo o un cable cruzado.



**Cable cruzado.**

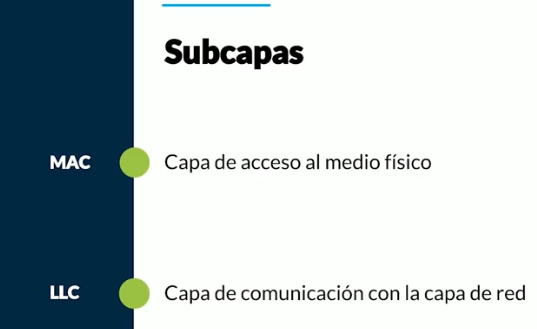
Este cable se utiliza cuando queremos conectar dos **dispositivos similares**, como dos computadoras, dos routers o dos hubs. Se llama cruzado pues la dirección cambia de un extremo a otro.

La configuración de pines debe ser diferente en ambos extremos del cable y es aquí donde vemos la utilidad de que existan dos estándares diferentes. En un extremo usaremos el estándar T568A y en el otro el T568B. En la siguiente imagen puedes ver un ejemplo más claro:



Con esto ya eres capaz de hacer un cable de red conociendo sus limitaciones y capacidades. Elige el cable que más le convenga al diseño de tu red y en la siguiente clase veremos cómo construirlo de manera física.

# Capa de enlace de datos: Elementos, funciones.

Es la que se encarga de comunicar la parte física con la parte lógica. Dentro de esta capa se encuentran otras dos subcapas que son:

**MAC**: Capa de acceso al medio físico. Esto es una dirección que identifica únicamente a cada una de las tarjeta de red que tiene nuestros dispositivos.

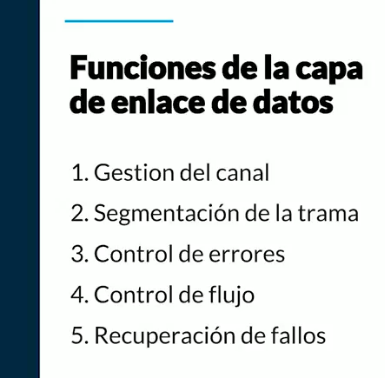
**LLC**: Capa de acceso lógico, esta capa es la que nos permite pasar los datos de forma lógica, transformarlos para que la capa de red pueda recibirla.

**Funciones.**

**Gestión del canal:** la capa va a contar con protocolos que le permiten a la señal decir si va a un solo canal o si es dúplex o full dúplex.

**Segmentación de la trama**: El tamaño del mensaje no puede ser muy grande ni muy pequeño. Verifica que no sean tramas muy largas ni cortas.

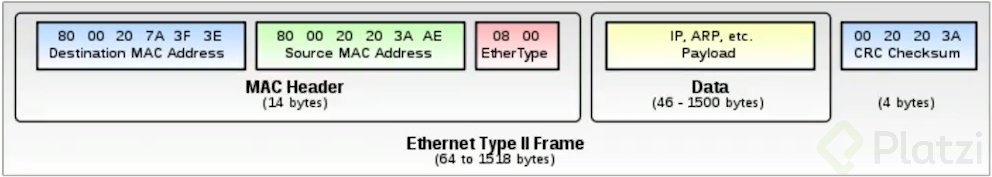
**Control de errores y recuperación de fallos**: Lo que hace es poner caracteres que nos ayudan al final de la trama para identificar si esos datos llegaron completos, si se agregó información por el camino o si se perdió.



# Trama de enlace de datos y direcciones mac

El protocolo ethernet se encarga de la gestión de direcciones físicas que nos ayudan a conectar con la capa lógica y la capa física. Está compuesta por un encabezado (direcciones físicas), datos (traen información de la capa de red y la capa de transporte) y tráiler.

**Trama de ethernet**

* Conecta la parte física con la parte lógica.
* Partes:  
  

**Direcciones MAC**

En las redes de computadoras, la dirección MAC es un identificador de 48 bits que corresponde de forma única a una tarjeta o dispositivo de red. Se la conoce también como dirección física, y es única para cada dispositivo.

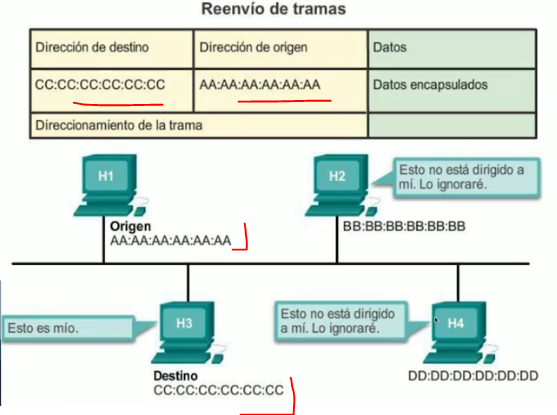
* Dirección física
* Identificador único de la NIC (Tarjeta de red en cada dispositivo).
* 12 dígitos hexadecimales.





# Procesamiento de tramas.

Ya sabemos que cada dispositivo que esta conectado a la red (celular, computador, etc) o equipos de red (switches, routers,APs, etc) son denominados **hosts**. Todos estos dispositivos tienen una dirección **MAC** que esta vinculada con su tarjeta de Internet **NIC** y que es única. Entonces vamos a ver como es el proceso que tiene una trama/frame desde que sale de un dispositivo hasta que es encontrado por el dispositivo de destino.



La dirección MAC suele denominarse “dirección física” (BIA) porque, históricamente, se graba en la ROM (memoria de solo lectura) de la NIC. Esto significa que la dirección se codifica en el chip de la ROM de manera permanente (el software no puede cambiarla).

BIA = bourned in address  
Dirección “quemada” en el hardware de la NIC

**Nota**: en los sistemas operativos de PC y en las NIC modernos, es posible cambiar la dirección MAC mediante software. Esto es útil cuando se trata de acceder a una red que filtra sobre la base de la BIA. Esto quiere decir que el filtrado o control del tráfico sobre la base de la dirección MAC ya no es tan seguro como antes.

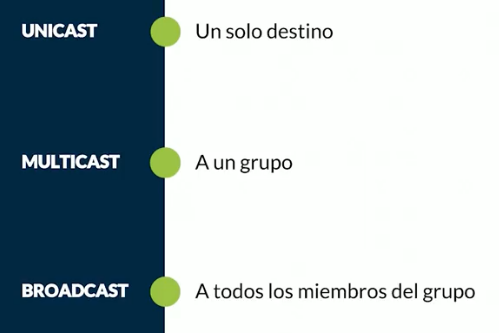
Las direcciones MAC se asignan a estaciones de trabajo, servidores, impresoras, switches y routers, es decir, a cualquier dispositivo que debe originar o recibir datos en una red. Todos los dispositivos conectados a una LAN Ethernet tienen interfaces con direcciones MAC. Diferentes fabricantes de hardware y software pueden representar las direcciones MAC en distintos formatos hexadecimales. Los formatos de las direcciones pueden ser similares a los siguientes:

00-05-9A-3C-78-00  
00:05:9A:3C:78:00  
0005.9A3C.7800

Cuando se inicia la PC, lo primero que hace la NIC es copiar la dirección MAC del ROM en la RAM. Cuando un dispositivo reenvía un mensaje a una red Ethernet, adjunta al paquete la información del encabezado. La información del encabezado contiene la dirección MAC de origen y destino. El dispositivo de origen envía los datos a través de la red.

Cada NIC en la red revisa la información en la subcapa MAC para ver si la dirección MAC de destino que está en la trama coincide con la dirección MAC física del dispositivo almacenada en la RAM. Si no hay coincidencia, el dispositivo descarta la trama. Cuando la trama llega al destino en que la MAC de la NIC coincide con la MAC de destino de la trama, la NIC pasa la trama a las capas OSI, donde se lleva a cabo el proceso de desencapsulación.

**Tipos de envíos.**



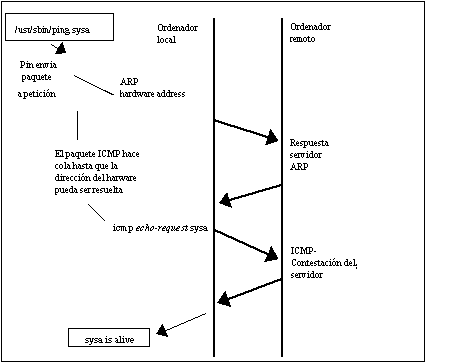
# Protocolo de resolución de direcciones

# Address Resolution Protocol (ARP).

# Ya vimos que con una combinación de dirección MAC y dirección IP podemos enviar paquetes a través de nuestra red, para ello contamos con el protocolo de resolución de direcciones ARP, este protocolo básicamente tiene dos funciones:

# Resuelve la resolución de conflictos entre la relación de direcciones IP y MAC es decir de direcciones lógicas de la capa de red y direcciones físicas de los dispositivos que estén conectados dentro de una red LAN

Cada dispositivo que está conectado a una red, tiene una tabla de cache ARP, que es la que se encarga de almacenar su dirección IP y MAC, por esto la otra funcion que tiene el ARP es mantener actualizada la tabla de cache ARP, su forma de efectuarlo es haciendo una consulta a todos los nodos dentro de la red, para verificar sus datos tanto el IP como la MAC, a los dispositivos que vaya consultando que sean nuevos se les agregara un cache ARP.



Por esto es importante recordar que cada dispositivo que tiene una dirección IP en una red Ethernet también tiene una dirección MAC Ethernet. Cuando un dispositivo envía una trama de Ethernet, esta contiene estas dos direcciones:  
**Dirección MAC de destino:** la dirección MAC de la NIC Ethernet, que es la dirección del destino final o del router.  
**Dirección MAC de origen:** la dirección MAC de la NIC Ethernet del remitente.

# Capa de Red.

Se encarga de enrutar los datos a través de diferentes redes. El **router** será el encargado de desencapsular y enrutar nuevamente las tramas. Las funciones principales son:

* Direccionamiento de paquetes – Asignación de direcciones lógicas
* Encapsulamiento de paquetes – Una vez vista la dirección vuelve a encapsular
* Enrutamiento – Determinar el siguiente salto
* Desencapsulamiento de los paquetes – Abre la trama para saber las direcciones  
  PDU de la capa de red (unidad de datos de protocolo)

Se asignan tres campos:  
Dirección de origen - ¿Quién envía la solicitud?  
Dirección de destino - ¿A dónde se envía el mensaje?  
TTL (**T**ime **T**o **L**ive) – Es un campo que nos indica la cantidad de saltos que va a dar un mensaje hasta que se determine que no llegará a ningún lado (regularmente se establece en 64 pero se puede cambiar)

# 

# Procesamiento de tramas.

**Un host**, cuando ha de enviar un paquete de datos a un destino, calcula, mediante la dirección IP de destino y la máscara de subred, a que red pertenece y en el caso de que no pertenezca a su red, mira en su tabla de routing, cual es la puerta de enlace, que es la dirección IP del siguiente salto (en este caso, el router), monta la trama acorde con el medio de transmisión y la envía.

**En el router**, se hace lo propio, desempaqueta la trama para averiguar cuál es la dirección IP del destino y vuelve a calcular, de acuerdo con la máscara de red de esa interfaz, a que red pertenece, para después, consultar en su tabla de routing (que se puede configurar do forma estática o mediante un protocolo de routing, como OSPF o RIP) cual es la interfaz por la que ha de enviarlo y en su defecto, cual es la interfaz predeterminada. Entonces, vuelve a montar la trama, acorde con el medio de ese interfaz, y así, hasta que llegue el paquete a destino.

# Para que haya comunicación de capa 2. Es decir en una red local es necesario tener la Ip y la máscara de subred.

# Para que haya comunicación de capa 3. Es decir en diferentes redes es necesario la dirección Ip, mascara subred y el Gateway.

# Puerta de enlace Predeterminada o Default Gateway: Es la ruta por defecto que se le asigna a un equipo y tiene como función enviar cualquier paquete del que no conozca por cual interfaz enviarlo y no esté definido en las rutas del equipo.

# 

# Protocolo IP Asignación de direcciones IP, máscara de bits.

**Protocolo IP Asignación de direcciones IP, máscara de bits**

El protocolo IP es el protocolo que básicamente nos permite hacer el direccionamiento y el enrutamiento de los mensajes a través de la red, a través de diferentes algoritmos, se encarga de trazar la ruta más eficiente para que los mensajes lleguen de un destino a otro.

**Enrutamiento**

Consiste en encontrar un camino que conecte una red con otro, ya vimos que esto se hace a través de la tabla de enrutamiento de los routers.

**Direccionamiento**

Se refiere a la forma en que se asignan las direcciones IP a los diferentes dispositivos, por ejemplo, la creación de subredes.

**Direcciones IP**

Es un identificador lógico de las interfaces de red de los dispositivos que utilizan protocolo IP para la comunicación.

IPv4 - 32 bits - 192.168.1.1  
IPv6 - 128 bits - 2001:0D88:000A:0000:0000:0000:0000:1000

Se pueden clasificar en diferentes clases.

**Clase A**

• El primer octeto identifica la red  
• Tres últimos octetos (24 bits) pueden ser asignados a los hosts  
• Cantidad máxima de hosts es 224 - 2  
• 167777214 hosts

**Clase B**

• Dos primeros octetos para identificar la red.  
• Dos octetos finales (16 bits) para que sean asignados a los hosts  
• Cantidad máxima de hosts por cada red es 216 – 2  
• 65534 hosts

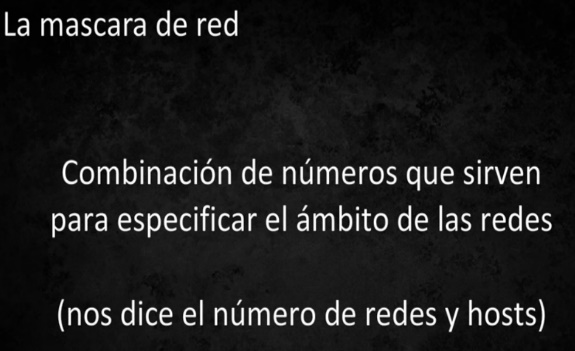
**Case C**

• Tres primeros octetos para identificar la red  
• Octeto final (8 bits) para que sea asignado a los hosts  
• Cantidad máxima de hosts por cada red es 28 – 2  
• 254 hosts

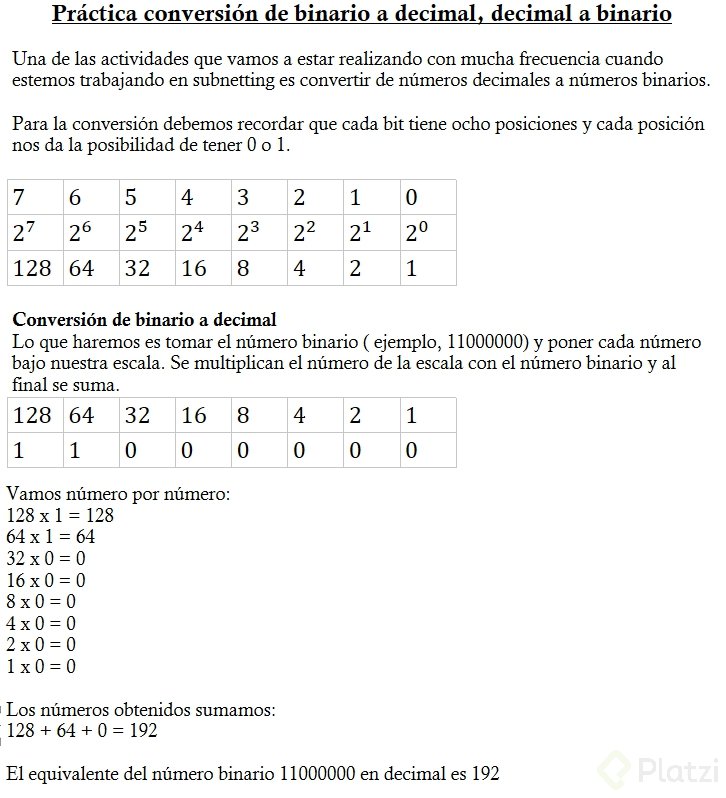
**Máscara de Subred**

Nos permite identificar a simple vista la porción de la dirección IP que se ha asignado a la identificación de la red y la porción que se ha asignado a los hosts.

A - 255.0.0.0 o 11111111.00000000.00000000.00000000.00000000  
B - 255.255.0.0 o 11111111.111111111.00000000.00000000.00000000  
C - 255.255.255.0 o 11111111.11111111.111111111.00000000.00000000

1. Direcciones privadas: no se pueden enrutar a través de internet.  
   a. 10.0.0.0/8 a 10.255.255.255  
   b. 172.16.0.0/16 a 172.31.255.255  
   c. 192.168.0.0/24 a 192.168.255.255
2. Direcciones de loopback  
   127.0.0.0/8 127.255.255.254
3. Direcciones de Link Local  
   169.254.0.0/16 169.254.254.254
4. Test  
   192.0.2.0/24

# 



# IPs Públicas y Privadas.

En las redes de área local se asignan direcciones a los dispositivos que permiten la conexión entre ellos. Las direcciones privadas son aquellas que no se pueden enrutar a través de Internet.

Las direcciones IP públicas son aquellas que permiten la conexión a Internet.

Todos los dispositivos que están atrás de un mismo router tienen diferentes direcciones IP privadas únicas en ese segmento de red y una dirección pública que permite la conexión entre diferentes redes alrededor del mundo, esta dirección ip pública es la dirección del router.

El segmento de direcciones privadas se encuentra entre

**10.0.0.0/8 a 10.255.255.255** que usualmente se asigna para redes con conexión inalámbrica ya que el rango es muy amplio y  
**192.168.0.0/16 a 192.168.255.255** que usualmente se asigna para redes conectadas por medio cableado, es importante resaltar que esto no implica ningún tipo de obligación o reserva de rangos, tú puedes asignar direcciones IP basándote en tus reglas de negocio.

# 

# Direccionamiento IP.

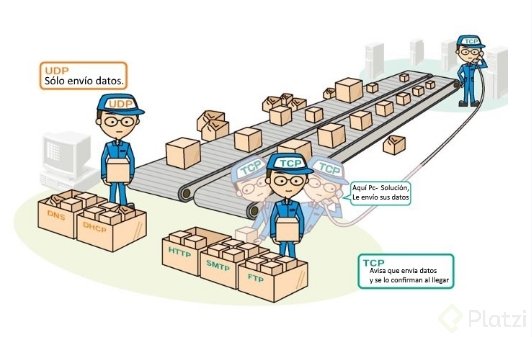
# 

# Capa de Transporte. Funciones, elementos protocolos, tareas.

# Es la que se encarga de definir cómo van a ser enviados los mensajes, de acordar o asignar puertos y establecer esos protocolos que nos van a ayudar a que el mensaje sea enviado o garantizar el envió del mensaje.

# Las funciones de esta capa son:

* Regula el flujo de información desde el origen hasta el destino.
* Segmentar los datos. (Segmentación)
* Agrega un encabezado en cada segmento.
* Re-ensamblaje.
* Pasa los datos a la aplicación correspondiente,
* Identifica las diversas conversaciones entre los host.
* Determina el protocolo que garantiza el envió del mensaje.
* Realizar el seguimiento de las conversaciones individuales.
* Identificar las aplicaciones de acuerdo con el puerto.

**Dispositivos que trabajan en esta capa:**

* Switch:
* Optimizadores WAN:
* Mejora el rendimiento de la red.
* Router + QoS:
* Prioriza cierto tráfico de red.

**Protocolos para el envio de datos**

* TCP (Protocolo de Control de Transmisión)
* UDP (Protocolo de datagramas de usuario)

# TCP y UDP.

# Protocolo TCP (Transmission Control Protocol)

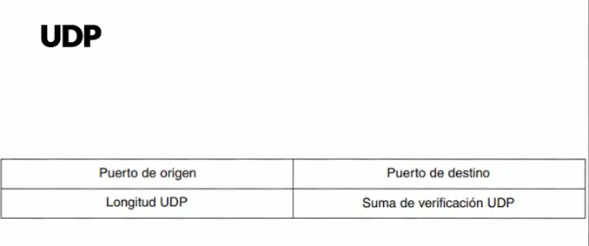
# Muchos programas dentro de una red de datos compuesta por computadoras pueden usar TCP para crear conexiones entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

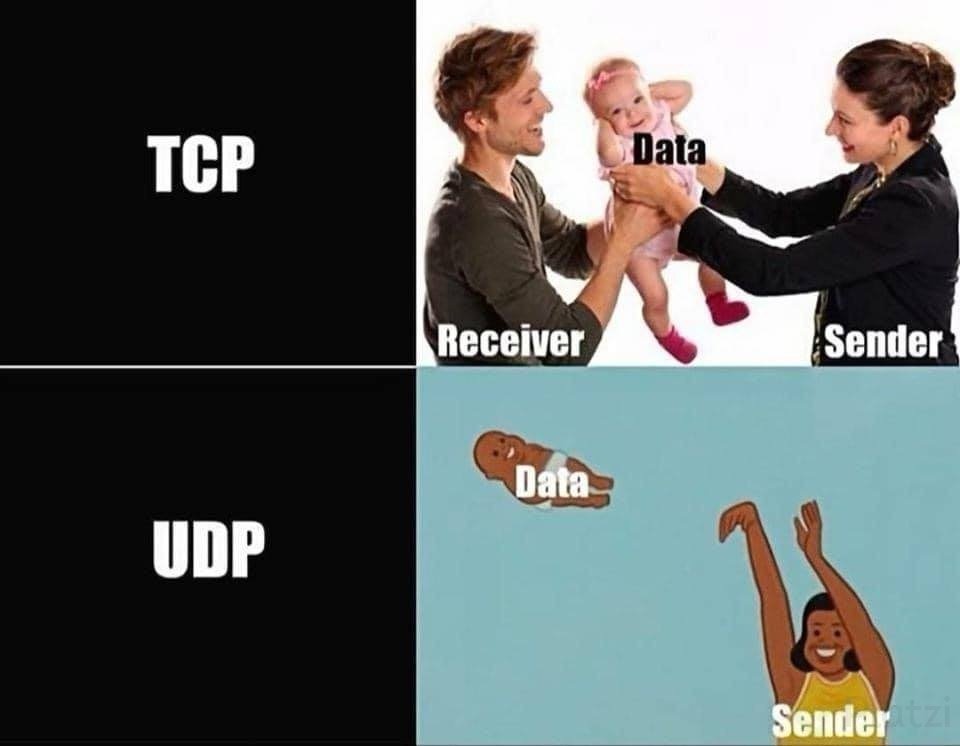
# Este protocolo es un poco más lento que el de UDP pero garantiza que toda la información sea enviada y recibida correctamente.

# Protocolo UDP (User Datagram Protocol)

# Es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

# Este protocolo es más rápido que por TCP pero este no garantiza que toda la información llegue correctamente.





# Capa de Aplicación.

La **Capa de Aplicación** es la que nos permite como usuarios acceder a los diferentes servicios que requerimos a través de la red. Esta capa nos da un acceso muy fácil y cómodo para que como usuarios podamos acceder y desarrollar nuestras actividades con tranquilidad a través de la red.

Algunos de los protocolos que se definen en la capa de aplicación son:

-> **DNS Domain Name System:** Se usa para la configuración de los nombres de red, como ya hemos visto los dispositivos tienen dos principales formas de ser identificados en la red la dirección MAC y la dirección IP ya sea v4 o v6, como seres humanos es difícil recordar tantos números, es más fácil recordar nombres con palabras, esto es lo que hace este protocolo, asignar nombres en texto a las direcciones de los dispositivos en la red.

-> **HTTP y HTTPS** protocolos de transferencia de hipertexto: Es el protocolo que transforma los mensajes de forma que puedan ser enviados y recibidos en sitios web. .

–> **SMTP y Protocolos de transferencia por correo**: Se usan para el envío de mensajes y archivos adjuntos a través de correo electrónico.

-> **DHCP** Protocolo de configuración dinámica de host: Se usa para asignar IPs, máscara de subred, dirección de gateway y DNS dinámicamente a los dispositivos que se conectan a la red.

–> **FTP** Protocolo de transferencia de archivos: Se utiliza para el envío de archivos entre dispositivos en la red.

**Funciones de la capa de Aplicación**

1. Codificación y conversión de los mensajes que serán enviados
2. Compresión de los datos
3. Encriptación de los mensajes que serán enviados de forma segura

*Important Questions and Answers.*

