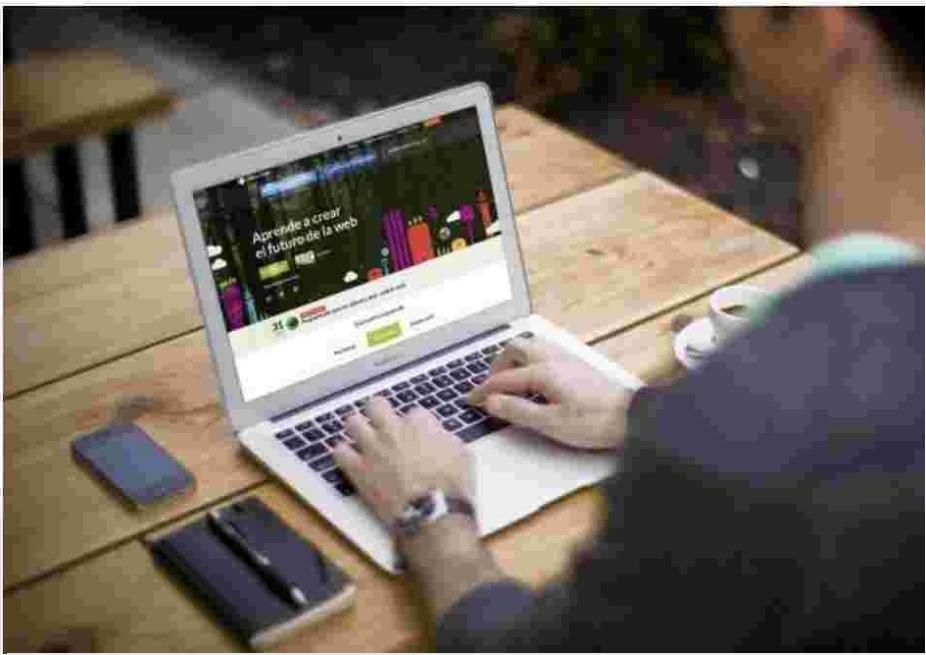


Bienvenido al

---

# Curso de Fundamentos de Redes y Conectividad

Mcs. Diego Yáñez





Cómo funciona la  
comunicación en redes



Modelos de referencia de protocolos  
de Internet OSI y TCP/IP

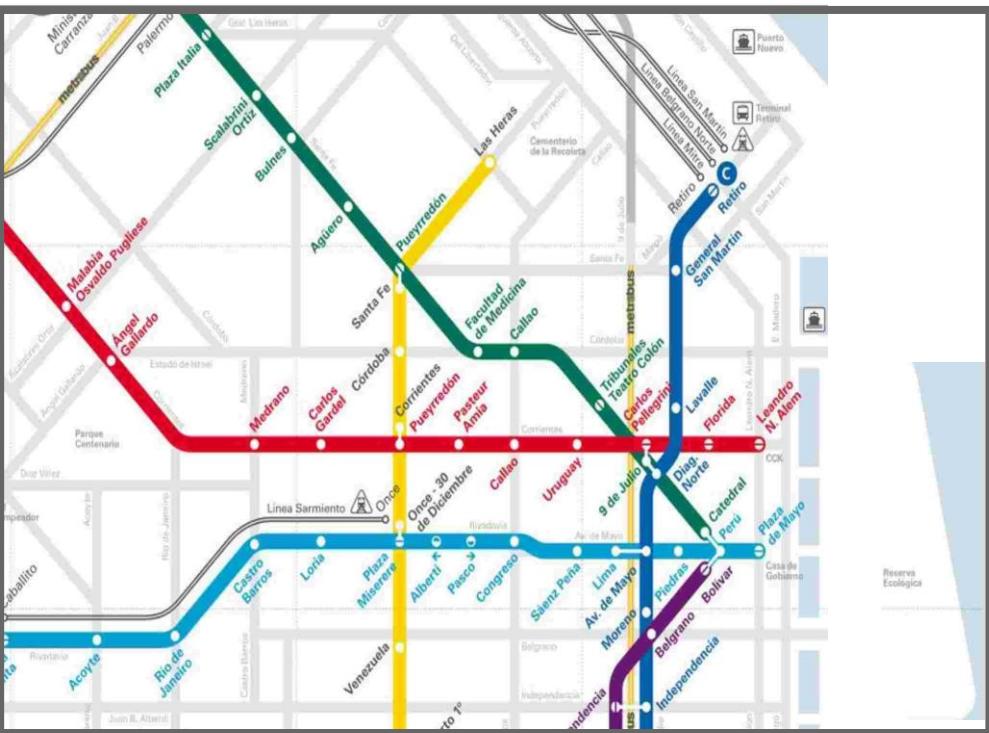
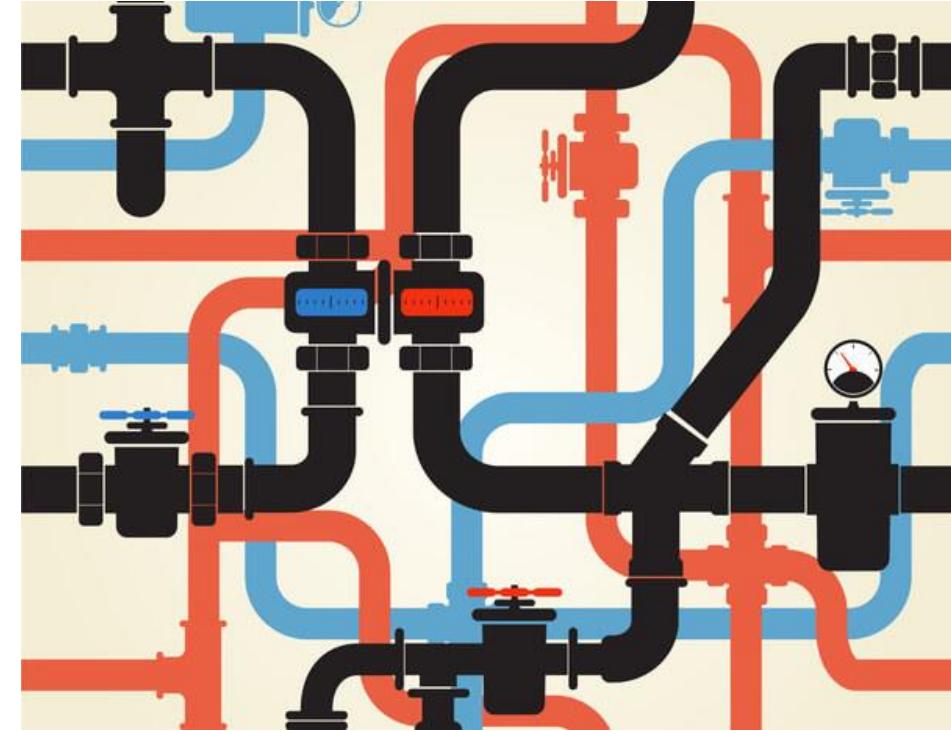


Diseño de redes y configuración  
de dispositivos

---

# Exploraremos la red

¿Qué es la RED?





Objetivo:  
Transportar  
algo de un  
lugar a otro

Punto de  
partida y  
llegada

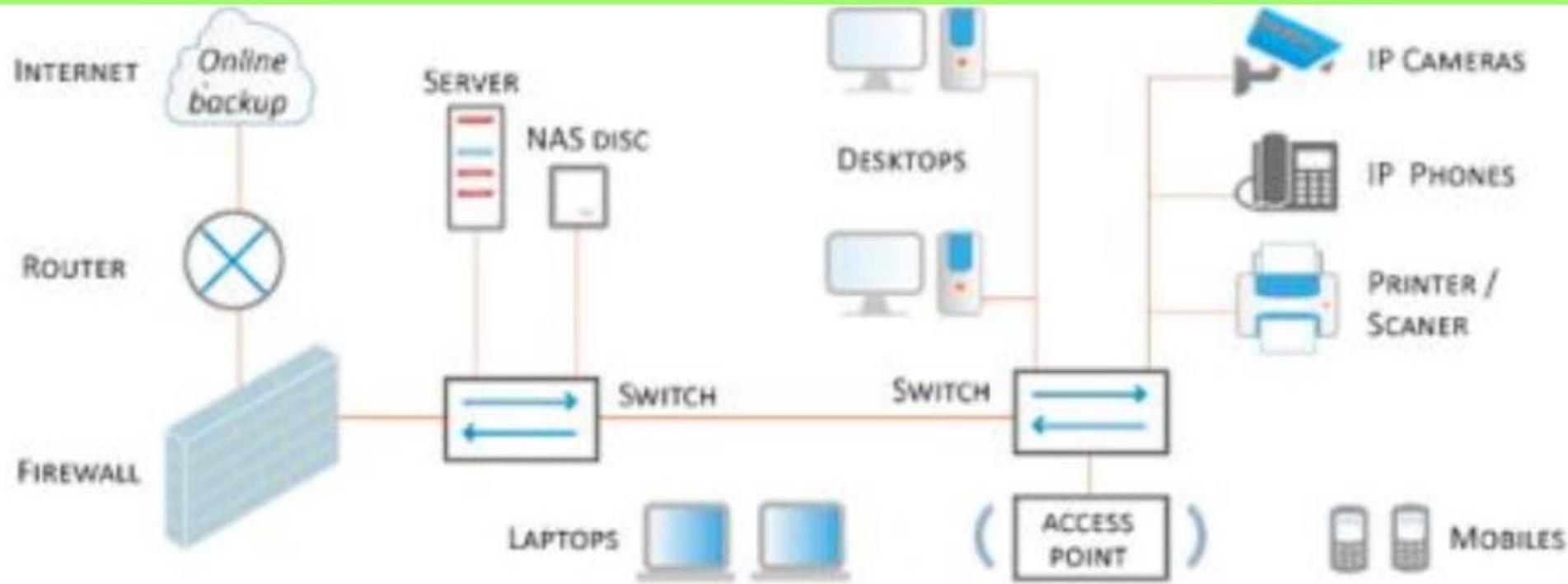
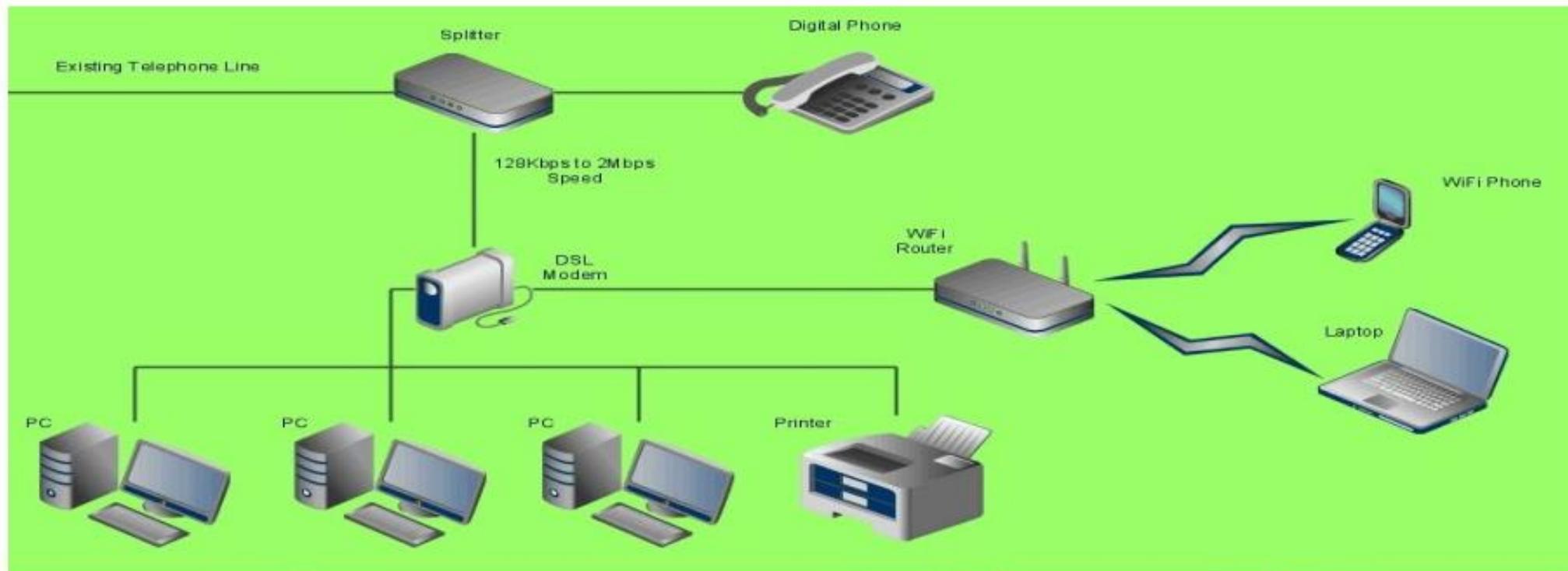
Puntos  
conectados  
por un medio

“

Una red de computadoras es un conjunto de equipos informáticos y software 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, con la finalidad de compartir información, recursos y ofrecer servicios.

”

Tanenbaum  
Redes de Computadoras



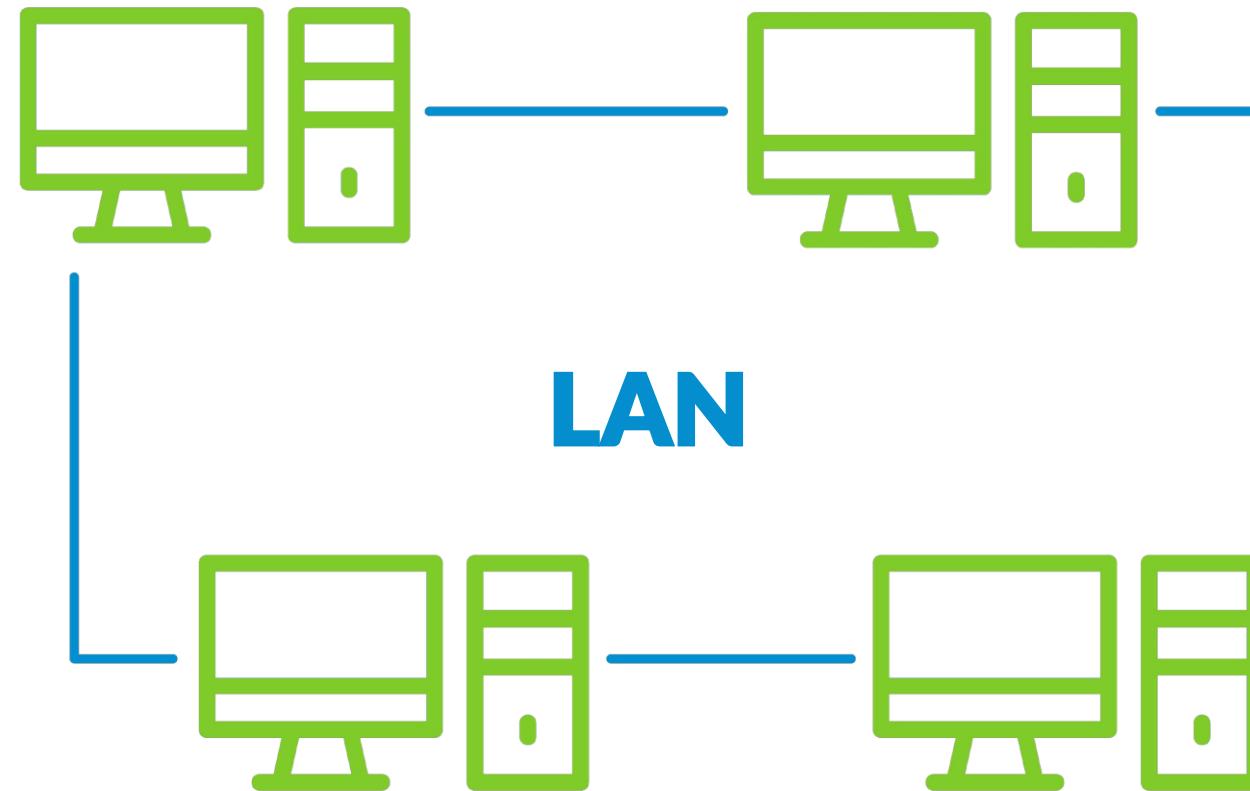
---

# Tipos de redes

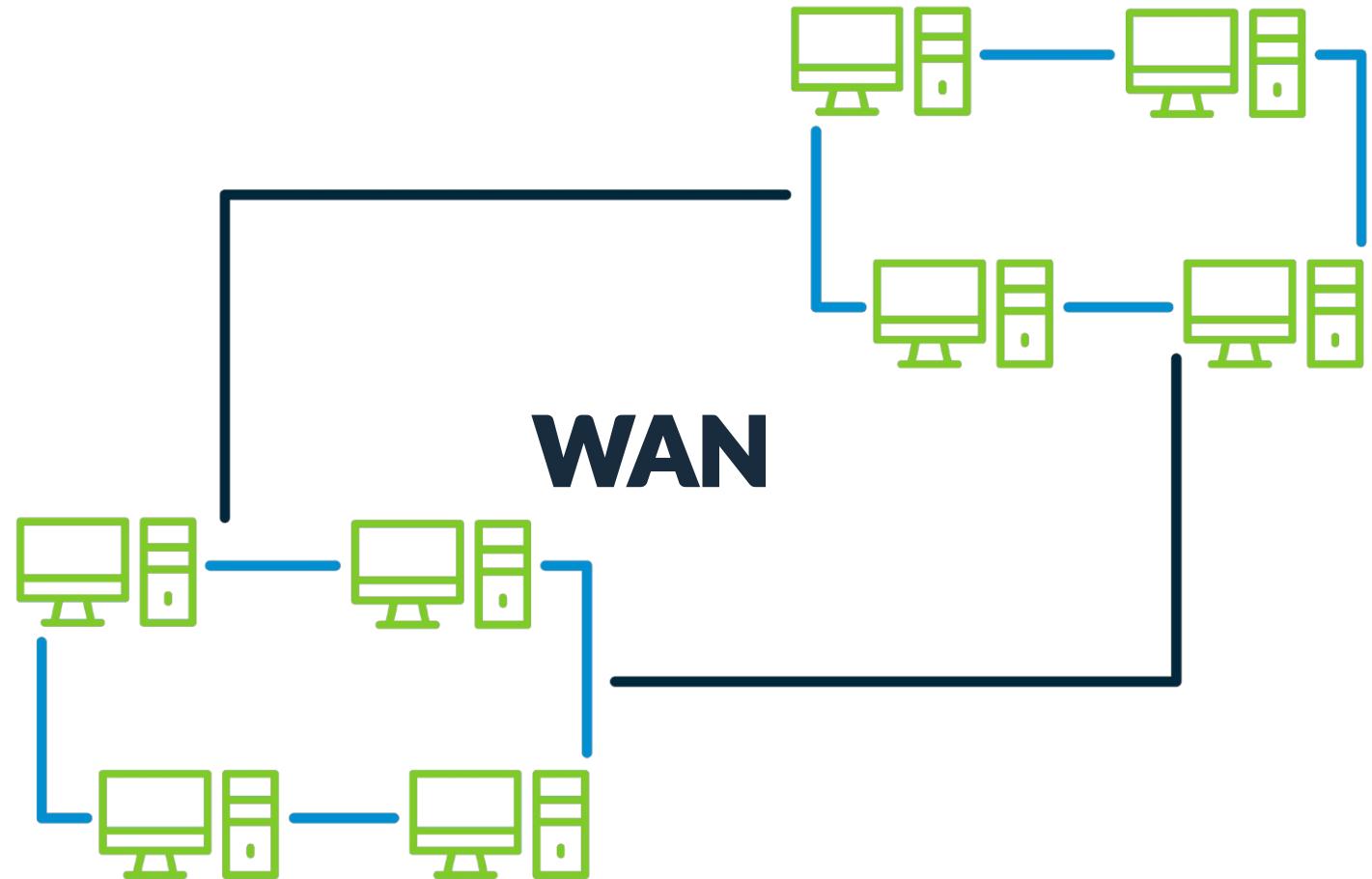
LAN, WAN, MAN

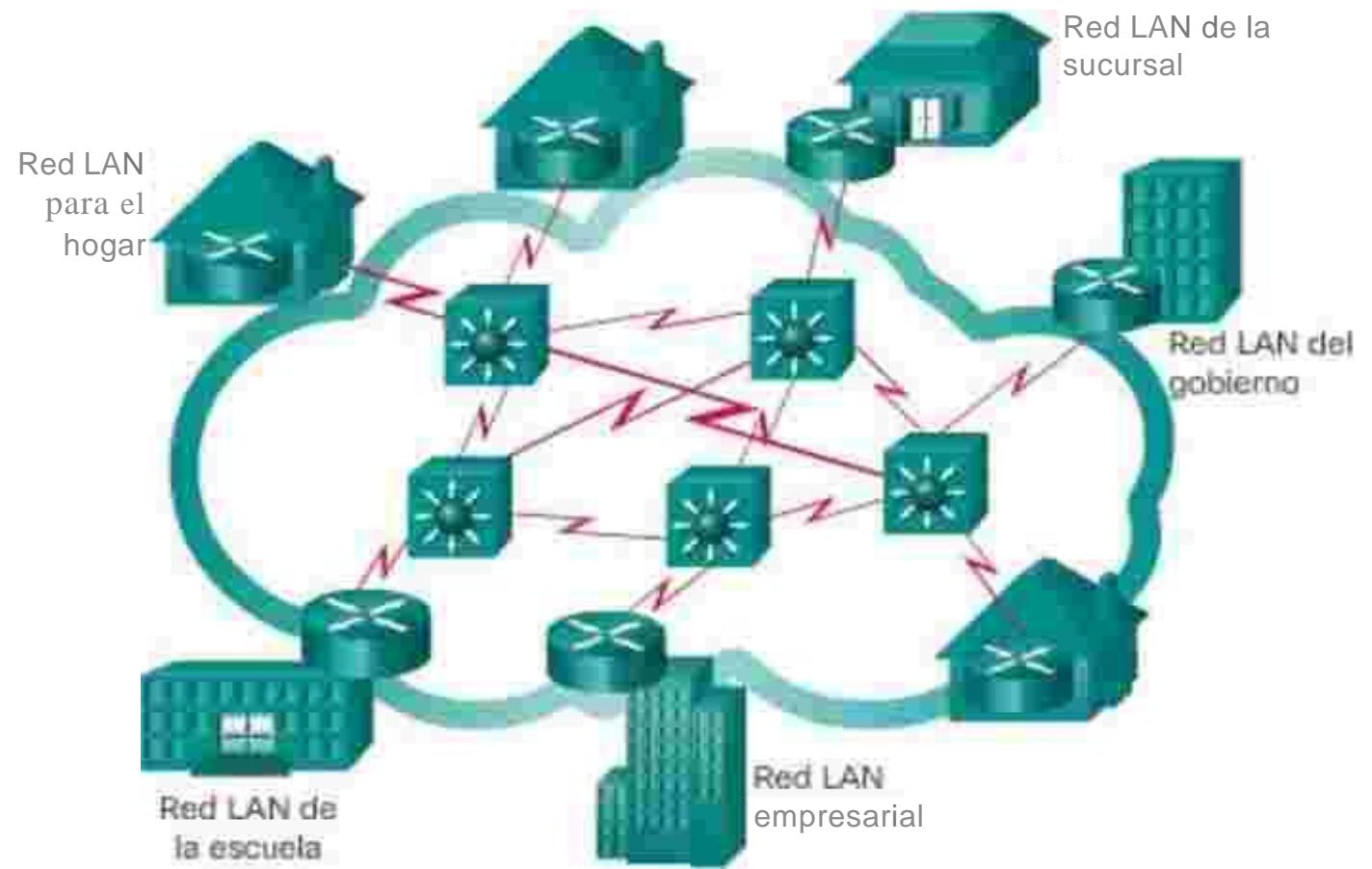
- 
- El tamaño del área que cubren
  - Cantidad de usuarios conectados
  - Cantidad y tipo de servicios disponible
  - El área de responsabilidad

# LOCAL AREA NETWORK LAN/WLAN



# WIDE AREA NETWORK **WAN**



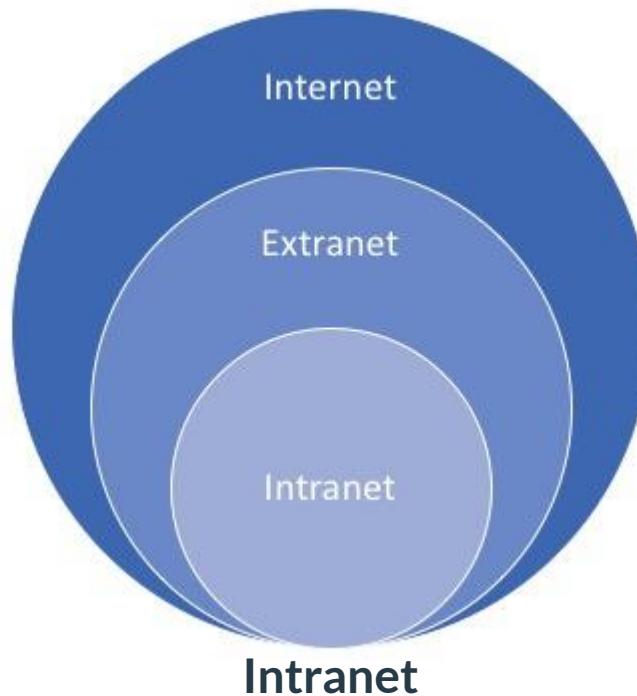


Internet es una red de  
redes interconectadas  
mundialmente

---

## 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.



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.

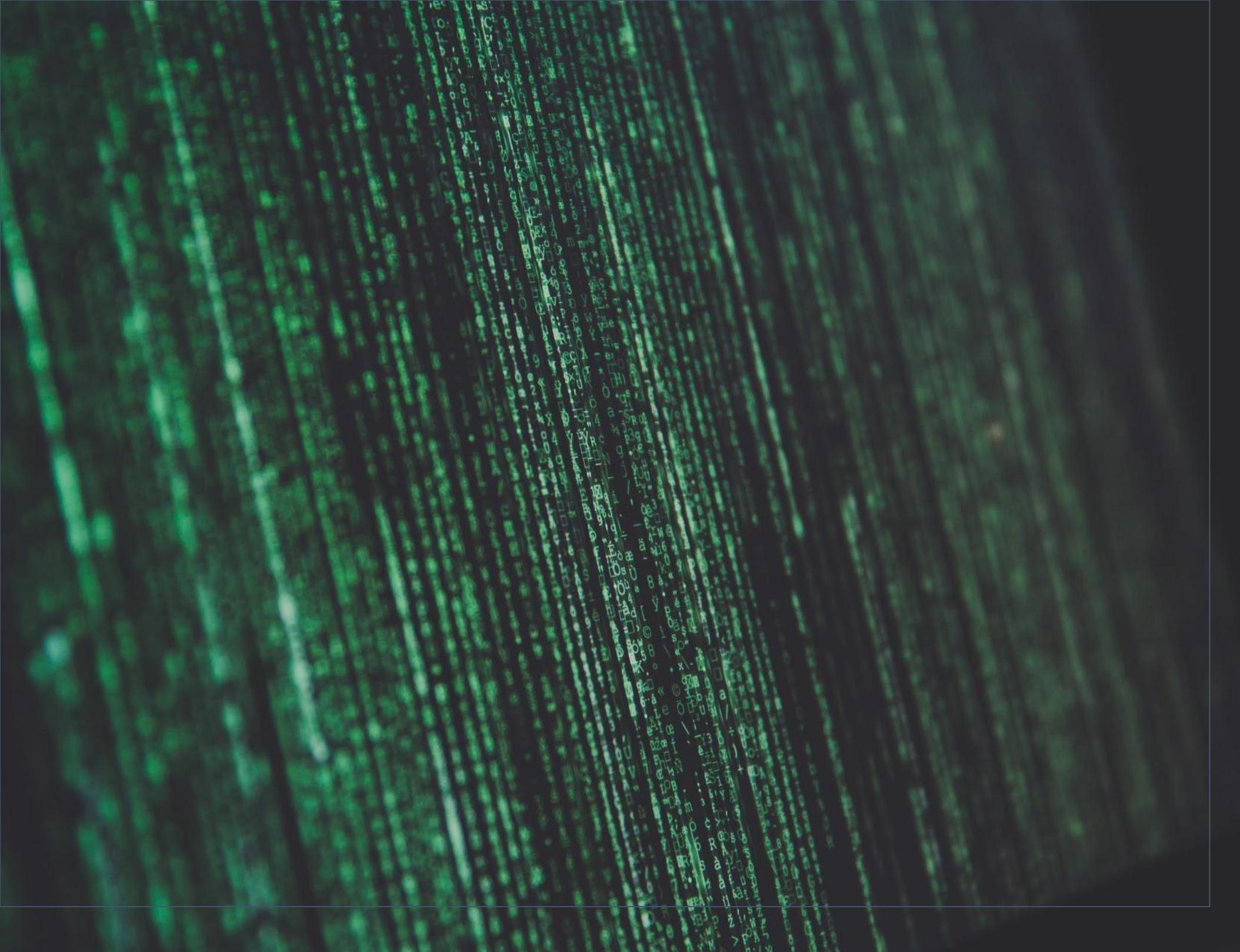
### Extranet

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.

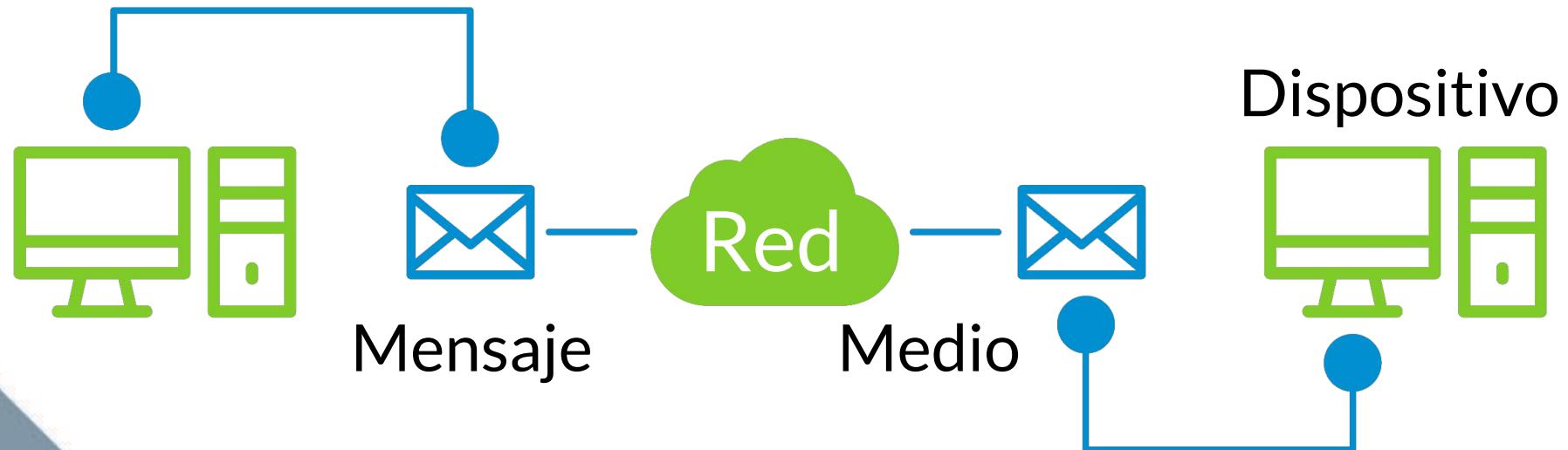
---

# Tecnologías de acceso a Internet



---

# Los elementos de la comunicación





# Velocidad

Generalmente estos ISP te venden el servicio en términos de MegaBITS por segundo.

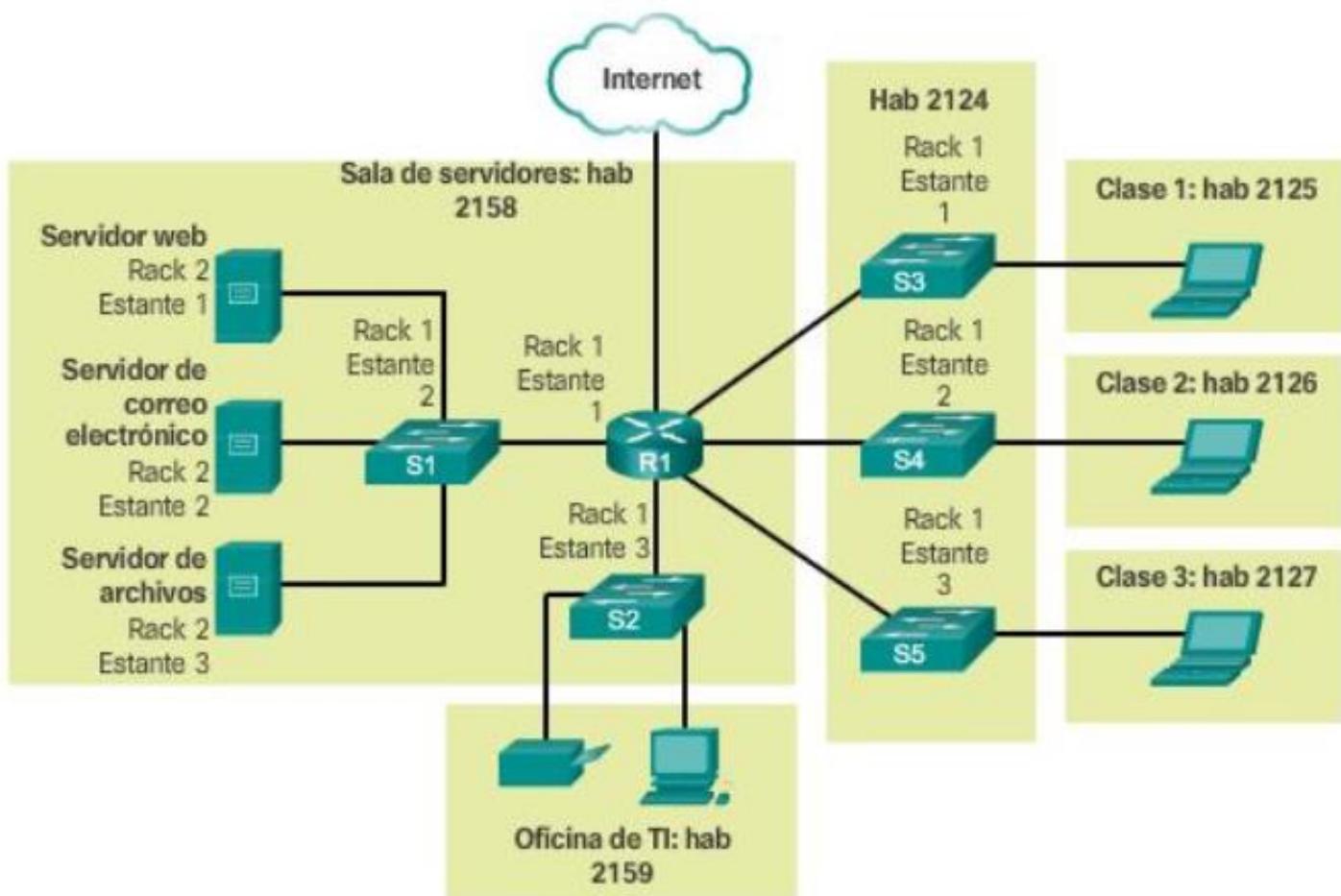
Tus archivos y todo el contenido que ves en internet se mide en términos de MegaBYTES.

- 0 y 1 son cada uno un bit.  
Un byte está conformado por 8 bits  
por ejemplo 01010101 es un byte.
- Las palabras clave aquí son bit y byte.

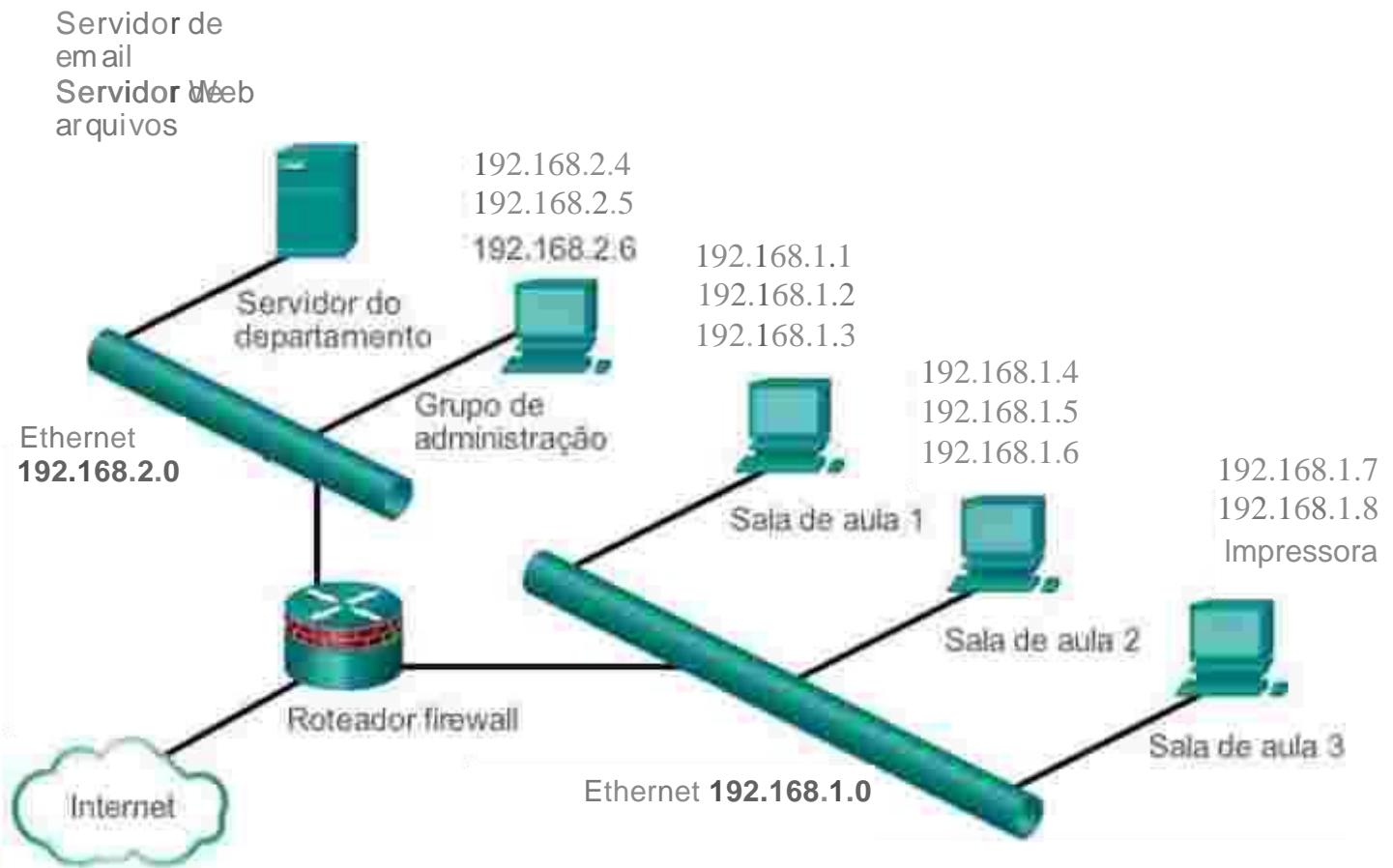
---

# Topologías de Red

# Diagrama de Topología Física



# Diagrama de Topología Lógica



# TOPOLOGÍA DE RED

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.



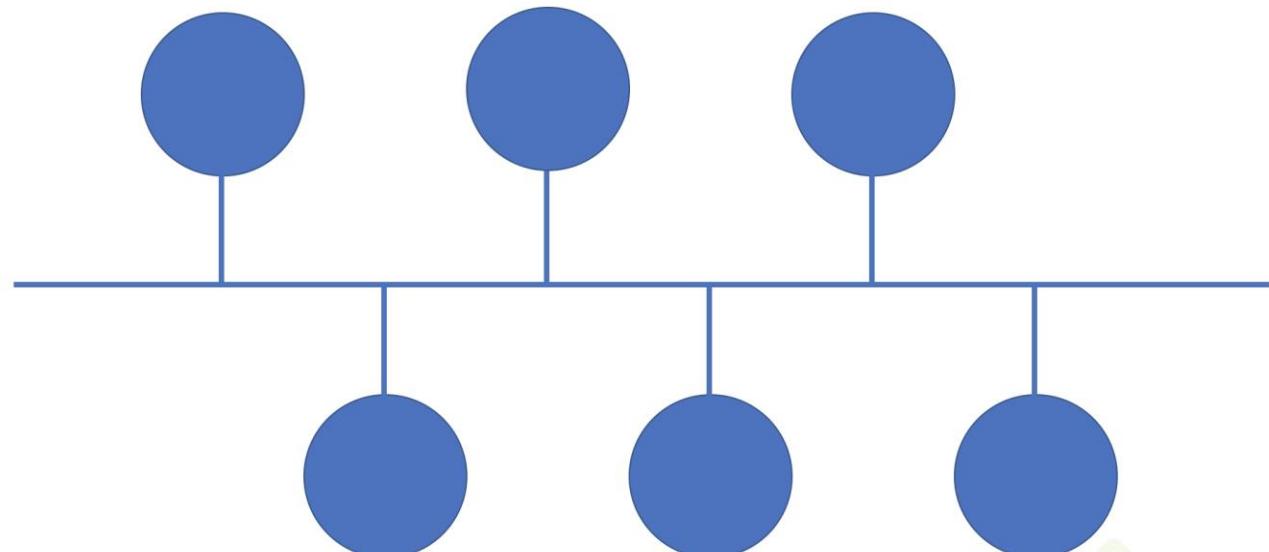
La topología mas rápida de implementar y de ver es cuando tenemos **dos nodos conectados por un medio para enviar información** esta es llamada Punto a Punto, un punto envía información al otro. Luego tenemos otras topologías, veamos algunas de sus características y ventajas.

# TOPOLOGÍA DE BUS

Este tipo de topología es el mas 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.

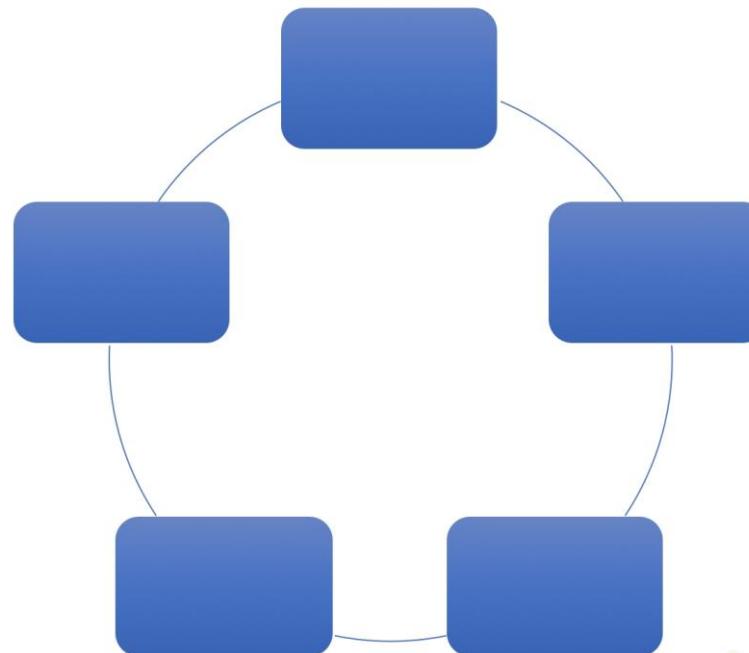
Esto, aunque es una gran ventaja y seguro le facilita la vida al administrador de la red, presenta dos inconvenientes, uno es que el tráfico de todos los nodos puede ser visto por los otros y el segundo es que a medida que la red crezca se va a ver afectado el rendimiento.



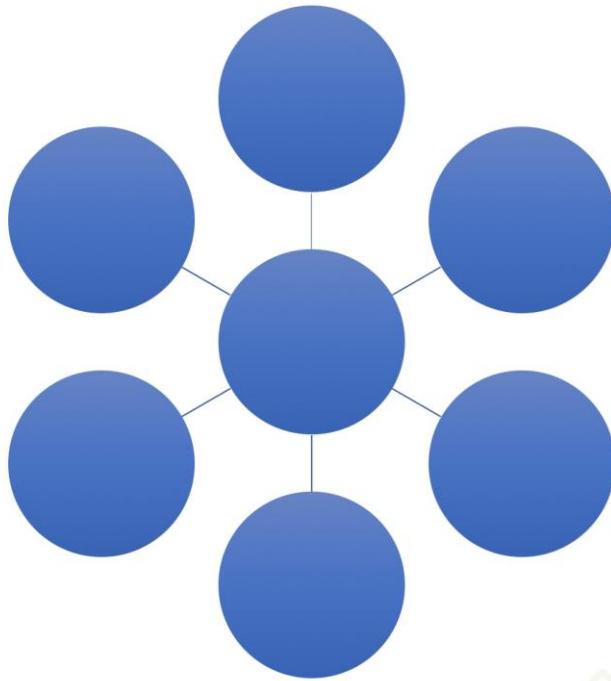
# TOPOLOGÍA DE ANILLO

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



Platzi

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.

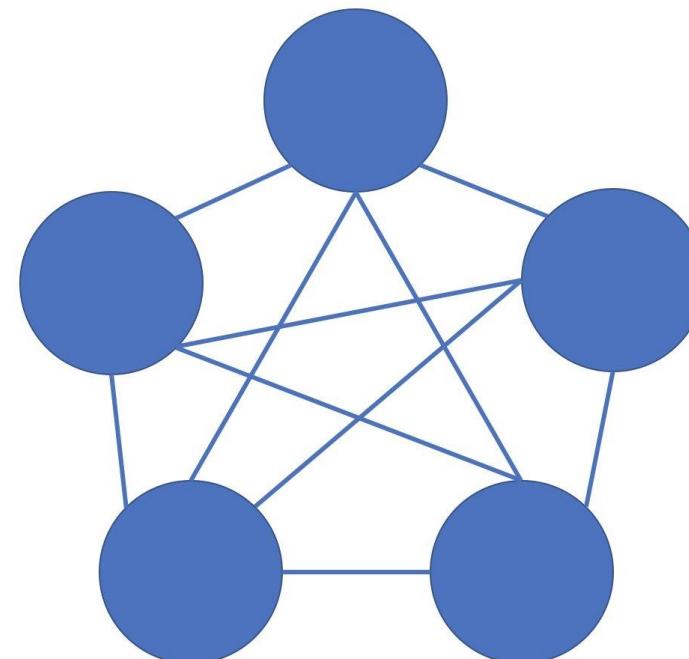
Esta topología se usa mucho en redes LAN, por ejemplo en oficinas en las que hay un switch al que llegan todas las conexiones de los dispositivos a través de cable.

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..

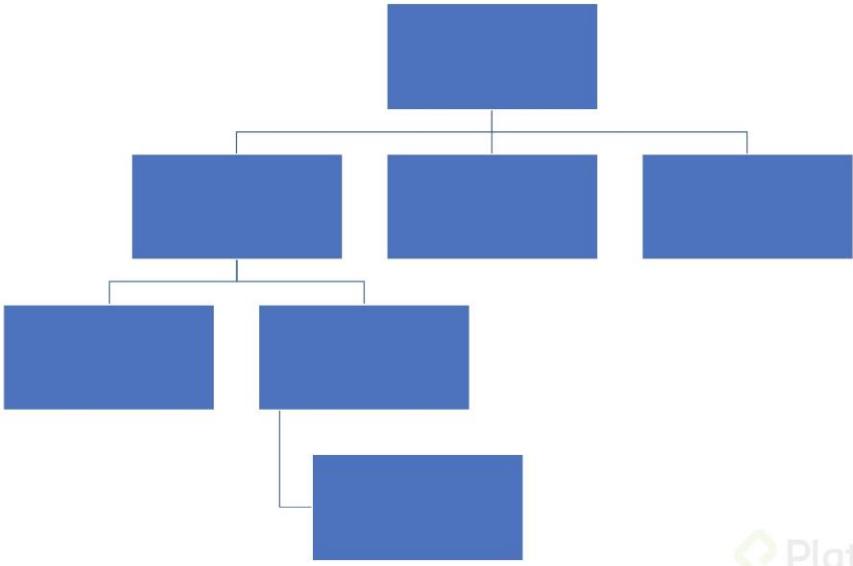
# TOPOLOGÍA DE MALLA

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



Platzi

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, 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.

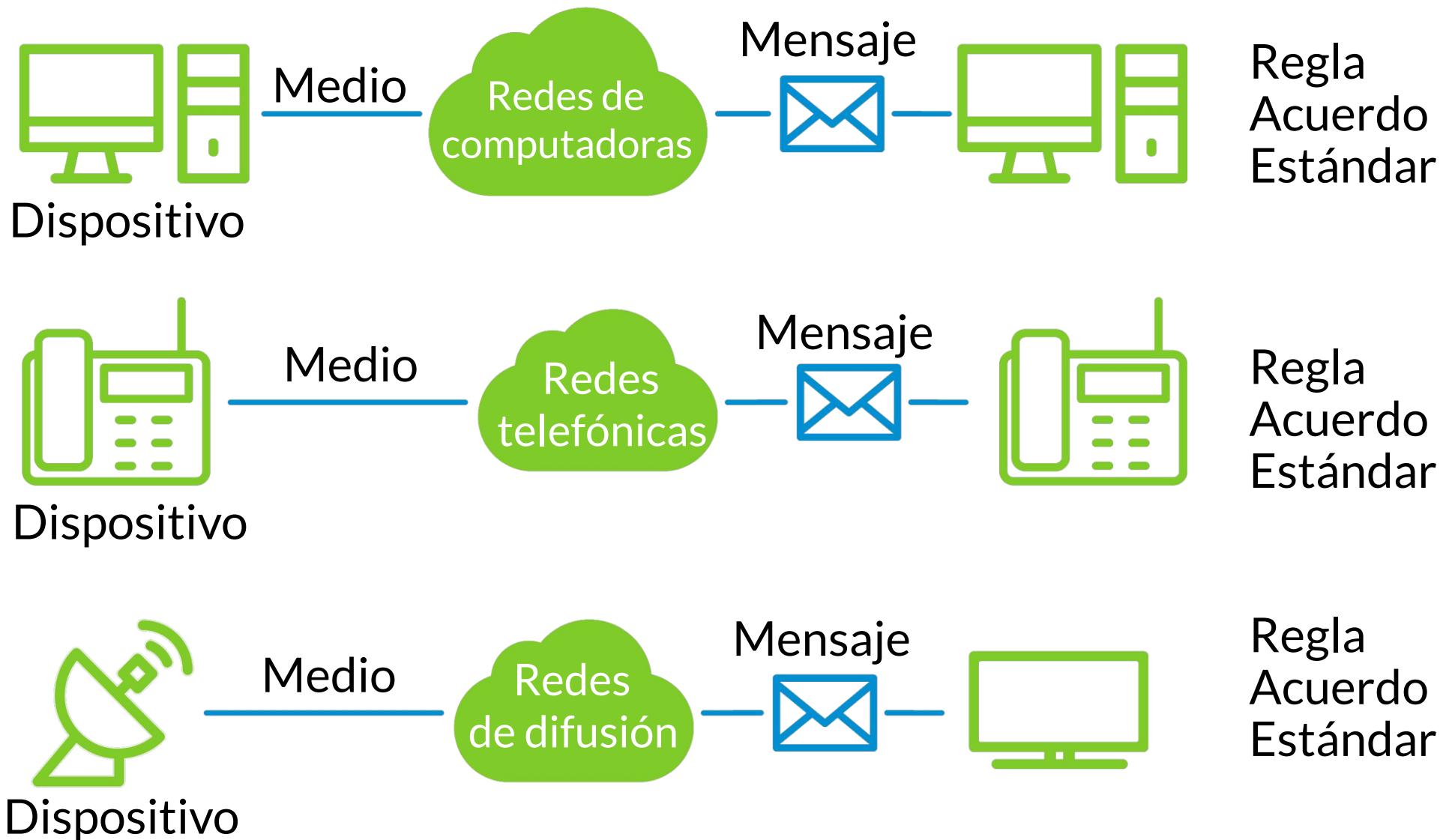
La forma de la red se parece mucho a un árbol.

También podemos hacer combinaciones de estas topologías para realizar nuestras propias implementaciones de acuerdo con las necesidades de los usuarios.

---

# Redes convergentes

# Redes tradicionales separadas



# Redes convergentes

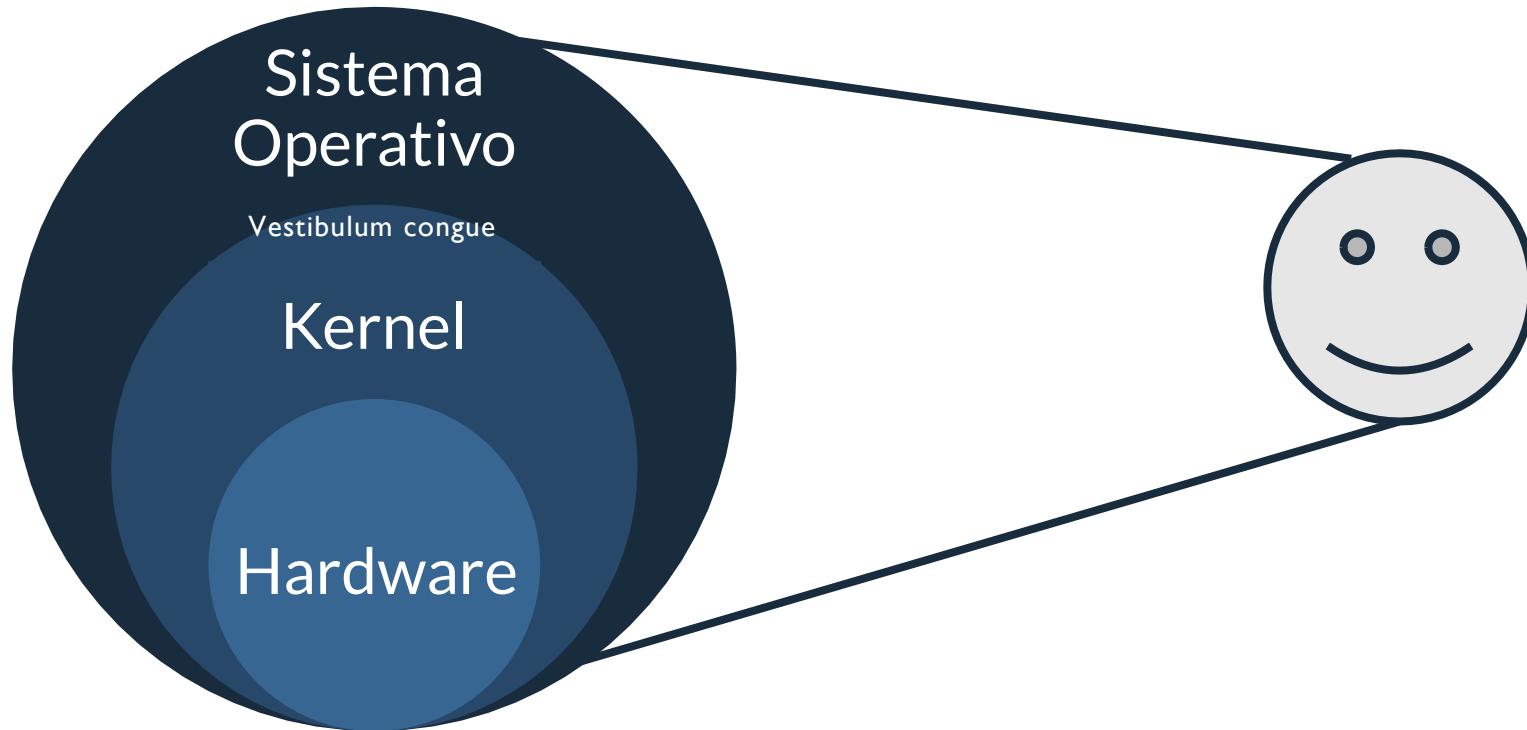


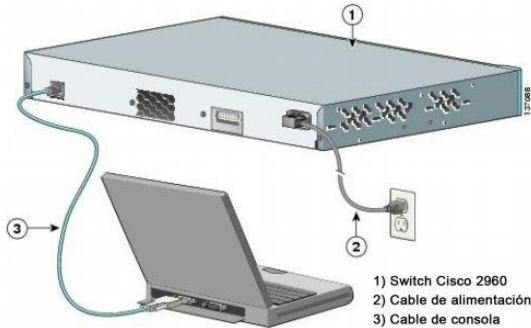
Configuración de dispositivos

---

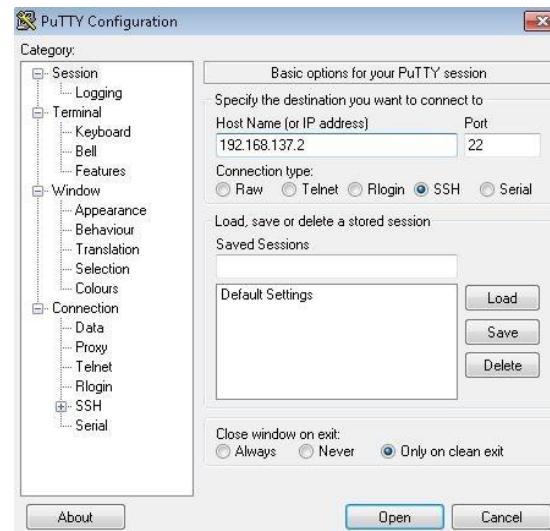
# Métodos de acceso a los dispositivos

# Sistema Operativo





## Acceso por consola



## Acceso por SSH

A screenshot of a Windows Command Prompt window titled 'cmd'. The command 'telnet' is being typed into the prompt. The text above the command shows the path 'C:\Windows\system32\cmd'.

```
C:\>pkgmgr /iu:"TelnetClient"
C:\>telnet
```

## Acceso por Telnet

## ¿Qué es 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.

## ¿Qué es SSH?

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.

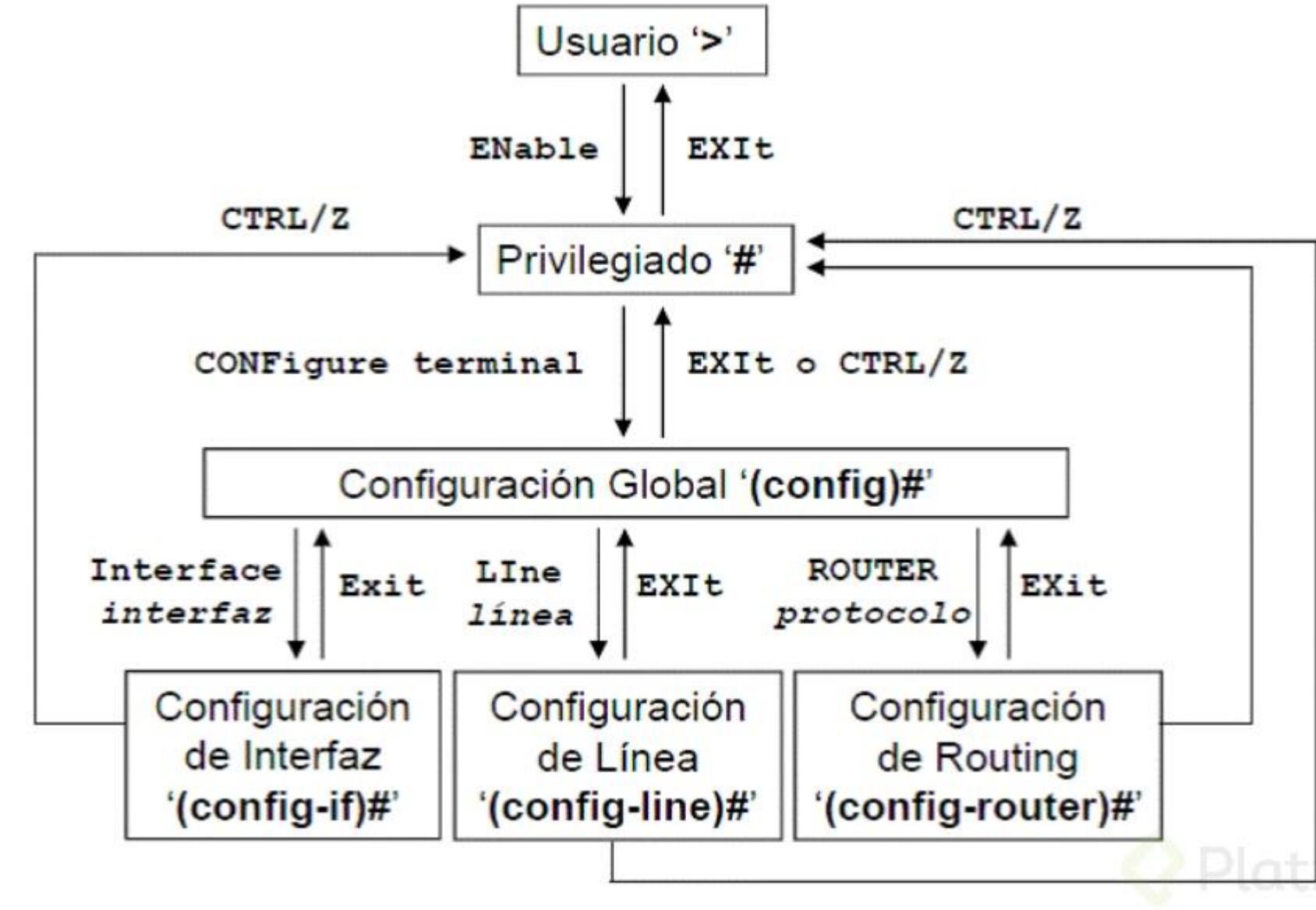
*Por defecto SSH usa el puerto 22 y Telnet utiliza el puerto 23, una medida básica de seguridad es configurarlos en otros puertos que no sean los establecidos por defecto.*

# **Práctica:**

## Navegación por el sistema operativo y configuración inicial de un dispositivo

Vamos a configurar un switch para que tenga un nombre, vamos a configurar algunos parámetros de seguridad y una dirección de administración.

Luego configuraremos los parámetros de red de PC y validamos la conexión al switch desde este dispositivo.



# Comandos para práctica

Comando	Función
show running-config	Muestra la configuración del dispositivo ( <i>modo privilegiado</i> )
enable	Modo privilegiado
configure terminal	Modo configuración global
hostname nombre	Configura el nombre del dispositivo ( <i>configuración global</i> )
enable secret contraseña	Configura la contraseña del modo privilegiado ( <i>configuración global</i> )
banner motd # hola bienvenido#	Configura mensaje de bienvenida ( <i>configuración global</i> )
interface vlan1	Modo de configuración de interfaces ( <i>configuración global</i> )
ip address 192.168.1.2 255.255.255.0	Configuramos la ip ( <i>config-if</i> )
no shutdown	Activa la interface ( <i>config-if</i> )
copy run startup-config	Guarda la configuración actual IMPORTANTE ( <i>modo privilegiado</i> )

# Configuracion del Swich Virtual



NIC = 192.168.1.10  
Mack = 255.255.255.0

vLan = 192.168.1.2  
Mack = 255.255.255.0

NIC = Network Interface Card

---

# Hardware de Red

Ahora es tiempo de dejar a un lado las aplicaciones y los aspectos sociales de las redes para enfocarnos en las cuestiones técnicas implicadas en su diseño. No existe una clasificación aceptada en la que encajen todas las redes, pero hay dos que sobresalen de manera importante: **la tecnología de transmisión y la escala**. Examinaremos ahora cada una de ellas por turno.

Hablando en sentido general, existen dos tipos de **tecnología de transmisión** que se emplean mucho en la actualidad: **los enlaces de difusión (broadcast) y los enlaces de punto a punto**.

**Los enlaces de punto a punto** conectan pares individuales de máquinas. Para ir del origen al destino en una red formada por enlaces de punto a punto, los mensajes cortos (conocidos como **paquetes** en ciertos contextos) tal vez tengan primero que visitar una o más máquinas intermedias. A menudo es posible usar varias rutas de distintas longitudes, por lo que es importante encontrar las más adecuadas en las **redes de punto a punto**. A la transmisión punto a punto en donde sólo hay un emisor y un receptor se le conoce como **unidifusión (unicasting)**.

## RED DE DIFUSIÓN.-

Los paquetes que envía una máquina son recibidos por todas las demás. Un campo de dirección dentro de cada paquete específica a quién se dirige. Cuando una máquina recibe un paquete, verifica el campo de dirección. Si el paquete está destinado a la máquina receptora, ésta procesa el paquete; si el paquete está destinado para otra máquina, sólo lo ignora. Una red inalámbrica es un ejemplo común de un enlace de difusión, en donde la comunicación se comparte través de una región de cobertura que depende del canal inalámbrico y de la máquina que va a transmitir.

Como analogía considere alguien parado en una sala de juntas gritando:

“Watson, ven aquí. Te necesito”.

Por lo general, los sistemas de difusión también brindan la posibilidad de enviar un paquete a todos los destinos mediante el uso de un código especial en el campo de dirección. Cuando se transmite un paquete con este código, todas las máquinas en la red lo reciben y procesan. A este modo de operación se le conoce como difusión (**broadcasting**).

Algunos sistemas de difusión también soportan la transmisión a un subconjunto de máquinas, lo cual se conoce como **multidifusión (multicasting)**. Hay un criterio alternativo para **clasificar las redes: por su escala**. La distancia es importante como medida de clasificación, ya que las distintas tecnologías se utilizan a diferentes escalas.

Distancia entre procesadores	Procesadores ubicados en el (la) mismo(a)	Ejemplo
1 m	Metro cuadrado	Red de área personal
10 m	Cuarto	
100 m	Edificio	Red de área local
1 km	Campus	
10 km	Ciudad	Red de área metropolitana
100 km	País	
1000 km	Continente	Red de área amplia
10000 km	Planeta	Internet

## Clasificar las redes: Por su escala.

En la parte de arriba están las redes de área personal, las cuales están destinadas a una persona. Después se encuentran redes más grandes. Éstas se pueden dividir en redes de área local, de área metropolitana y de área amplia, cada una con una escala mayor que la anterior. Por último, a la conexión de dos o más redes se le conoce como **interred (internetwork)**. La Internet de nivel mundial es sin duda el mejor ejemplo (aunque no el único) de una interred. Pronto tendremos interredes aún más grandes con la Internet interplanetaria que conecta redes a través del espacio (Burleigh y colaboradores, 2003).

---

# Modelos de Referencia

## MODELOS DE REFERENCIA : OSI Y TCP/IP

Analizaremos dos arquitecturas de redes importantes: el modelo de referencia OSI y el modelo de referencia TCP/IP.

Aunque ya casi no se utilizan los protocolos asociados con el modelo OSI, el modelo en sí es bastante general y sigue siendo válido; asimismo, las características en cada nivel siguen siendo muy importantes. El modelo TCP/IP tiene las propiedades opuestas: el modelo en sí no se utiliza mucho, pero los protocolos son usados ampliamente.

## MODELOS DE REFERENCIA : OSI

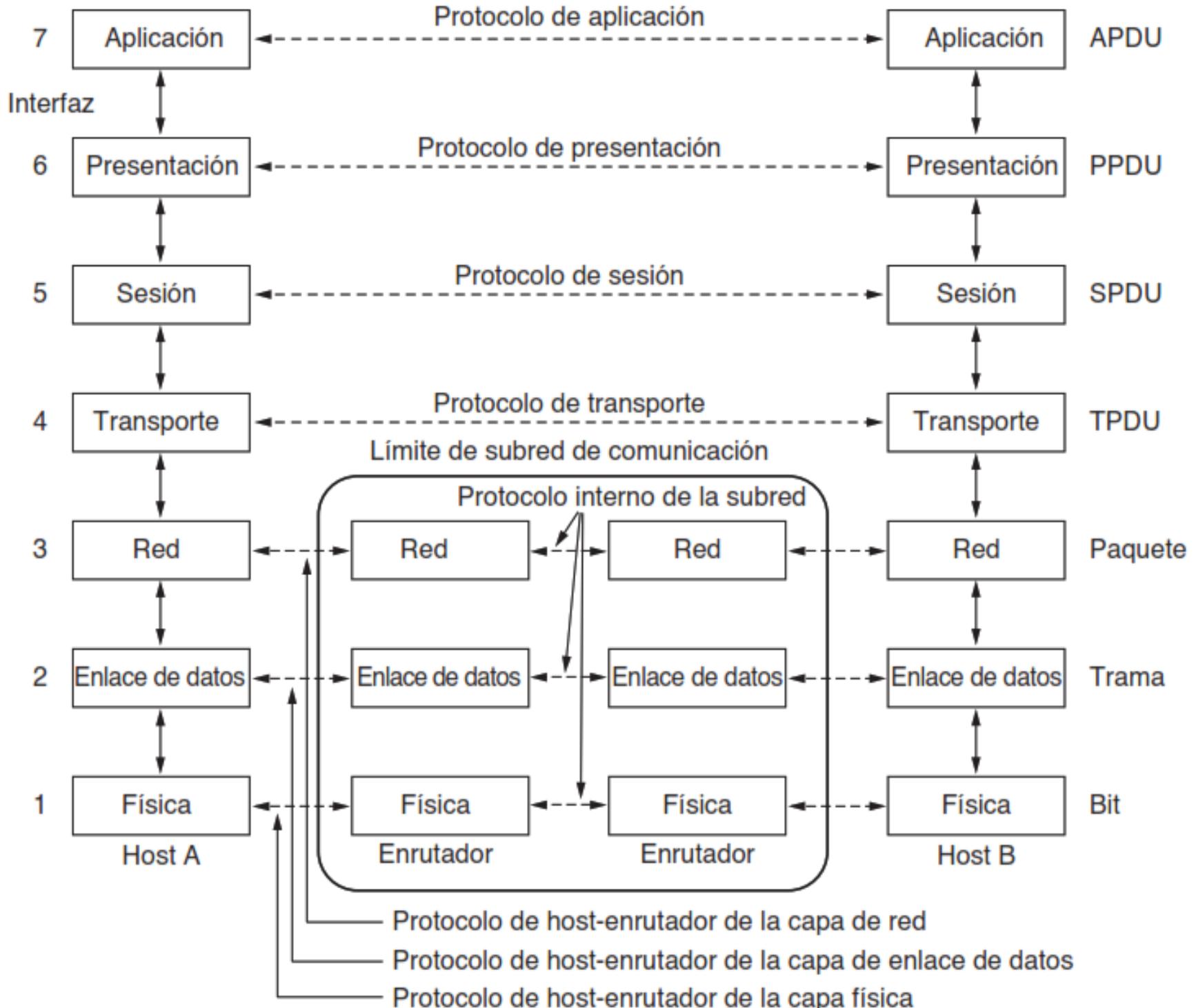
Modelo de referencia OSI (**Interconexión de Sistemas Abiertos**, del inglés **Open Systems Interconnection**) de la iso puesto que se ocupa de la conexión de sistemas abiertos;

Esto es, sistemas que están abiertos a la comunicación con otros sistemas. Para abbreviar, lo llamaremos modelo OSI. El modelo OSI tiene **siete capas**. Los principios que se aplicaron para llegar a las siete capas se pueden resumir de la siguiente manera:

1. Se debe crear una capa en donde se requiera un nivel diferente de abstracción.
2. Cada capa debe realizar una función bien definida.
3. La función de cada capa se debe elegir teniendo en cuenta la definición de protocolos estandarizados internacionalmente.

Capa

Nombre de la unidad  
intercambiada



## **La capa física**

La capa física se relaciona con la transmisión de bits puros a través de un canal de transmisión. Los aspectos de diseño tienen que ver con la acción de asegurarse que cuando uno de los lados envíe un bit 1 el otro lado lo reciba como un bit 1, no como un bit 0.

La principal tarea de la capa de enlace de datos es transformar un medio de transmisión puro en una línea que esté libre de errores de transmisión. Enmascara los errores reales, de manera que la capa de red no los vea. Para lograr esta tarea, el emisor divide los datos de entrada en tramas de datos (por lo general, de algunos cientos o miles de bytes) y transmite las tramas en forma secuencial. Si el servicio es confiable, para confirmar la recepción correcta de cada trama, el receptor devuelve una trama de confirmación de recepción

## **La capa de enlace de datos**

## **Control de acceso al medio**

Las redes de difusión tienen una consideración adicional en la capa de enlace de datos: cómo controlar el acceso al canal compartido. Una subcapa especial de la capa de enlace de datos, conocida como subcapa de control de acceso al medio, es la que se encarga de este problema.

---

# **Suite 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:

## Suites de protocolos

## **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.

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

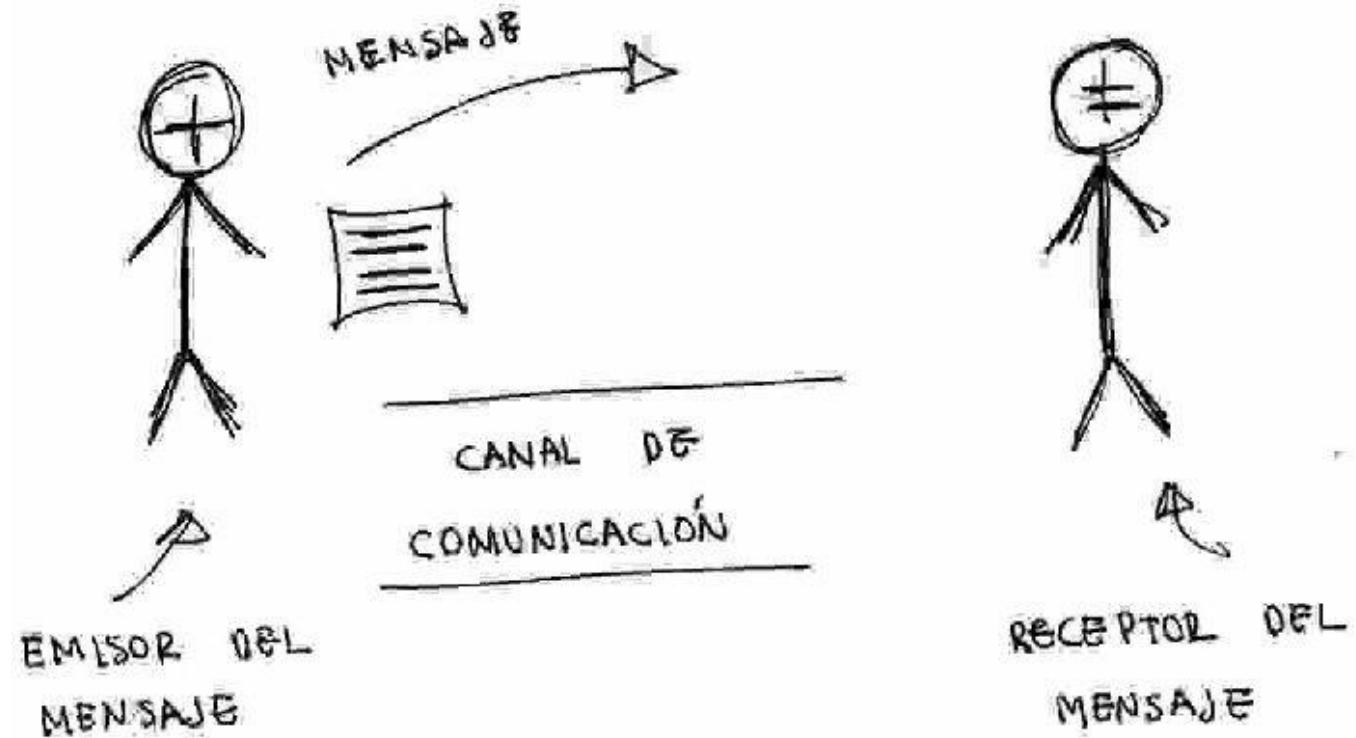
Este protocolo apoya al protocolo IP proporcionando mensajes y notificaciones de error cuando un mensaje no puede alcanzar su destino. Válida que el mensaje haya alcanzado su destino, válida también si el tiempo de vida del mensaje ya ha sido superado entre otras cosas. Su labor es únicamente informar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

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

---

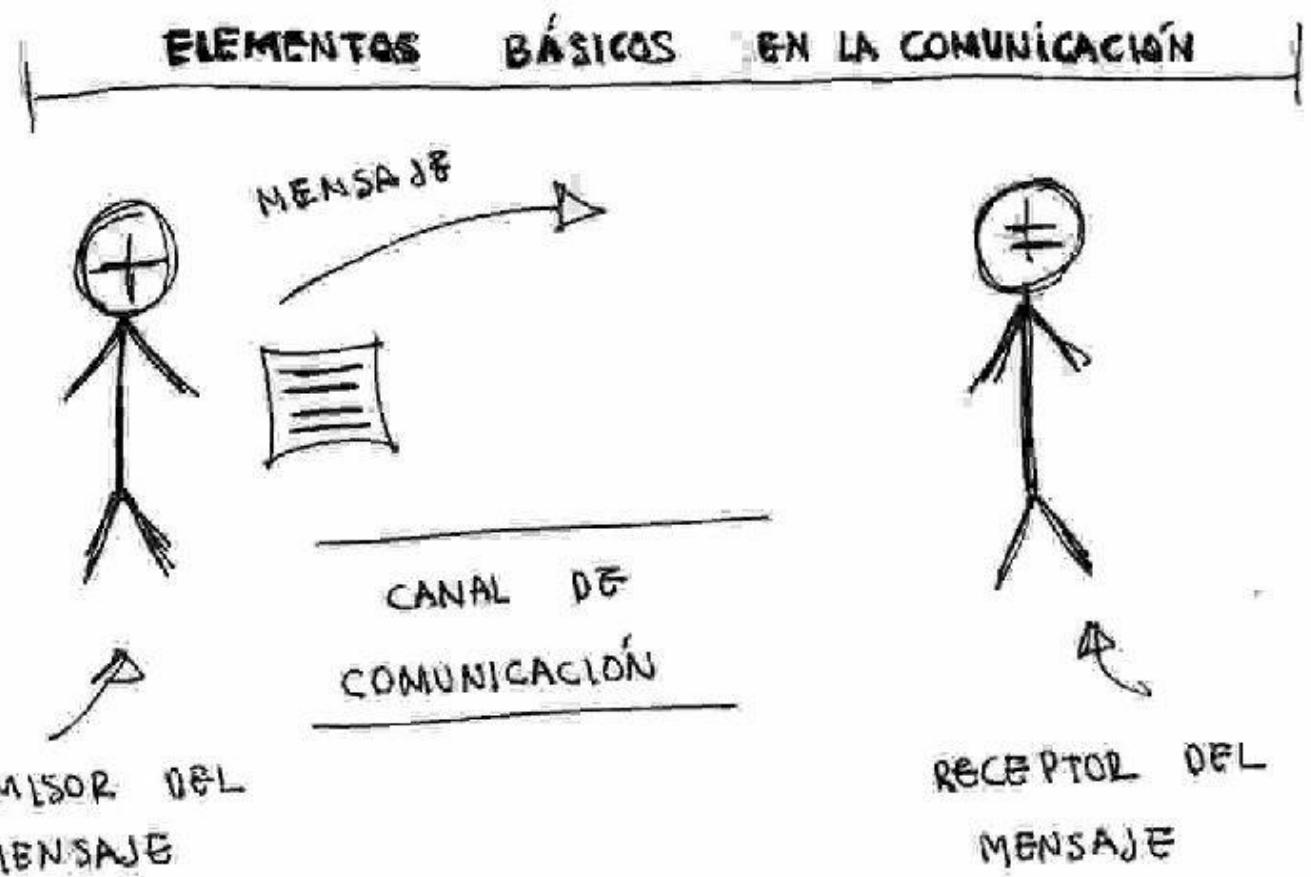
# Protocolos y comunicaciones de Red

## ELEMENTOS BÁSICOS EN LA COMUNICACIÓN



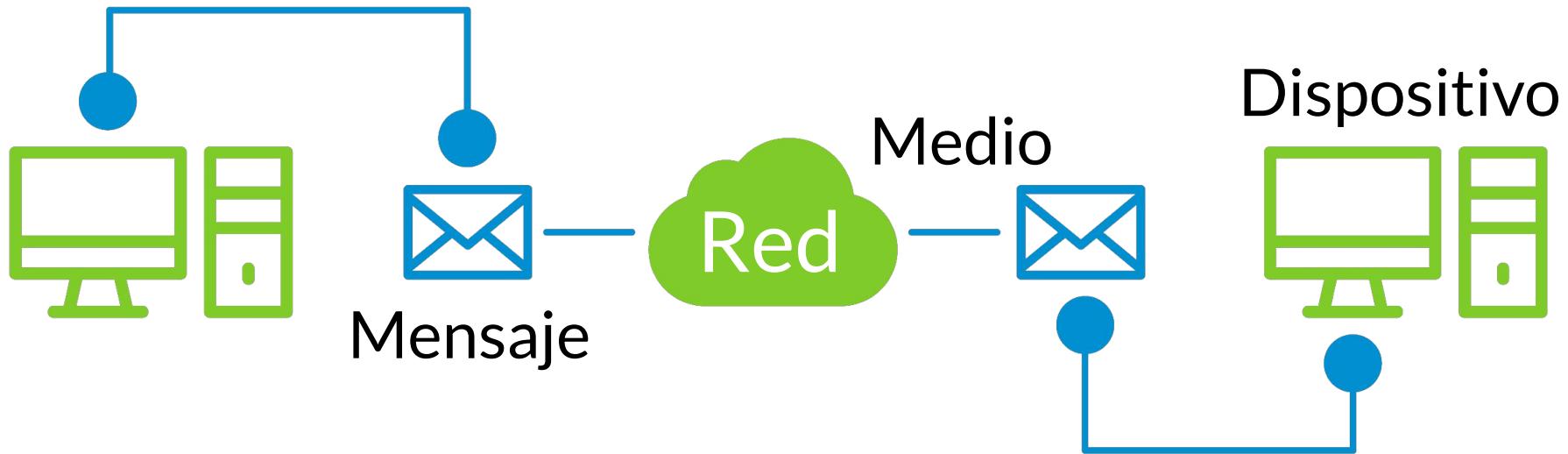
# Elemento indispensable: Reglas de comunicación

# Los protocolos son las reglas que rigen la comunicación



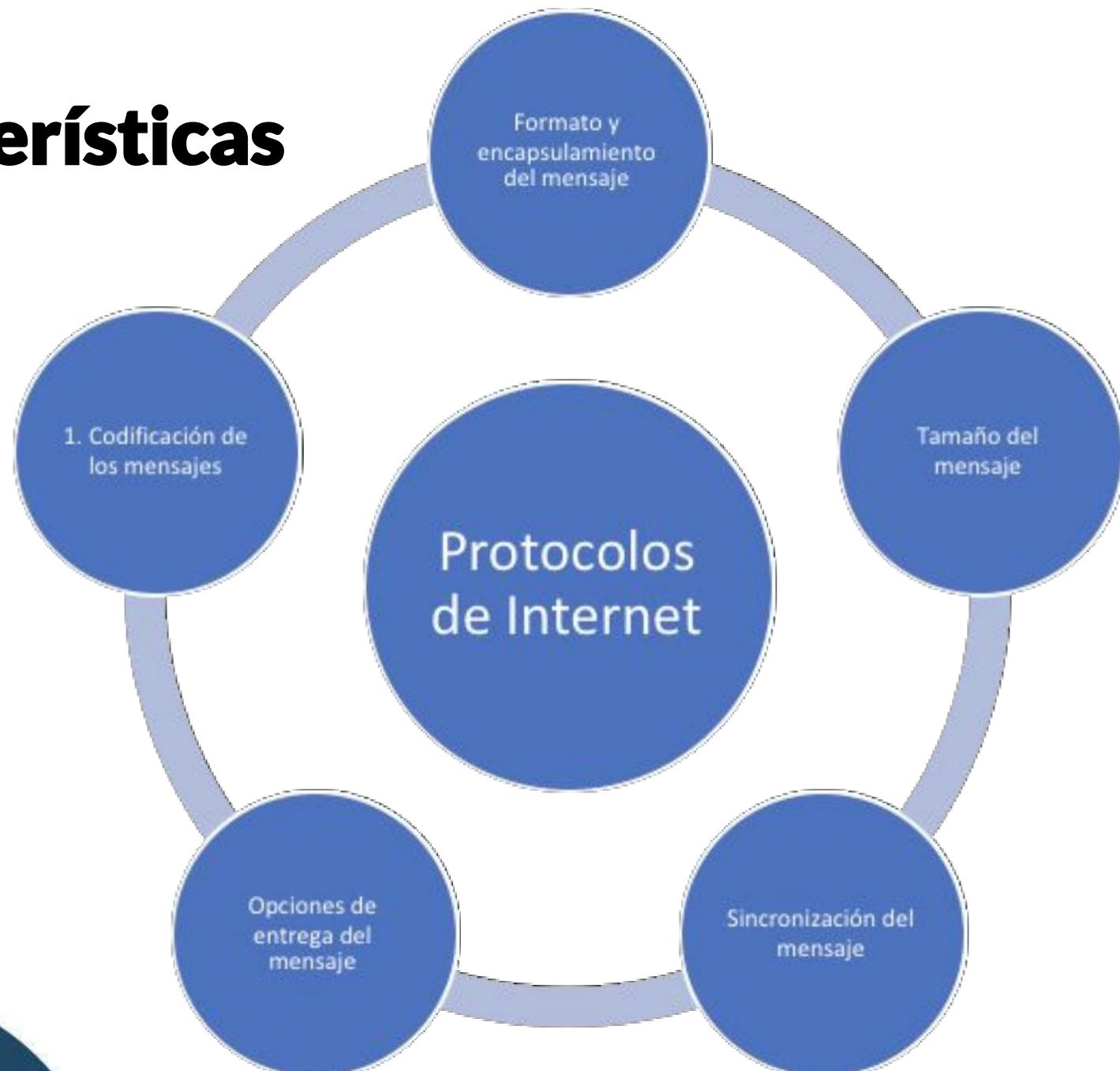
- ¿Qué tipo de comunicación usamos?
  - ¿Señas? ¿Voz? ¿Escrito?
- ¿Cuál va a ser el lenguaje?
  - Idioma

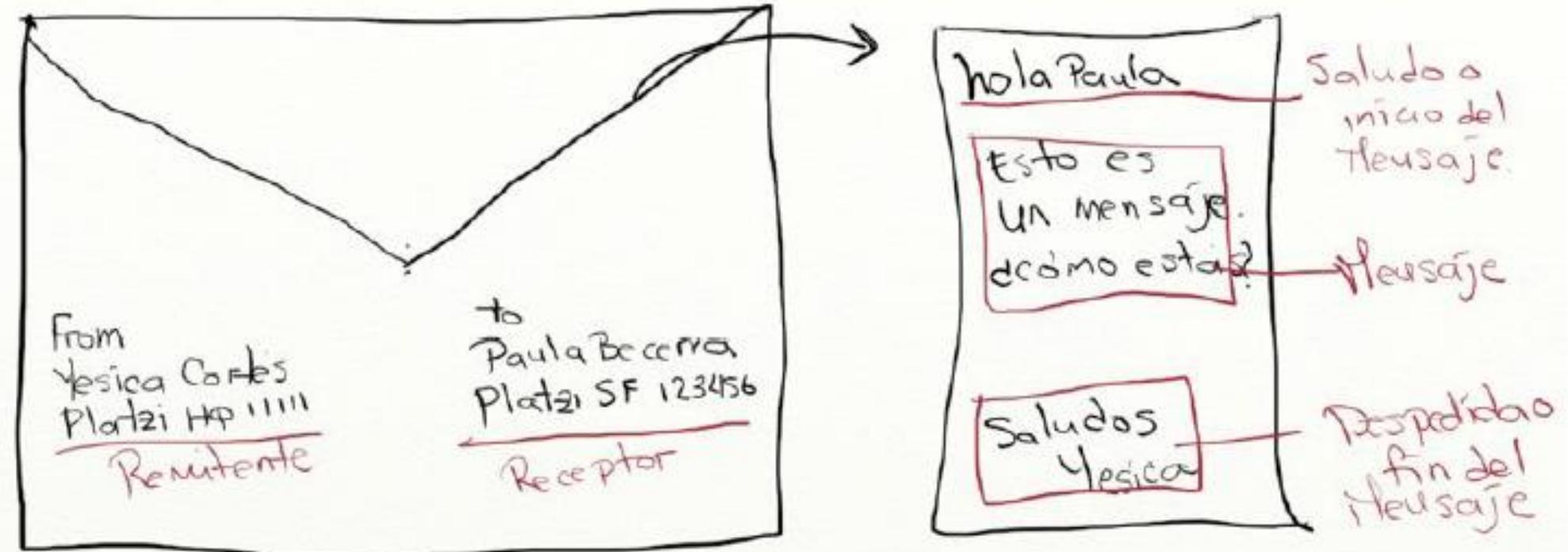
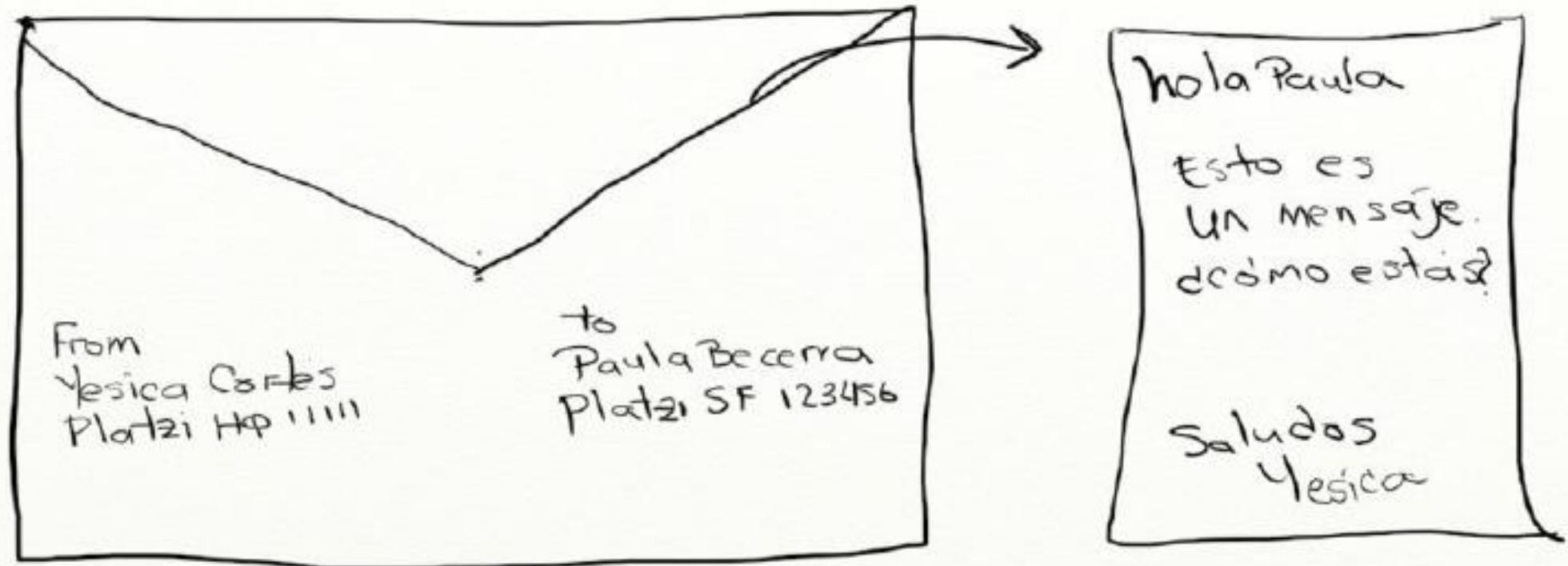
# **Los protocolos son las reglas que rigen la comunicación**



**Reglas:**  
Regla  
Acuerdo  
Estándar

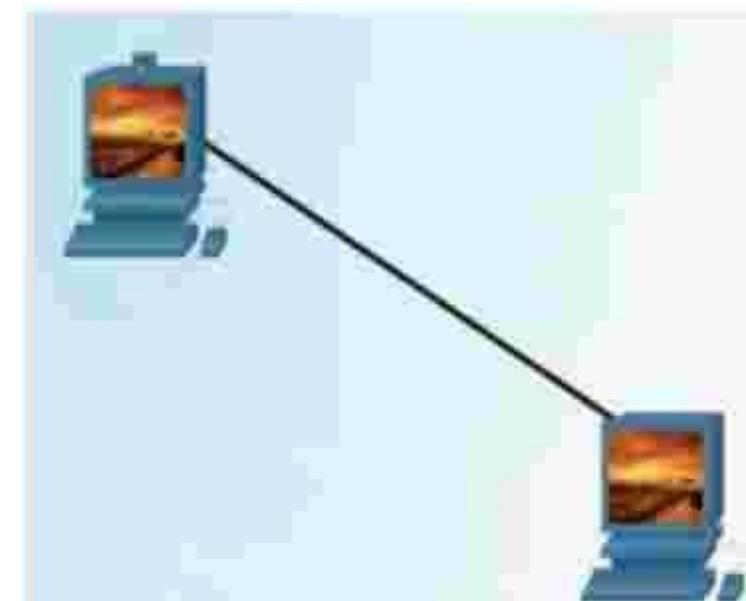
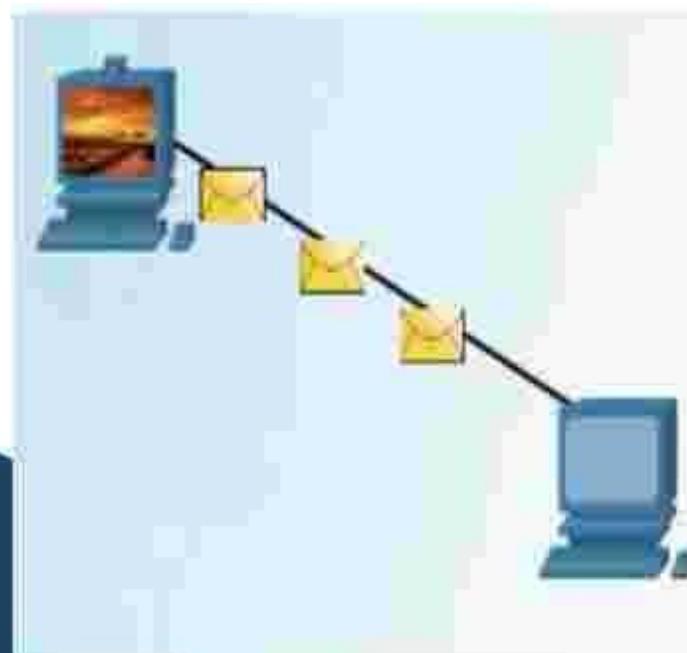
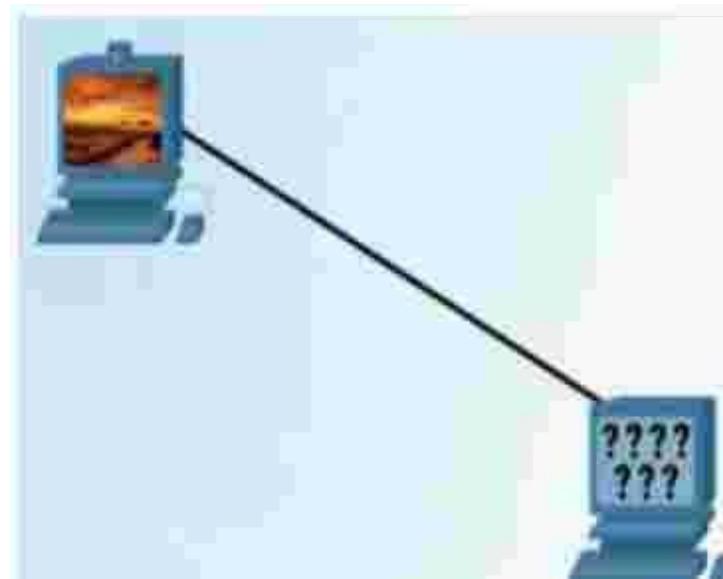
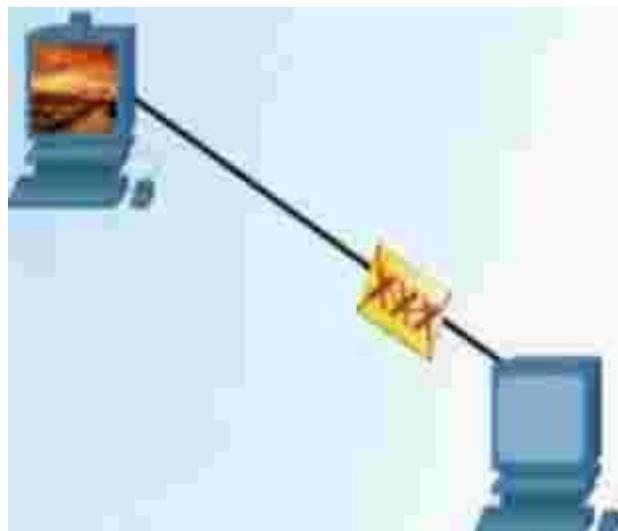
# Características





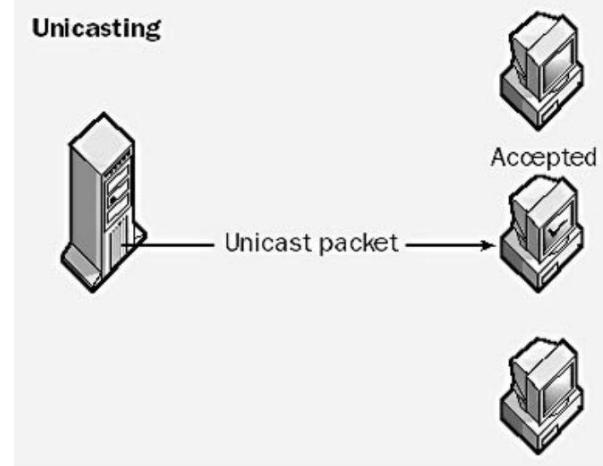
Destination (physical / hardware address)	Source (physical / hardware address)	Start Flag (start of message indicator)	Recipient (destination identifier)	Sender (source identifier)	Encapsulated Data (bits)	End of Frame (end of message indicator)
Frame Addressing		Encapsulated Message				

- 
- Codificación del mensaje
  - Formato y encapsulamiento del mensaje
  - Tamaño del mensaje

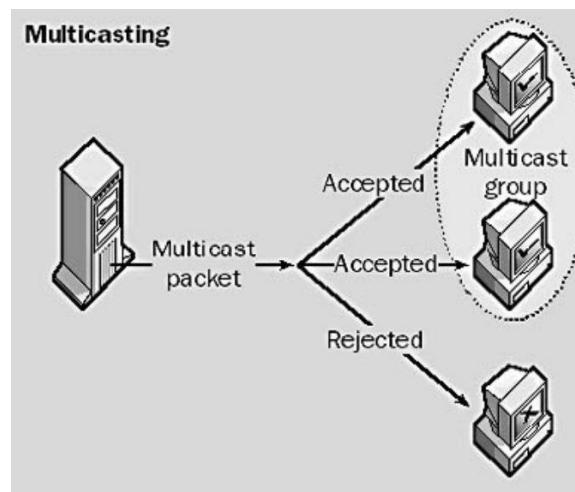


- 
- Codificación del mensaje
  - Formato y encapsulamiento del mensaje
  - Tamaño del mensaje
  - Sincronización
  - Opciones de entrega

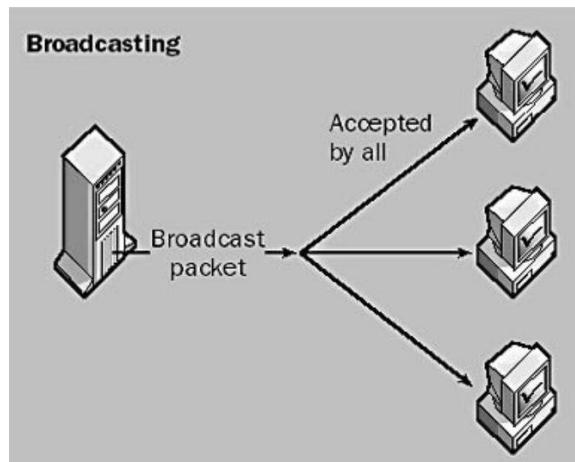
## Unicast / Unidifusión



## Multicast / Multidifusión



## Broadcasting / difusión



Nos ayudan a entender a hacer la codificación del mensaje  
El formato y la estructura del mensaje, la información que queremos transmitir debe tener una forma para que pueda ser enviada por el medio que queremos enviarlo.

**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 cuando se esta enviando un mensaje, que ya llego un mensaje, que se puede llegar otro.

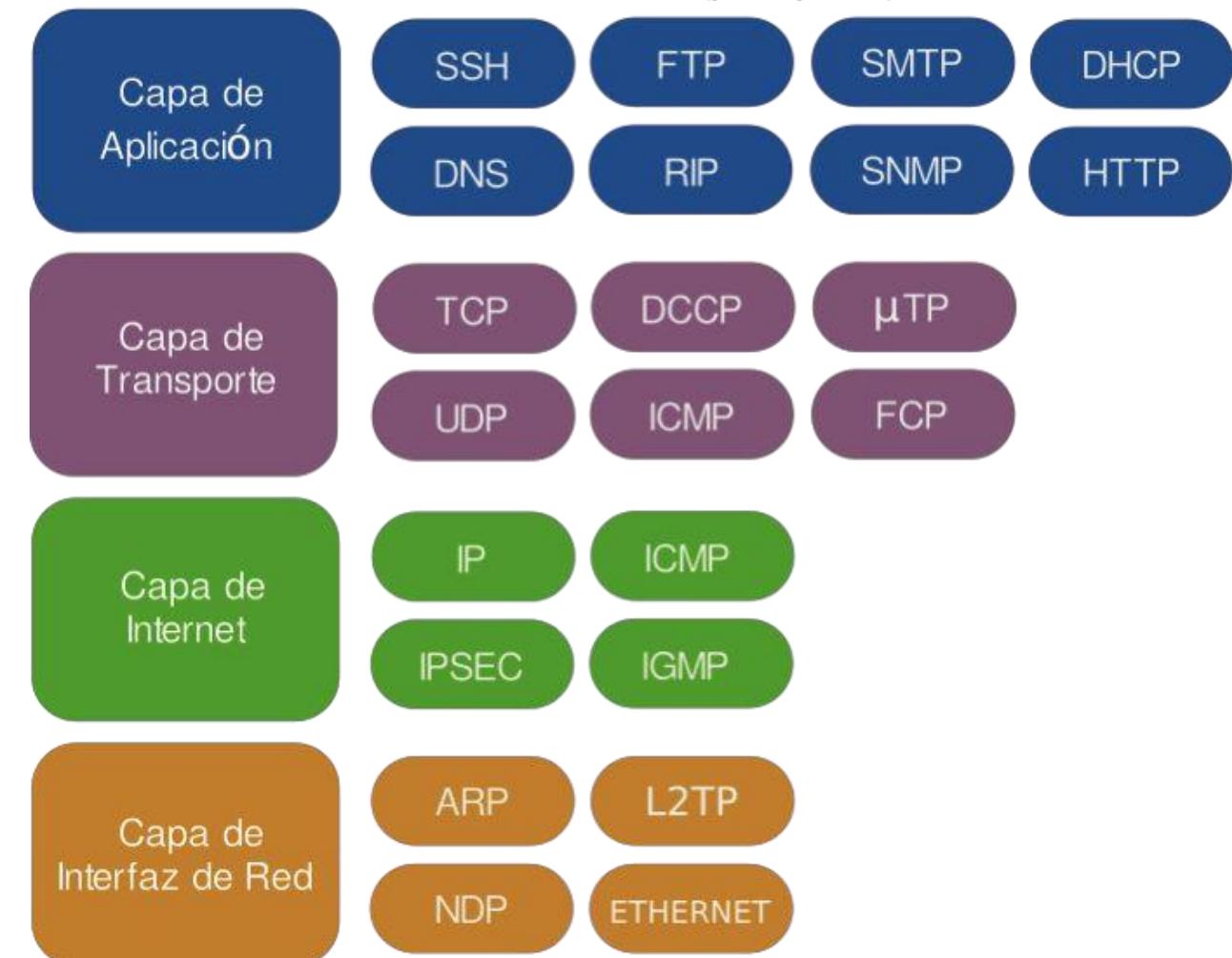
**Opción de entrega:** Unicast se le envía a un solo host, Multicast permite enviar a un grupo más pequeño, no a todos los host, Broadcasting nos envía paquetes a toda la red.

---

# Modelos de referencia

# TCP/IP

Modelo  
TCP/IP



Suite de Protocolos  
(principales)

# OSI

Grupo	#	Nombre	Tecnología y protocolos	Componentes comunes
Capas superiores	7	Aplicación	DNS – DHCP – SNMP – FTP – POP3 – HTTP – TELNET	Aplicaciones compatibles con la red, correo electrónico, navegadores, servidores WEB
	6	Presentación	SSL – Shells – MIME	
	5	Sesión	NetBIOS Llamadas de procedimiento remoto	
Capas inferiores	4	Transporte	TCP & UDP	VoIP & Video – Firewall
	3	Red	IPv4 – IPv6 IPNAT – ARP RARP - ICMP	Direccionamiento IP – Ruteo
	2	Enlace de datos	Frame Ethernet – WLAN - ATM	Interfaces de red y controladores – WAN
	1	Física	Señales eléctricas – Ondas luminosas – Radio	Medios físicos, hubs y repetidores

- **Física** - medios por los que se transportan las señales que llevan los mensajes.
- **Enlace a datos** - los equipos en los que se hace el direccionamiento físico.
- **Red** - direccionamiento lógico.
- **Transporte** - conexión extremo a extremo y garantiza la fiabilidad de los datos. Son los protocolos que nos aseguran que el mensaje se envía y es recibido. Nos da la conexión de extremo a extremo. Tiene los protocolos TCP y UDP. Nos aseguran que el mensaje fue enviado y recibido.
- **Sesión** - mantiene abierta la comunicación entre los dispositivos de red.
- **Presentación** - representación de los datos, tipos de archivo etc.
- **Aplicaciones** que acceden a información desde Internet.

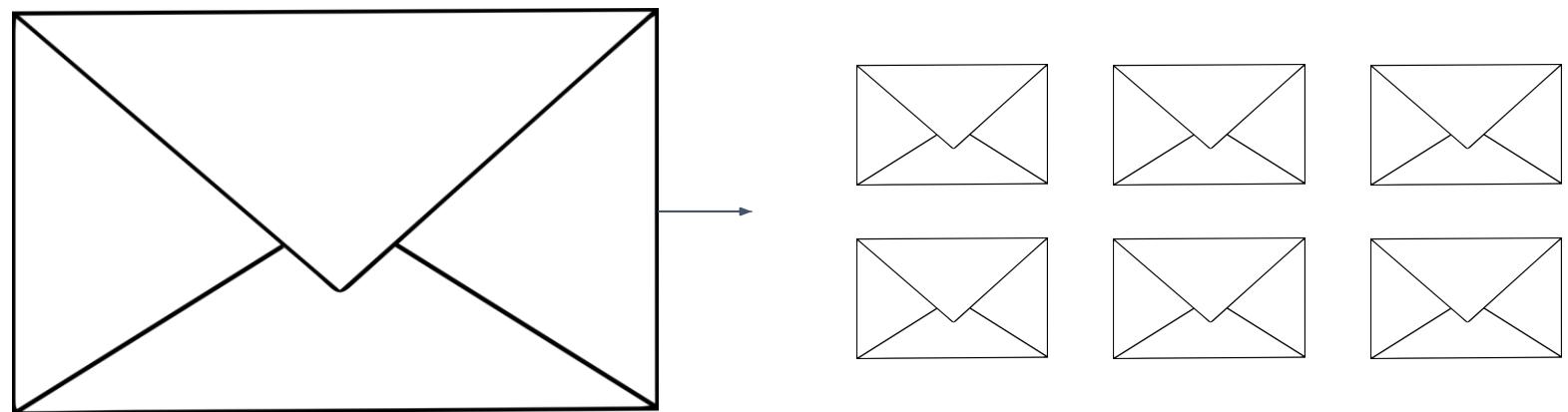
---

# Protocol Data Unit

Segmentación / multiplexión de mensajes

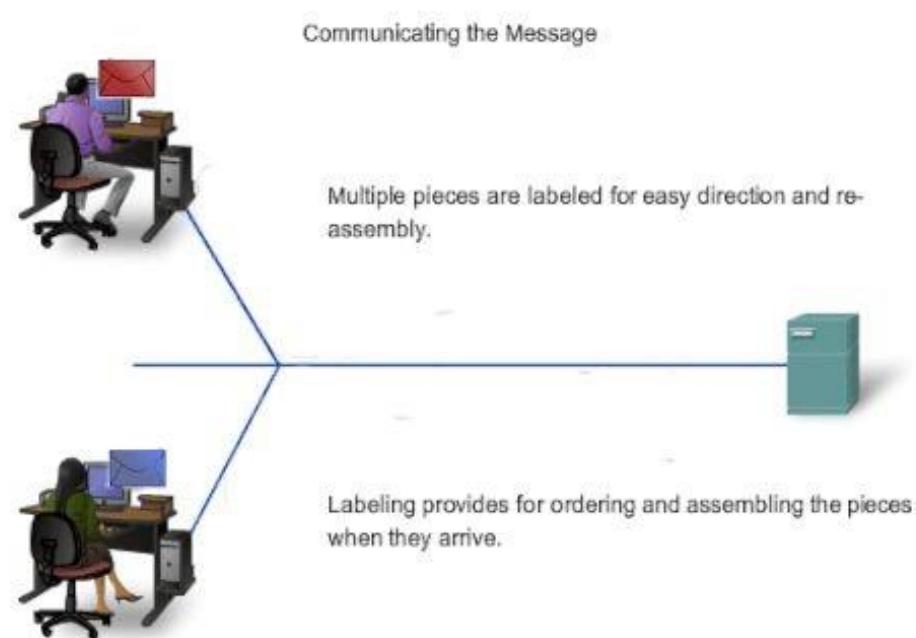
# Segmentación

Tomar un mensaje y dividirlo en pequeñas partes



# Multiplexación

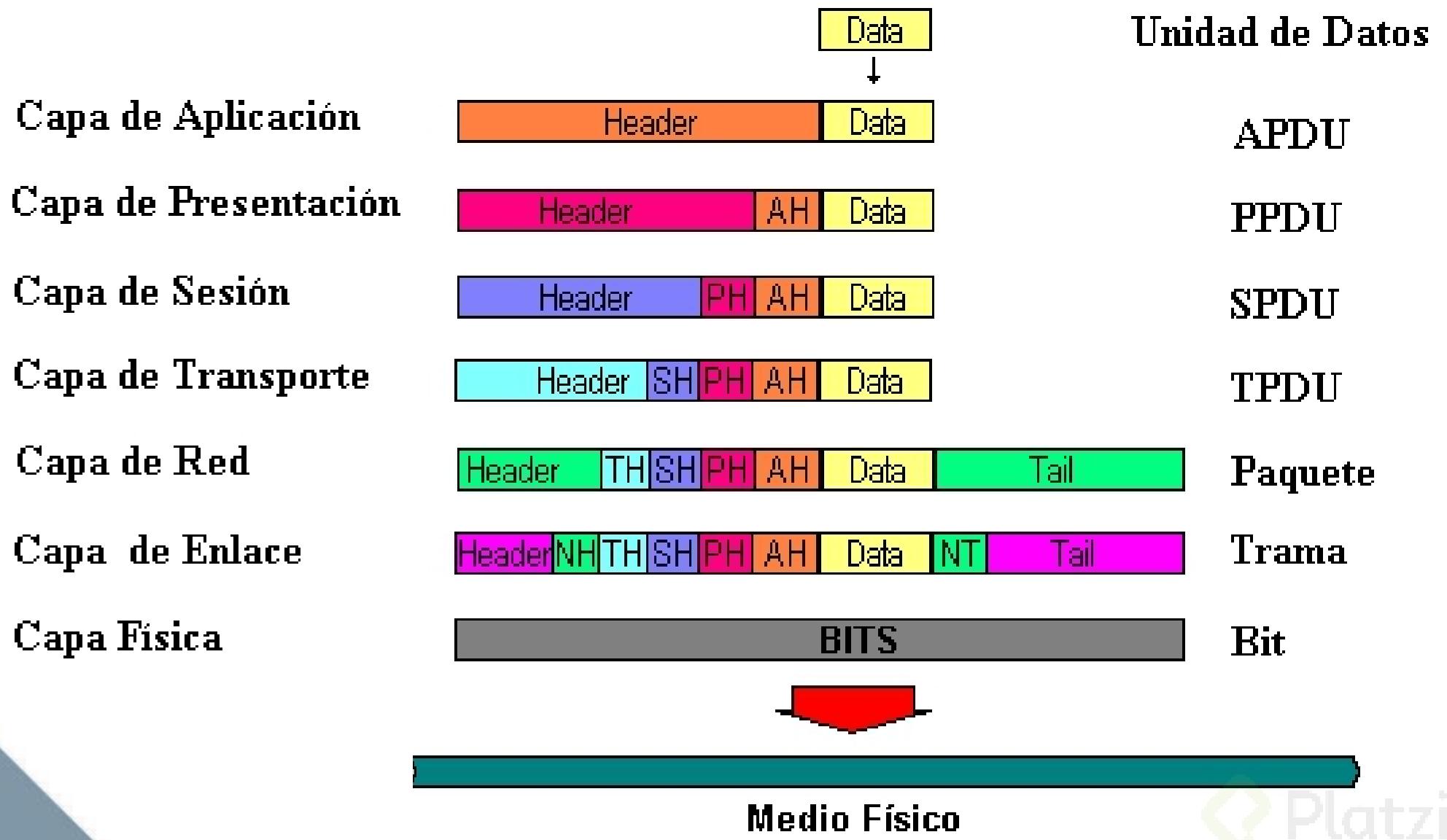
Es la combinación de dos o más canales de información en un solo medio de transmisión (permite varias comunicaciones de forma simultánea)



# Multiplexación

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.



Unidad de Datos

Capa de Aplicación



APDU

Capa de Presentación



PPDU

Capa de Sesión



SPDU

Capa de Transporte



TPDU

Capa de Red



Paquete

Capa de Enlace



Trama

Capa Física



Bit

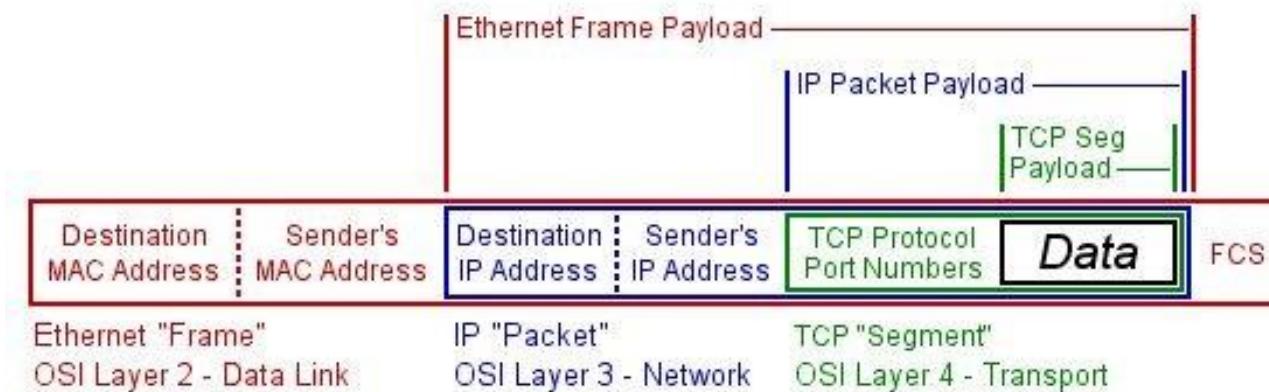


Medio Físico

# PDU Protocol Data Unit

Unidad que nos permite identificar la información a medida que es transmitida a través de las capas de

## Encapsulation Payloads



---

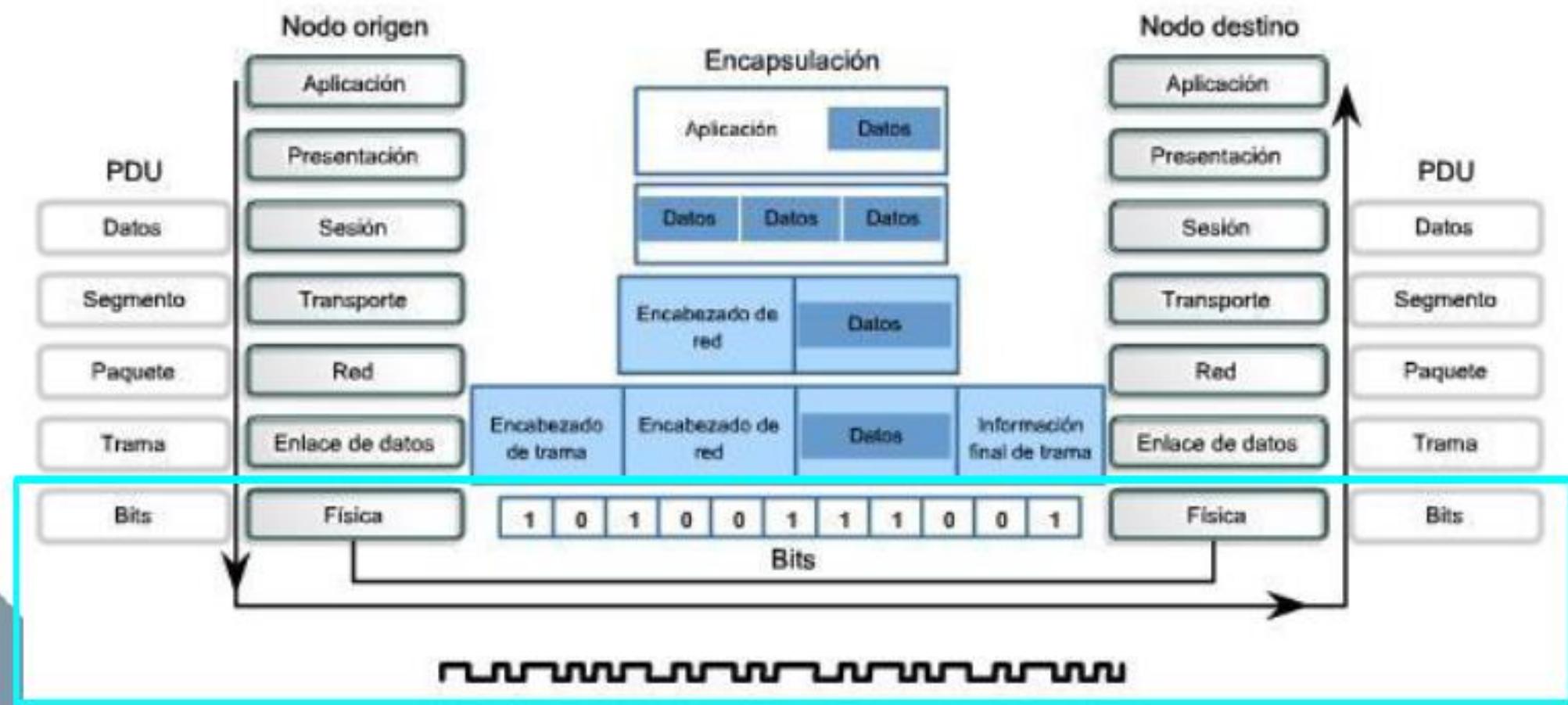
# Práctica

Usa Wireshark para analizar el tráfico de red

---

# Capa Física

Medios de RED



En los diagramas, las señales en los medios físicos están representadas por medio de este símbolo.

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 otro 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.

**NIC**

# Dispositivos y medios

Network Interface Card



**Cable**



**Inalámbrica**

# La capa física - Capa 1

1

- Los datos se ponen en paquetes en la capa de **red**.
- Los datos se encapsulan en frames en la capa de **enlace de**

2

- La **capa física** codifica los frames y crea las ondas eléctricas, ópticas o de radio que representan los bits en cada frame.

3

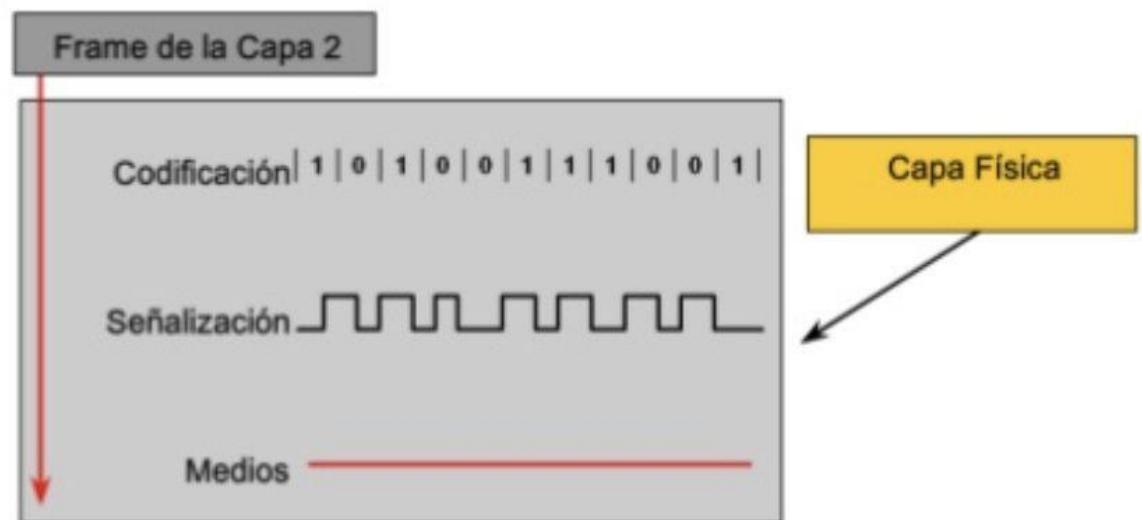
- Las señales son enviadas a los medios.

4

- El receptor toma las señales del medio, las transforma de nuevo en bits.
- Luego pasa por la capa de enlace de datos como un frame completo.

# Funciones de la capa Física

1. Controlar los componentes físicos.
2. Codificar/decodificar los datos.
3. Señalización

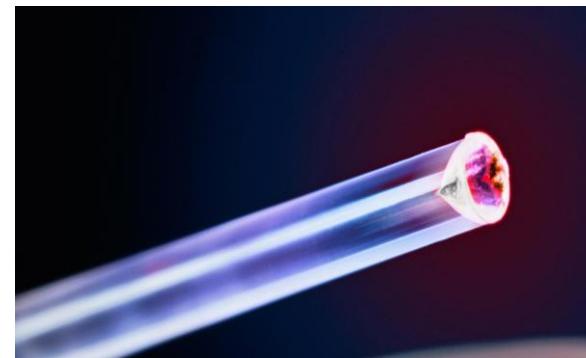


---

# Señales que son transmitidas en la capa física



Cable de cobre



Cable de fibra  
óptica



Inalámbrico

# **Organizaciones que regulan los estándares de la capa Física**

- La Organización Internacional para la Estandarización (ISO)
- El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)
- El Instituto Nacional Estadounidense de Estándares (ANSI)
- La Unión Internacional de Telecomunicaciones (ITU)  
La Asociación de Industrias Electrónicas/Asociación de la Industria de las Telecomunicaciones (EIA/TIA)  
Autoridades de las telecomunicaciones nacionales, como la Comisión Federal de Comunicaciones (FCC) en EE.UU.

---

# Medidas de rendimiento de los medios

## Ancho de banda

Capacidad de un medio para transportar datos

Unidad de ancho de banda	Abreviatura	Equivalencia
Bits por segundo	bps	1 bps = unidad fundamental del ancho de banda
Kilobits por segundo	kbps	1 kbps = 1,000 bps = $10^3$ bps
Megabits por segundo	Mbps	1 Mbps = 1,000,000 bps = $10^6$ bps
Gigabits por segundo	Gbps	1 Gbps = 1,000,000,000 bps = $10^9$ bps
Terabits por segundo	Tbps	1 Tbps = 1,000,000,000,000 bps = $10^{12}$ bps

## Rendimiento

Rendimiento

## Capacidad de útil

Cantidad de datos útiles que pueden ser enviados por la red

---

# Medios de red

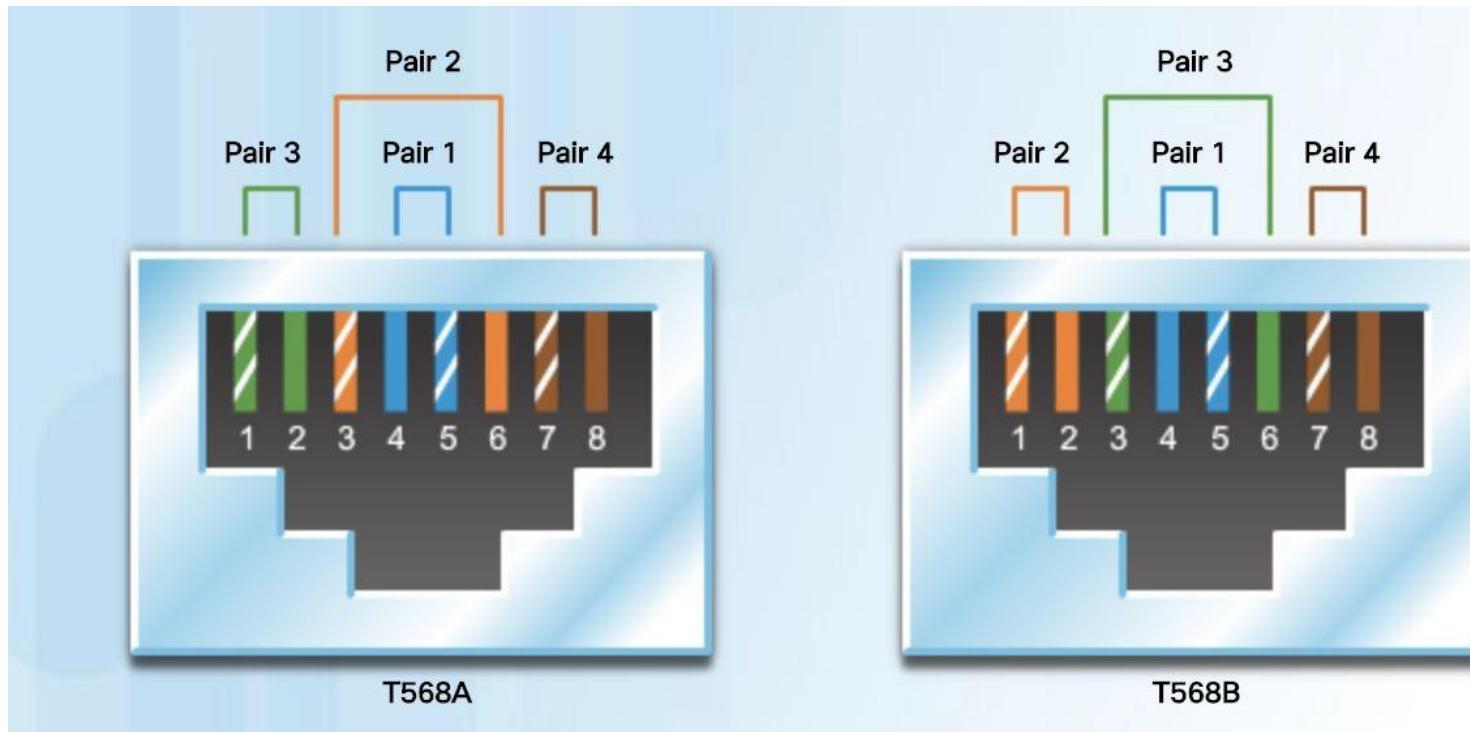
# Cable de cobre

UTP - Par trenzado sin blindaje

- STP - Par trenzado blindado
- Coaxial



# Práctica: Construcción de cables



---

# Capa de Enlace de Datos

Ethernet

---

# **Subcapas**

**MAC**



Capa de acceso al medio físico

**LLC**



Capa de comunicación con la capa de red

---

# **Funciones de la capa de enlace de datos**

1. Gestión del canal
2. Segmentación de la trama
3. Control de errores
4. Control de flujo
5. Recuperación de fallos

**Capa de Enlace de Datos:** Es la que se encarga de comunicar la parte física con la parte lógica.

**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.

**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 duplex o full duplex.

**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 ethernet

## ISO/OSI

7 Application layer

6 Presentation layer

5 Session layer

4 Transport layer

3 Network layer

2 Data link layer

1 Physical layer

## Internet

HTTP

SNMP

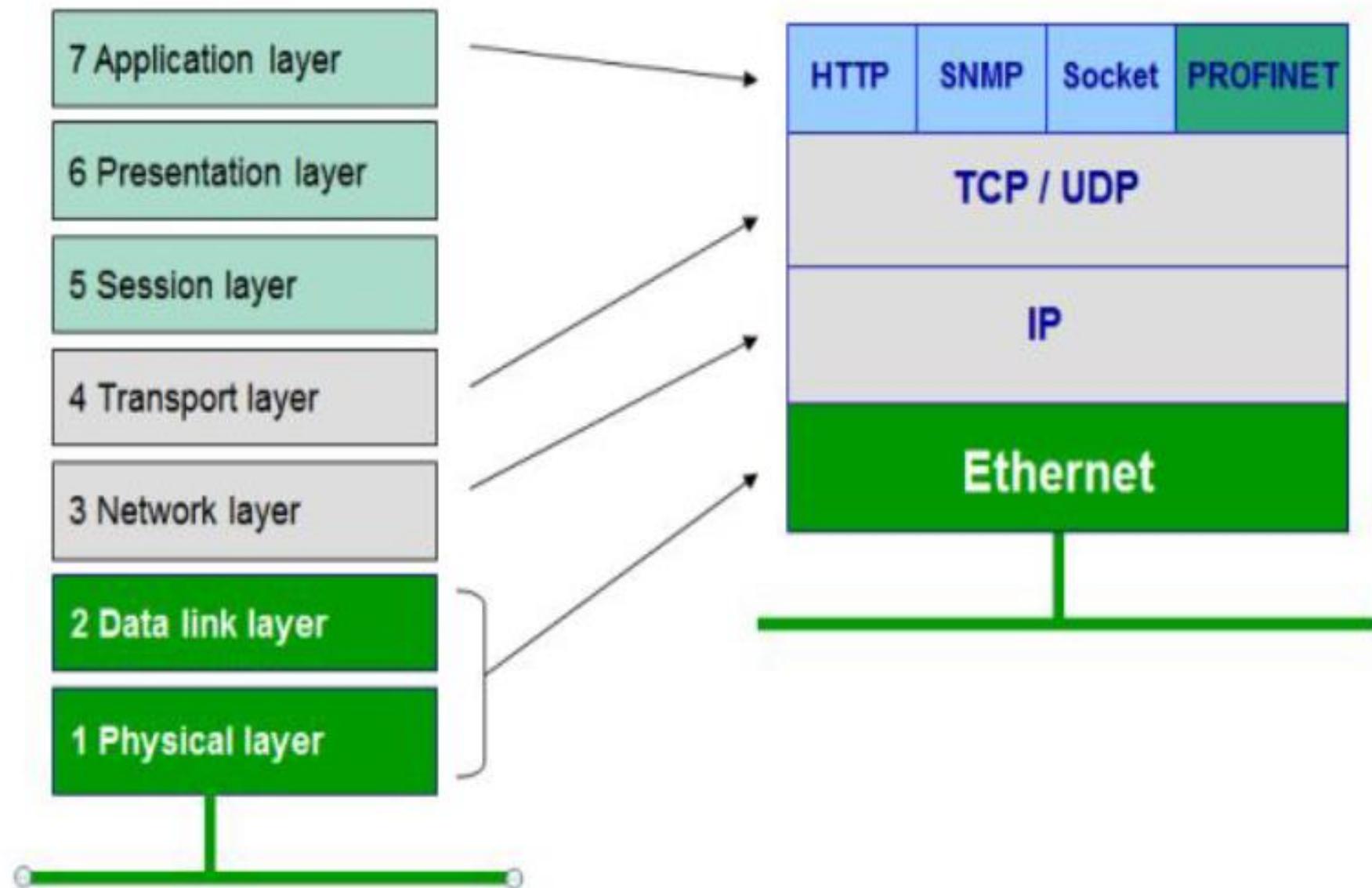
Socket

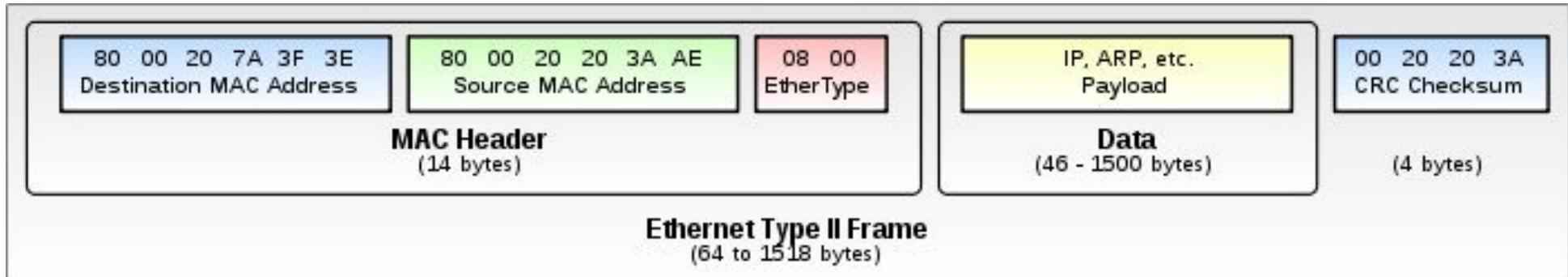
PROFINET

TCP / UDP

IP

Ethernet





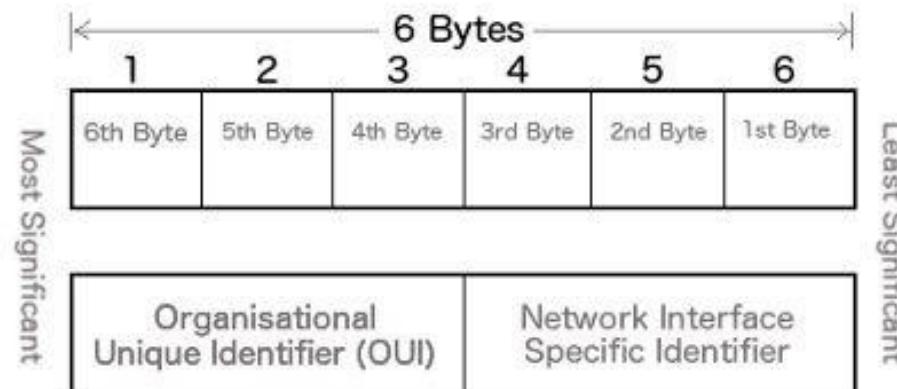
- Encabezado
  - Direcccionamiento
- Datos
- Trailer
  - FCS Frame Check Sequence
  - Stop Frame

# Direcciones MAC

Identificador ÚNICO de la NIC

- 12 dígitos hexadecimales
- Es ÚNICA por dispositivo

F0:E1:8D:52:39:A2



## Hablando un poco de temas de seguridad

Actualmente existen diferentes ataques enfocados a la clonación de las direcciones MAC, una de ellos es el MAC Spoofing:

¿Cual es el sentido de MAC Spoofing? :

- Suplantación de identidad
- Acceso a servicios no contratados
- Evasión de filtros MAC
- Anonimato
- Envenenamiento ARP

# Trama de Ethernet

La unidad de empaquetamiento de esta capa de enlace se llama **Trama o Frame** y se conforma de las siguientes partes:

- Encabezado

- Direccionamiento

- Direccion MAC de Origen

- Direccion MAC de Destino

- Datos

- Datos empaquetados en la capa de RED

- Trailer

- Bits que ayudan a determinar si llego completa la trama

- FCS(Frame Check Sequence)

- Es un número que se calcula apartir de los datos y determina si llego completo

- Stop Frame

- Identificador para determinar que la trama termino

---

# Procesamiento de tramas

## Reenvío de tramas

Dirección de destino	Dirección de origen	Datos
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA	Datos encapsulados
Direccionamiento de la trama		



Origen

AA:AA:AA:AA:AA:AA



Esto no está dirigido a mí. Lo ignoraré.

BB:BB:BB:BB:BB:BB

Esto es mío.



Destino

CC:CC:CC:CC:CC:CC

Esto no está dirigido a mí. Lo ignoraré.



DD:DD:DD:DD:DD:DD

**UNICAST**



Un solo destino

**MULTICAST**



A un grupo

**BROADCAST**



A todos los miembros del grupo

# La dirección MAC

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)

**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.

## La dirección MAC

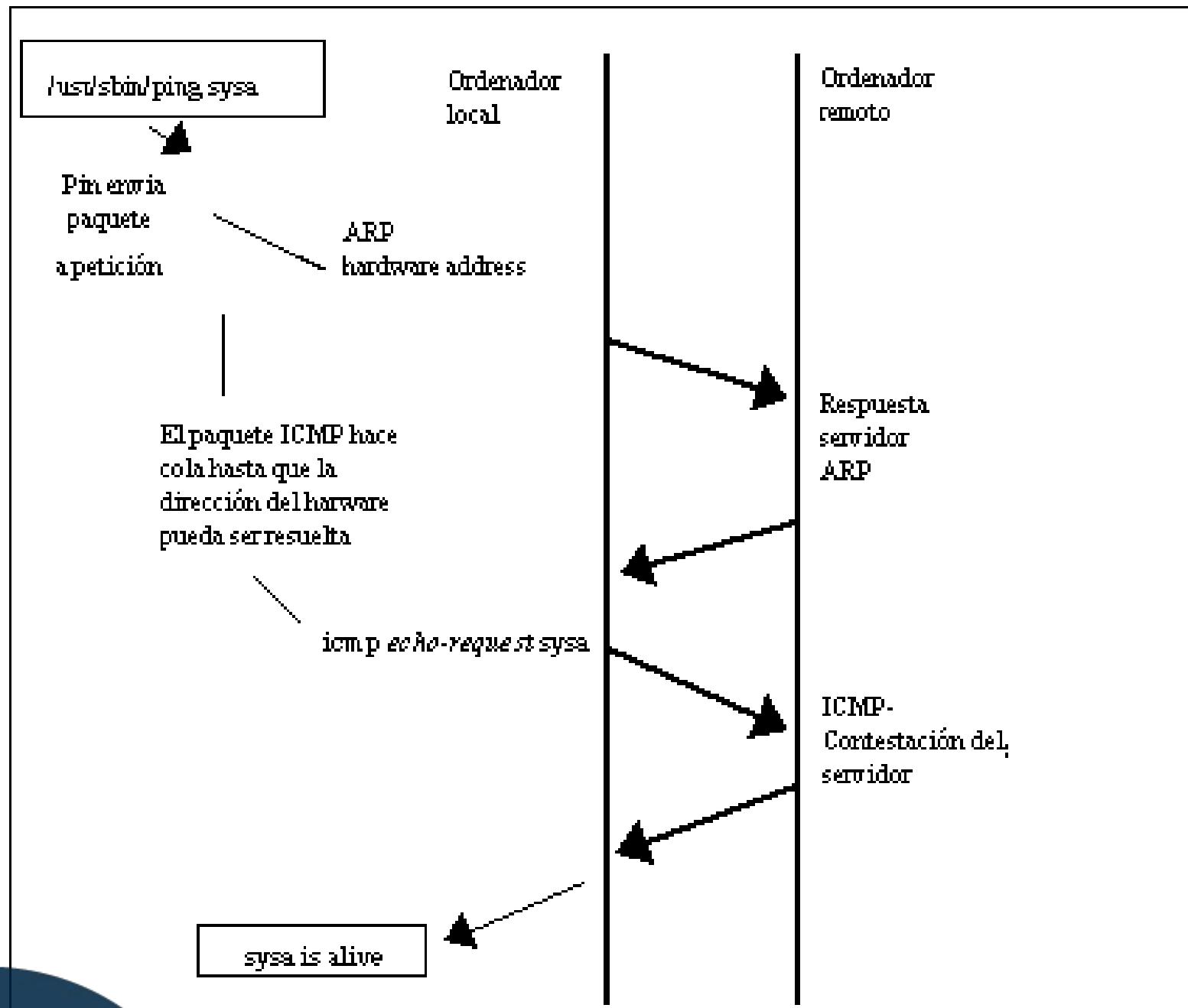
Cada NIC en la red revisa la información en la subcapa MAC para ver si la dirección MAC de destino que está en la trama coincide con la dirección MAC física del dispositivo almacenada en la RAM. Si no hay coincidencia, el dispositivo descarta la trama. Cuando la trama llega al destino en que la MAC de 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.

## La dirección MAC

---

# Protocolo de Resolución de Direcciones

ARP



En red de computadoras, el protocolo de resolución de direcciones (ARP, del inglés Address Resolution Protocol) es un protocolo de comunicaciones de la capa de enlace, responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast, MAC = FF FF FF FF FF FF) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto solo funciona si todas las máquinas lo soportan.

ARP está documentado en el RFC 826. El protocolo de resolución de direcciones inverso (RARP) realiza, obviamente, la operación inversa y se encuentra descrito en el RFC 903.

## Address Resolution Protocol (ARP)

---

# Capa de RED

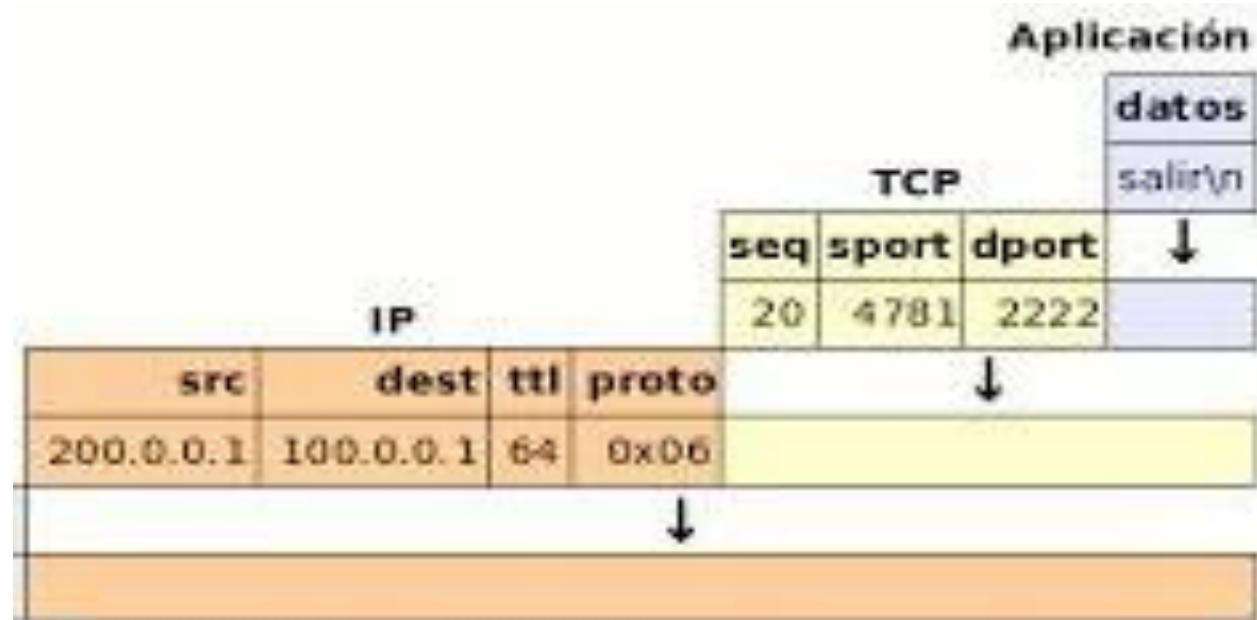
---

# **Funciones de la capa de Red**

Hacer el direccionamiento de paquetes

- Encapsulamiento de los paquetes
- Enrutamiento
- Desencapsulamiento de los paquetes

# PDU de la capa de Red



---

# **TTL Time To Live**

Es la cantidad máxima de saltos por los que debe pasar un mensaje hasta que es rechazado

# CAPA DE RED

---

Se encarga de enrutar los datos a través de diferentes redes. El router será el encargado de des encapsular 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

# CAPA DE RED

---

PDU de la capa de red (unidad de datos de protocolo)

Se asignan tres campos:

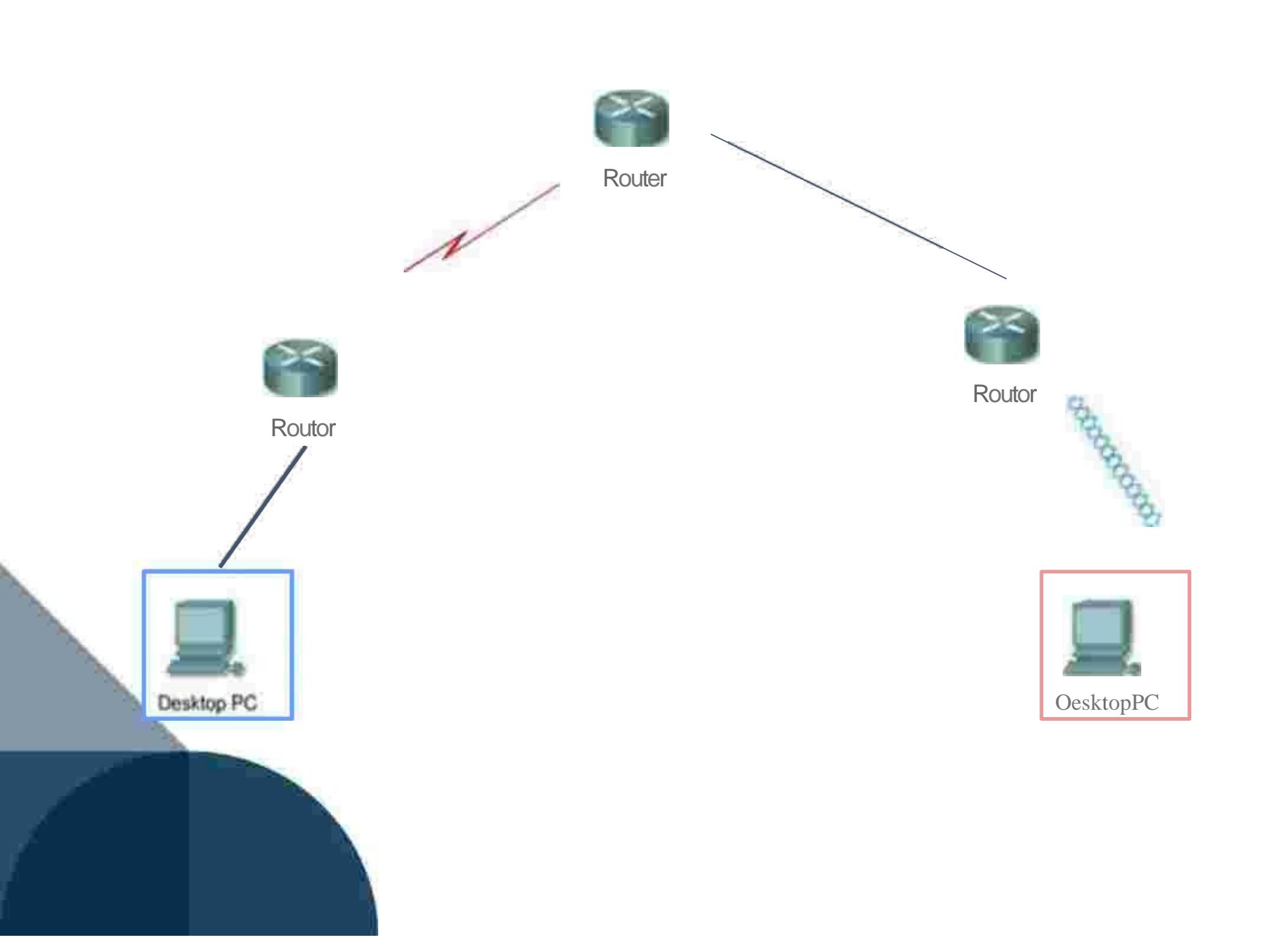
**Dirección de origen** - ¿Quién envía la solicitud?

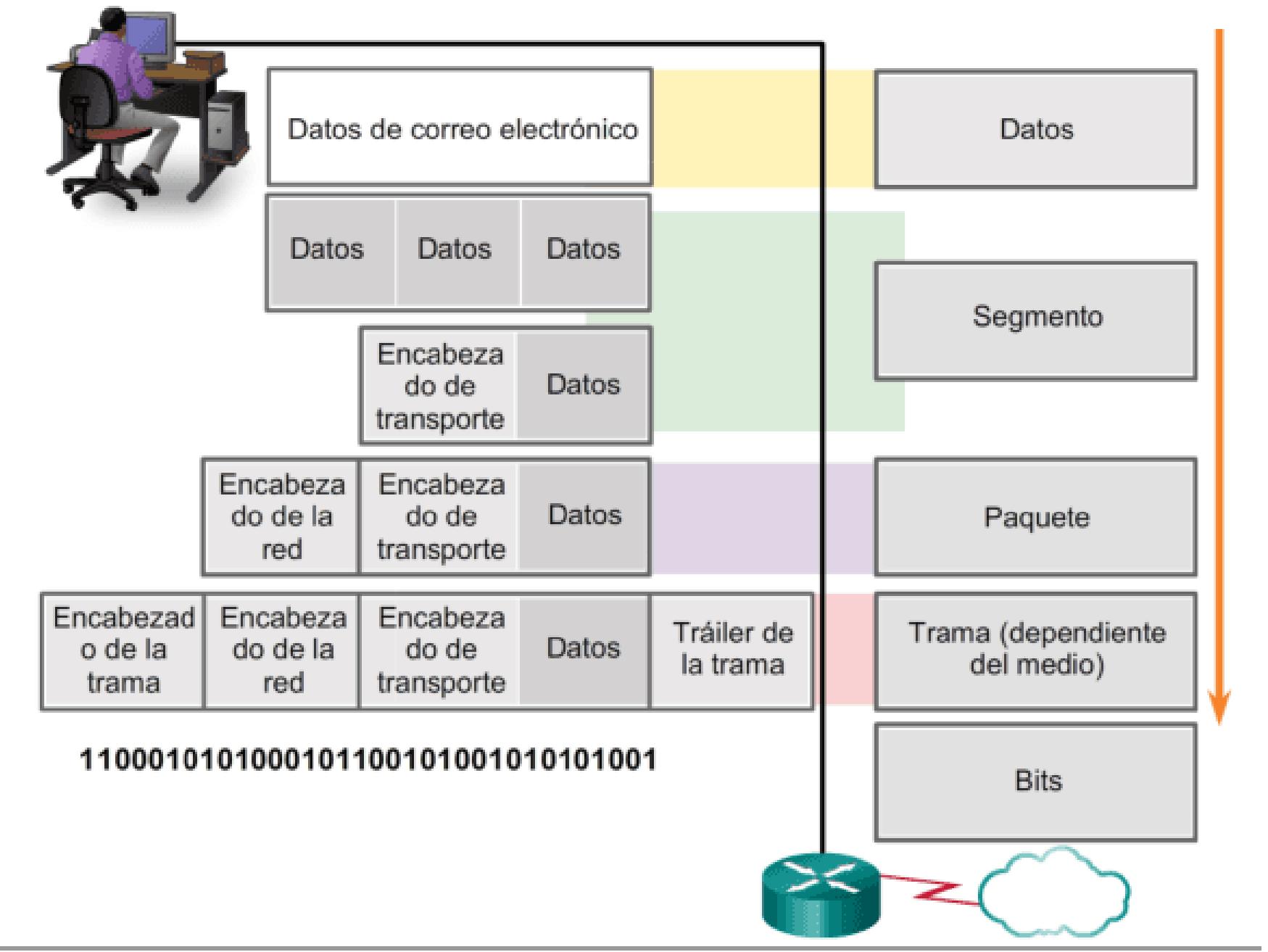
**Dirección de destino** - ¿A dónde se envía el mensaje?

**TTL (Time To Live)** – 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





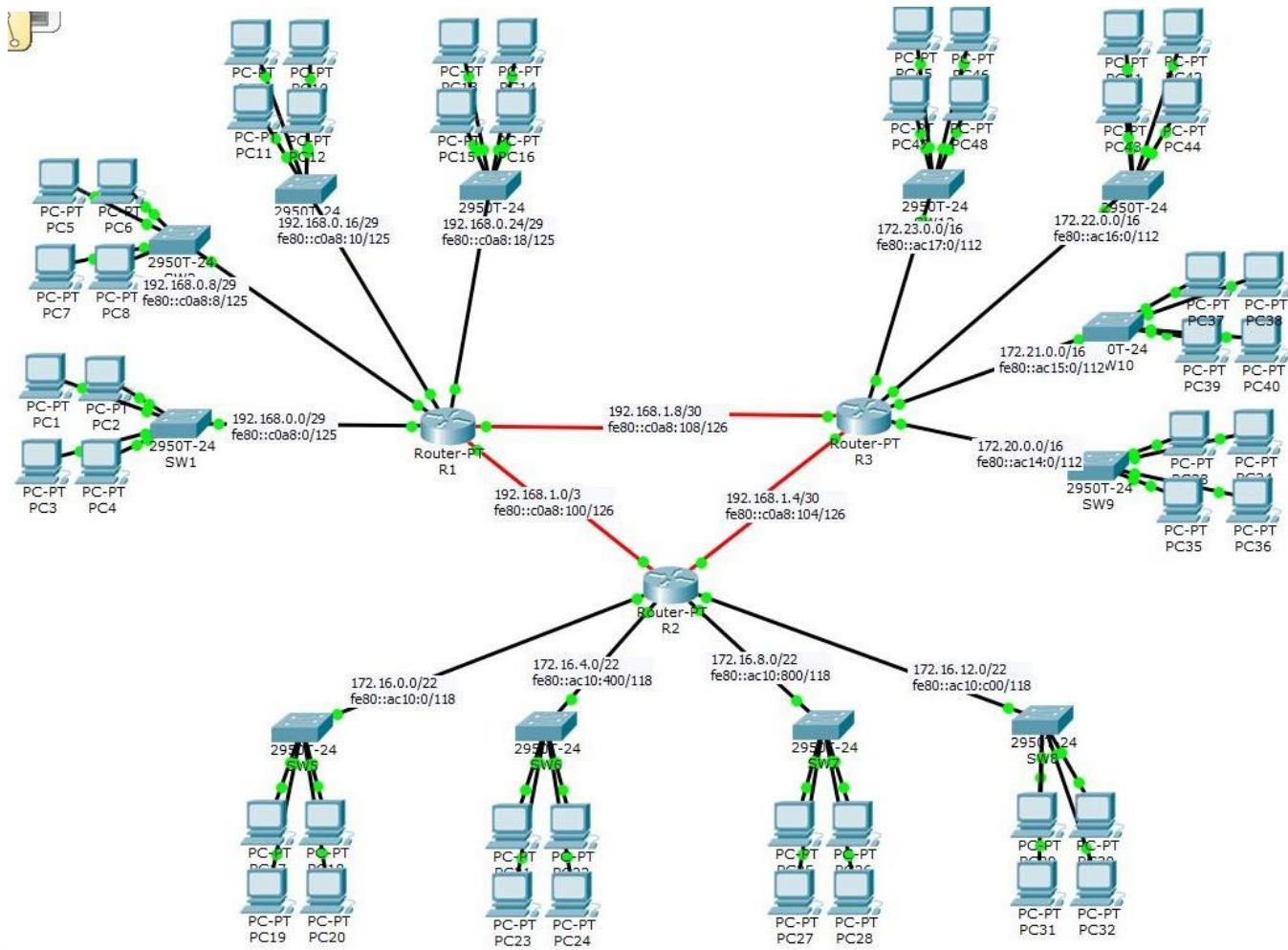
# **Default Gateway o Puerta de enlace predeterminada**

Es la ruta predeterminada o ruta por defecto que se le asigna a un equipo y tiene como función enviar cualquier paquete del que no conozca por cuál interfaz enviarlo y no esté definido en las rutas del equipo.

Un host, cuando ha de enviar un paquete de datos a un destino, calcula, mediante la dirección IP de destino y la mascara 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 cual es la dirección IP del destino y vuelve a calcular, de acuerdo con la mascara de red de esa interfaz, a que red pertenece, para después, consultar en su tabla de routing (que se puede configurar de 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.

# Enrutamiento





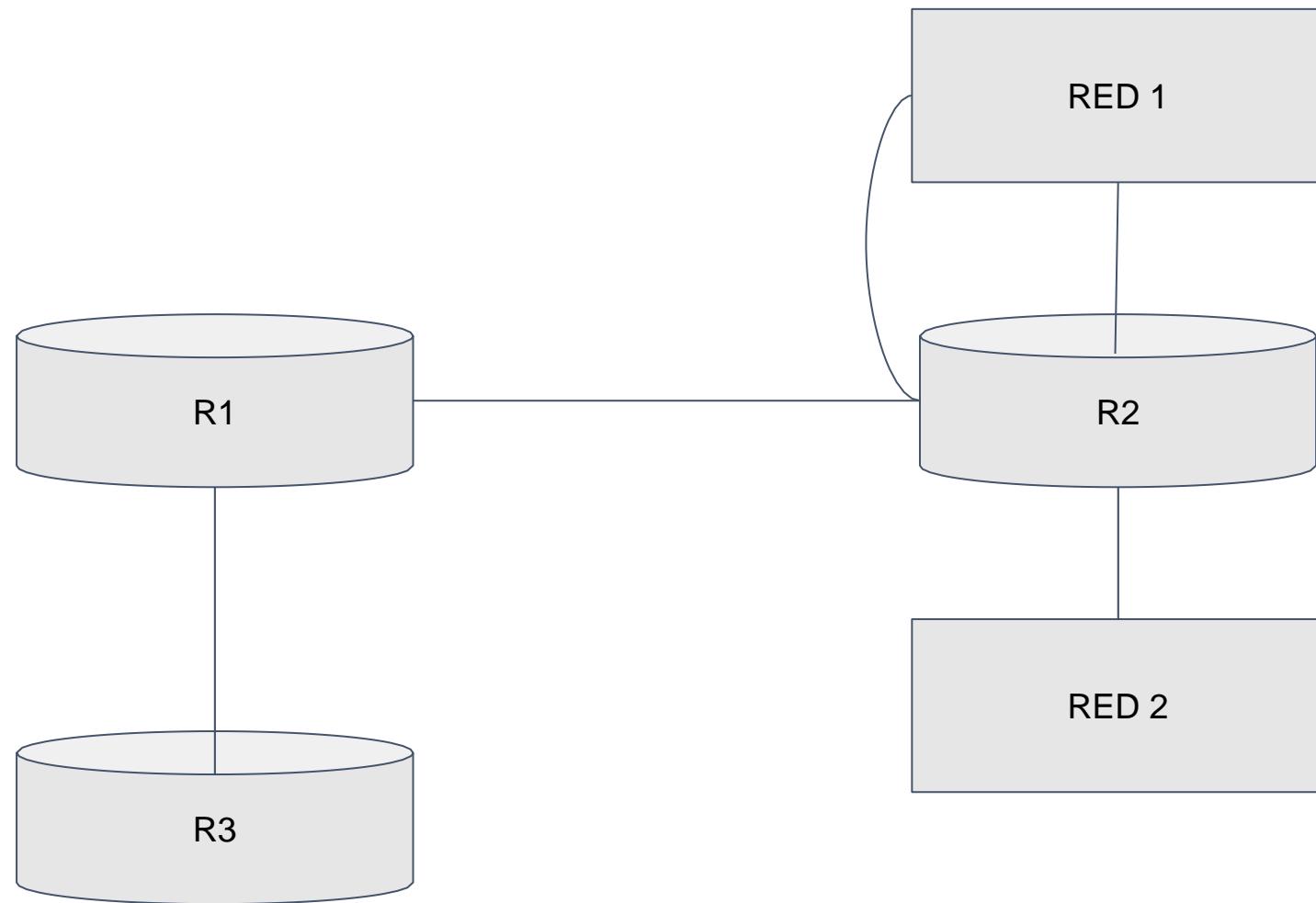
IP



Mascara de Subred



Dirección del siguiente salto



---

# Protocolo IP

Direcciones IP y Máscara de Bits

---

**Enrutamiento:** Consiste en encontrar un camino que conecte una red con otra, 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



- Gama de direcciones host
- I. 0. 0. 0 a 127. 255. 255. 255
- I28. 0. 0. 0 a I91. 255. 255. 255
- I92. 0. 0. 0 a 223. 255. 255. 255
224. 0. 0. 0 a 239. 255. 255. 255
240. 0. 0. 0 a 247. 255. 255. 255
- |   |              |                            |      |
|---|--------------|----------------------------|------|
| A | <b>0</b>     | Red                        | Host |
| B | <b>10</b>    | Red                        | Host |
| C | <b>110</b>   | Red                        | Host |
| D | <b>1110</b>  | Dirección multitransmisión |      |
| E | <b>11110</b> | Reservado para uso futuro  |      |

## CLASE A

- El primer octeto identifica la red.  
Tres últimos octetos (24 bits) pueden ser asignados a los hosts.
- Cantidad máxima de *hosts* es  $2^{24} - 2$
- 16 777 214 *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  $2^{16} - 2$ .
- 65 534 *hosts*.

## CLASE 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  $2^8 - 2$ .
- 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.

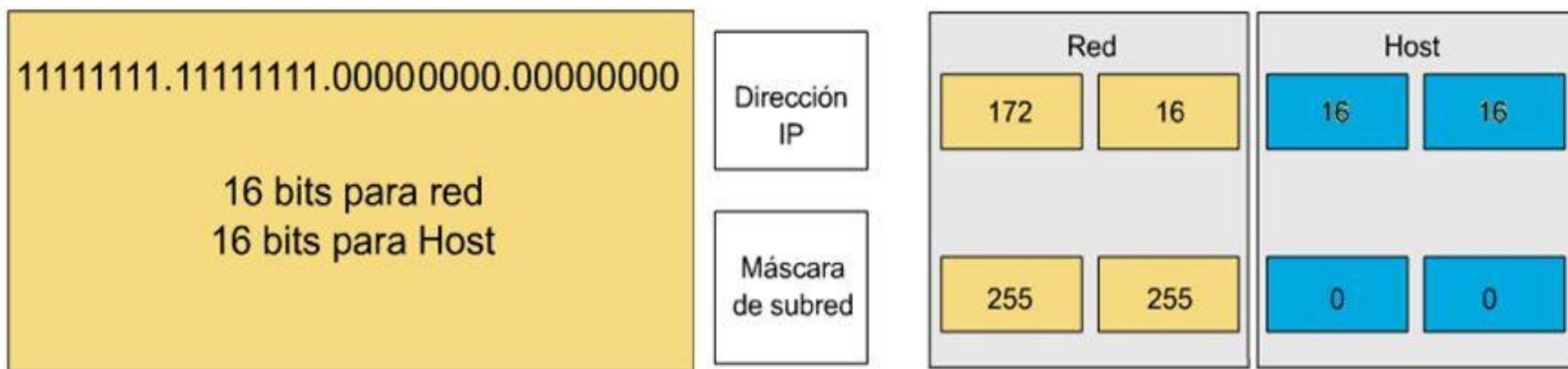
A - 255.0.0.0 o 1111111.0000000.0000000.0000000

B - 255.255.0.0 o 1111111.1111111.0000000.0000000

C-255.255.255.0 o 1111111.1111111.1111111.0000000

# Máscara de Subred

- El propósito de una máscara de subred, es ayudar a los host y routers a determinar la ubicación de la red en la que se pueda ubicar el host destino.
- Una máscara de subred tiene una longitud de 32 bits y posee 4 octetos, al igual que la dirección IP.
- La porción de red se componen exclusivamente de unos.
- La porción del host, se compone exclusivamente de ceros.



- 
- 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  
169.254.0.0/16 169.254.255.254
  4. Test  
192.0.2.0/24

## IP PUBLICA Y PRIVADA

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, tu puedes asignar direcciones IP basándote en tus reglas de negocio.

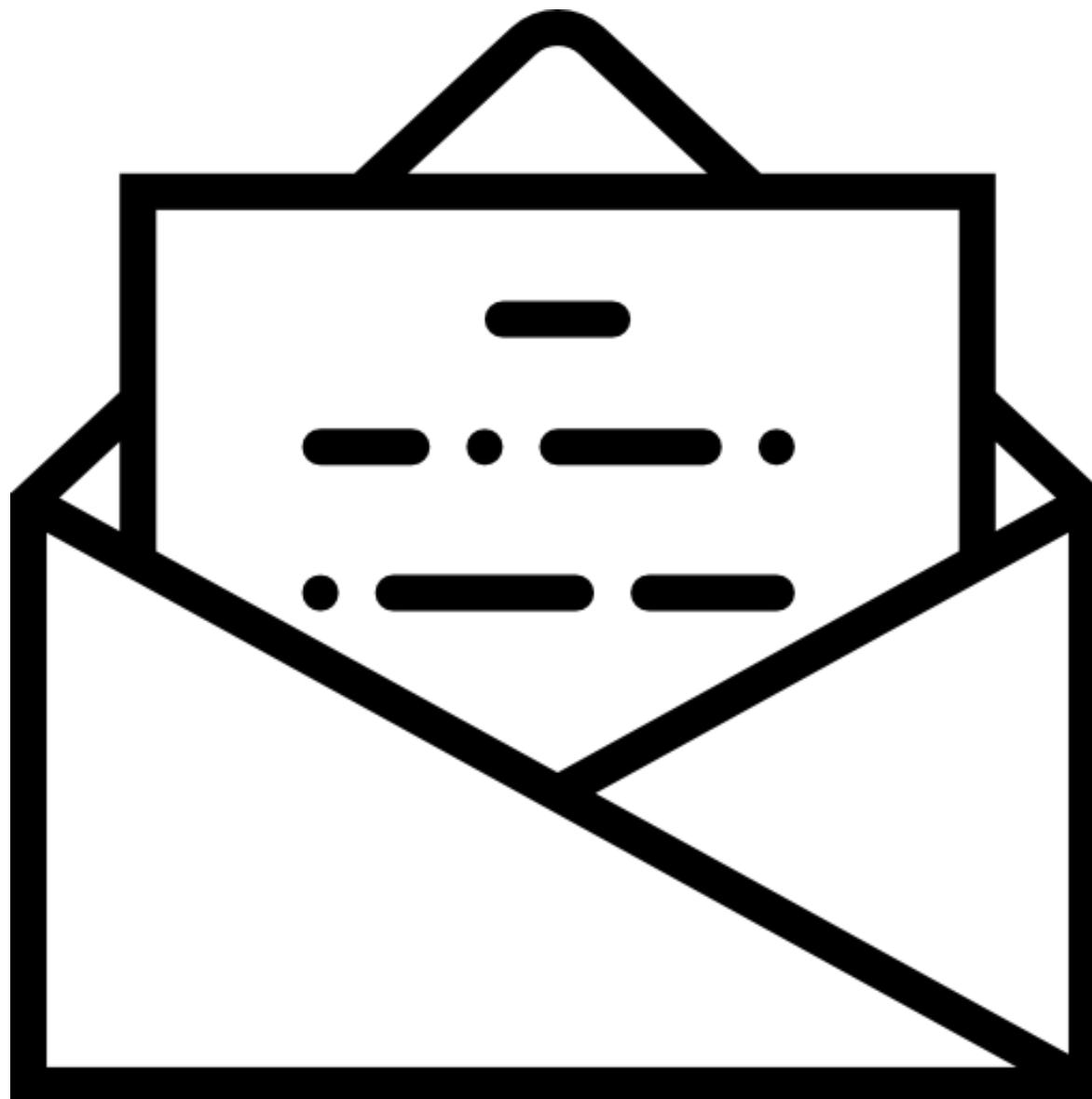
---

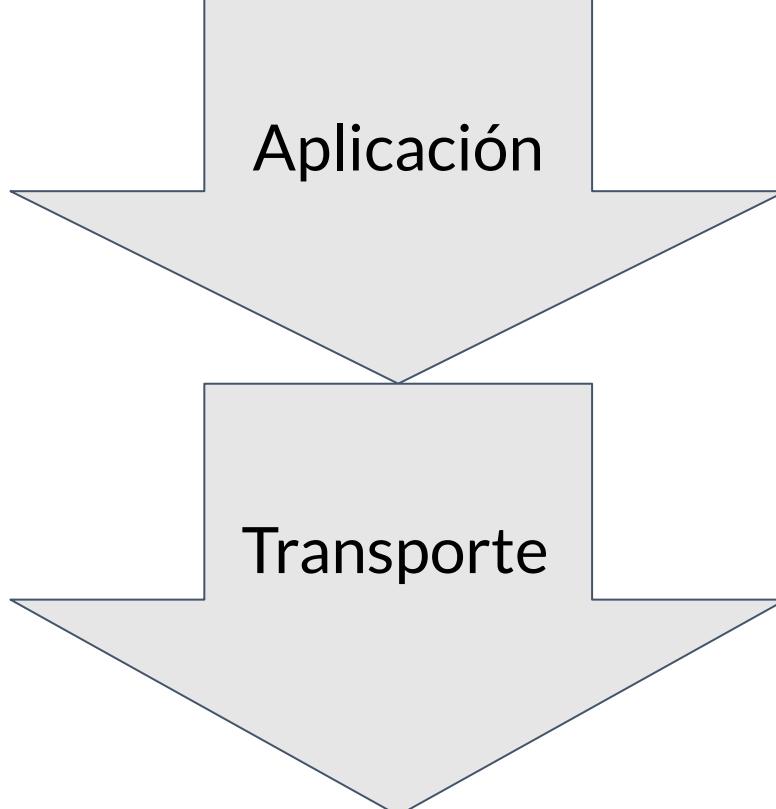
# Capa de Transporte

---

# **Tareas de la capa de Transporte**

- Segmentar los datos
- Realizar el seguimiento de las conversaciones individuales
- Identificar las aplicaciones de acuerdo con el puerto





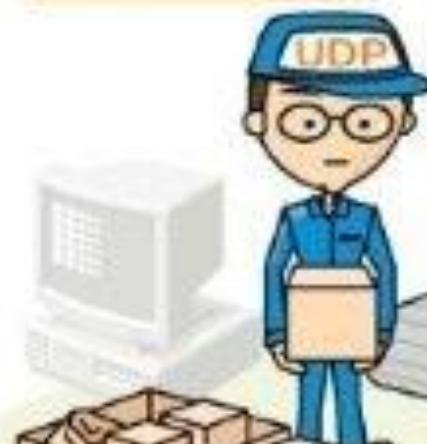
Aplicación

Transporte

---

# TCP y UDP

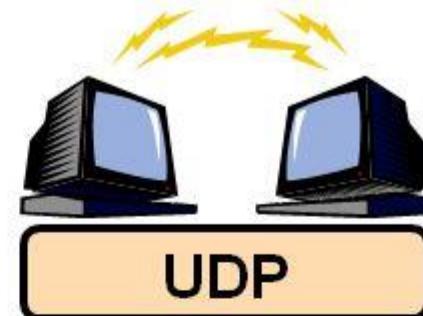
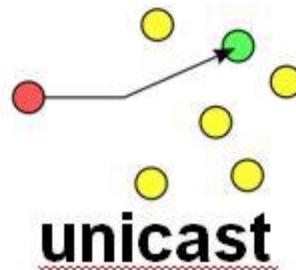
**UDP**  
Sólo envío datos.



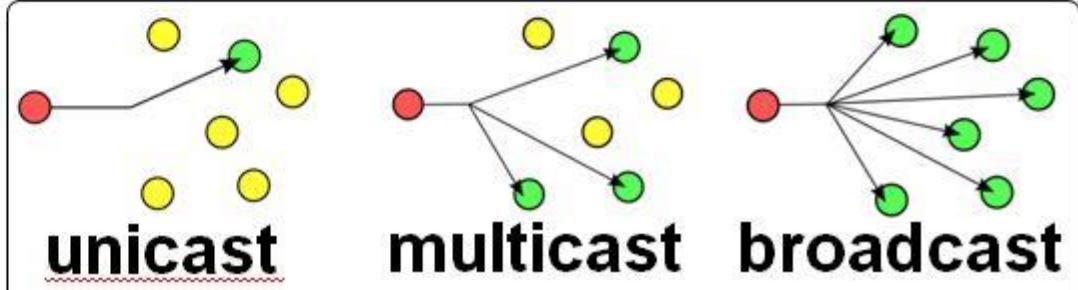
**TCP**  
Avisa que envía datos  
y se lo confirman al llegar



- Slower but reliable transfers
- Typical applications:
  - Email
  - Web browsing



- Fast but non-guaranteed transfers ("best effort")
- Typical applications:
  - VoIP
  - Music streaming

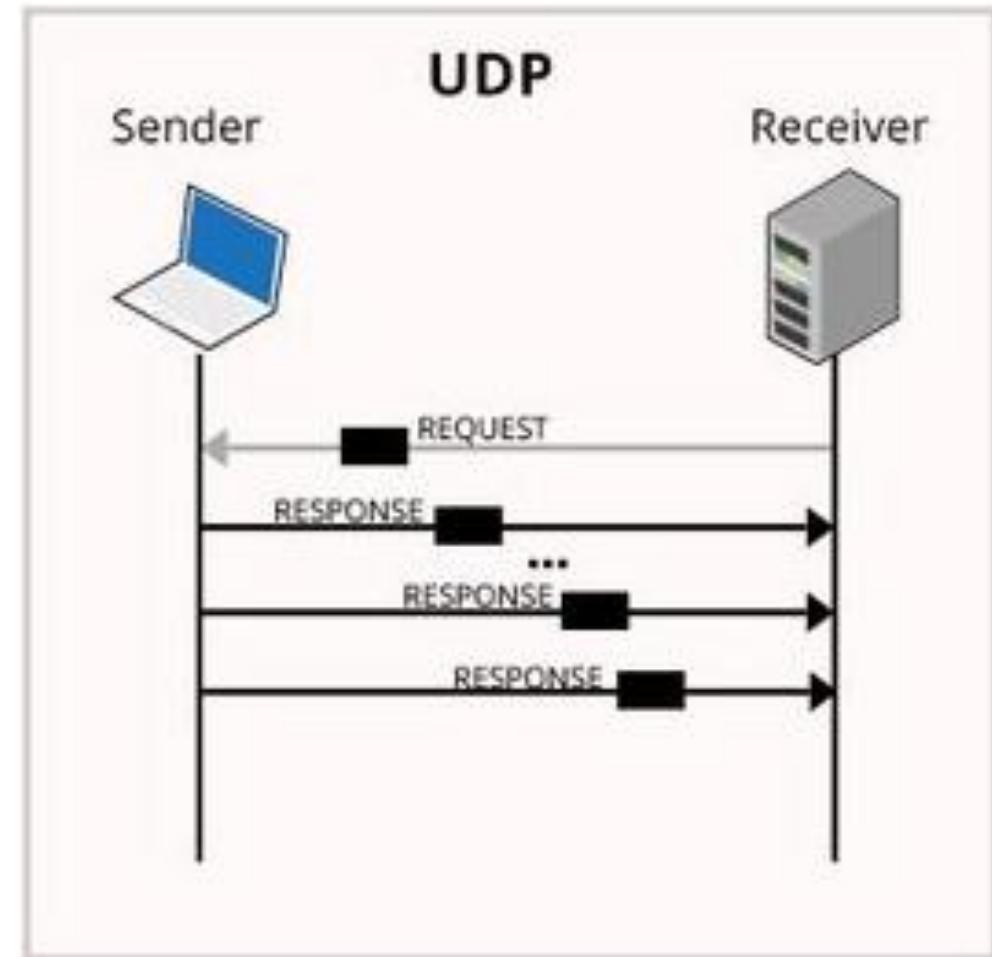
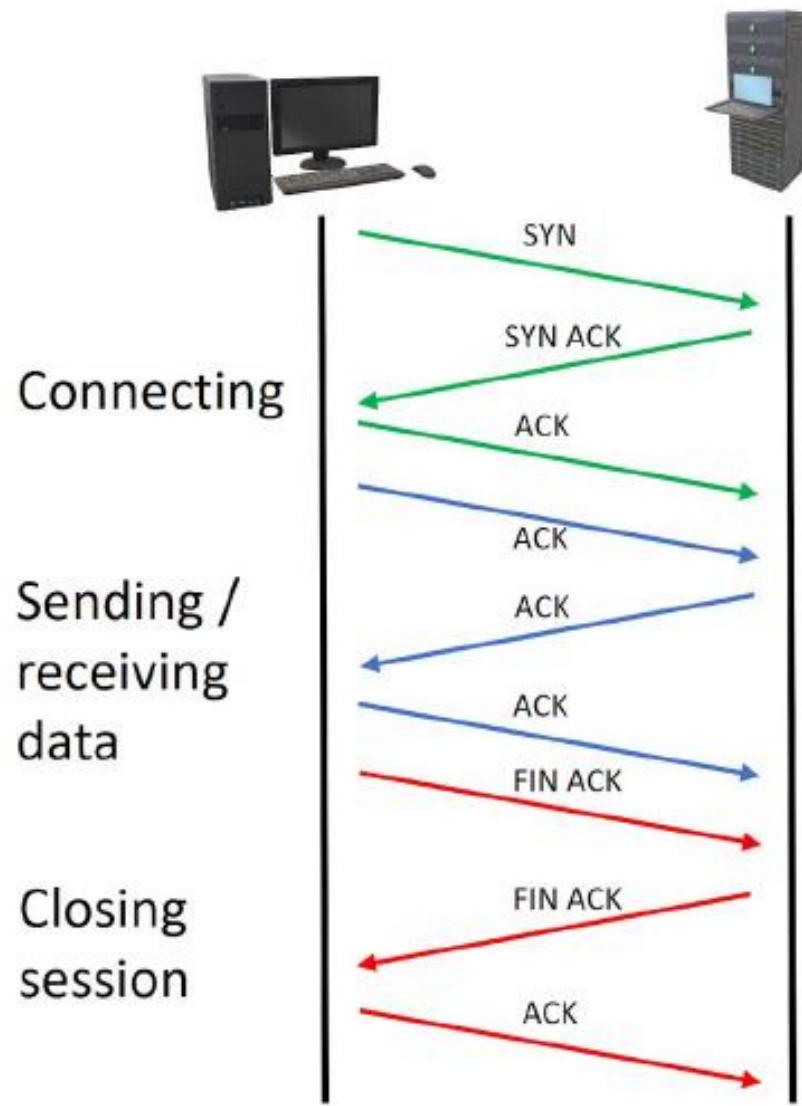


# TCP (Protocolo de Control de Transmisión)

**TCP Segment Header Format**

Bit #	0	7	8	15	16	23	24	31
0			Source Port			Destination Port		
32				Sequence Number				
64				Acknowledgment Number				
96	Data Offset	Res		Flags		Window Size		
128			Header and Data Checksum			Urgent Pointer		
160...				Options				

# Comunicaciones de datos



# UDP

## UDP Datagram Header Format

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Length				Header and Data Checksum			

## Protocolo TCP

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.

## Protocolo UDP

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.

---

# Practica CISCO

#	Ip SubRed	1st	Last	Broadcast
1	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31
2	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63
3	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95
4	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127

---

# Planteamiento

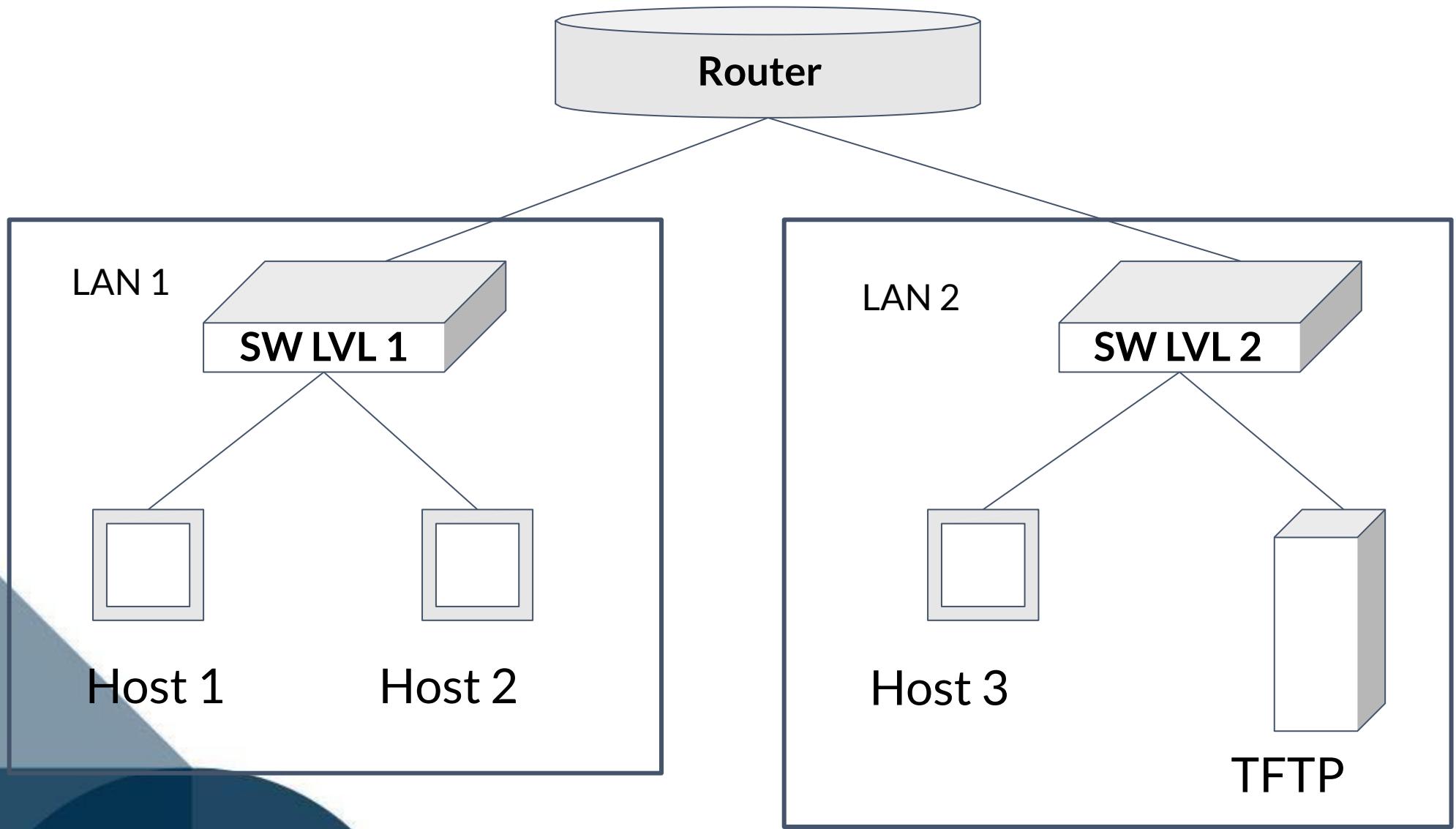
Configuración de los dispositivos de la red

- 1 Router
- 2 switches level 1y level 2
- 3 pcs
- 1 servidor TFTP para el backup de las configuraciones

**RETO: toma la última dirección de red y haz subredes de forma que tengamos en total  
4 redes con 30 hosts  
2 redes con 14 hosts**

#	Ip SubRed	1st	Last	Broadcast
1	192.168.1.0	192.168.1.1	192.168.1.30	192.168.1.31
2	192.168.1.32	192.168.1.33	192.168.1.62	192.168.1.63
3	192.168.1.64	192.168.1.65	192.168.1.94	192.168.1.95
4	192.168.1.96	192.168.1.97	192.168.1.126	192.168.1.127
5	192.168.1.128	192.168.1.129	192.168.1.142	192.168.1.143
6	192.168.1.144	192.168.1.145	192.168.1.158	192.168.1.159

Dispositivo	Interfaz	IPv4	Máscara de subred	IPv4 Default Gateway
Router Platzi	G 0/0	192.168.1.126	255.255.255.224	
	G 0/1	192.168.1.158	255.255.255.240	
	Link Local	FE80::1		
Switch LVL 2	Vlan 1	192.168.1.157	255.255.255.240	192.168.1.158
Host 1	NIC	192.168.1.97	255.255.255.224	192.168.1.126
Host 2	NIC	192.168.1.98	255.255.255.224	192.168.1.126
Host 3	NIC	192.168.1.145	255.255.255.240	192.168.1.158
TFTP	NIC	192.168.1.146	255.255.255.240	192.168.1.158



---

Gracias :)