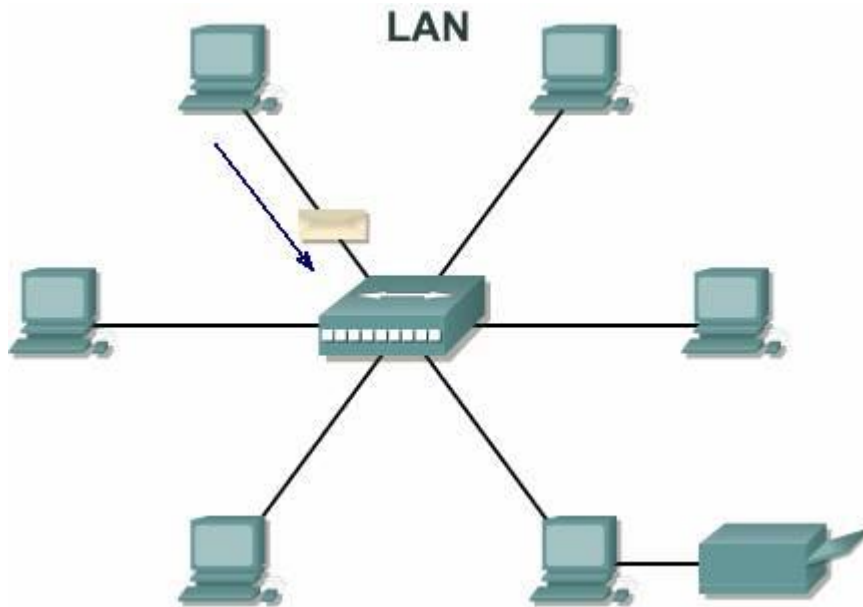


# Sistemas Informáticos

---

## UD 10. Redes de área local



# ÍNDICE

1. Características.....	2
2. Componentes Hardware de una red.....	2
2.1. Tarjeta de red.....	2
2.2. Medios de transmisión.....	3
2.2.1. Medios guiados .....	4
2.2.2. Medios no guiados .....	8
2.3. Dispositivos de interconexión.....	9
2.3.1. Repetidor.....	9
2.3.2. Hub.....	10
2.3.3. Puente.....	11
2.3.4. Access Point (punto de acceso).....	12
2.3.5. Switch.....	13
2.3.6. Router .....	13
3. Componentes software.....	14
3.1. Driver de la NIC (tarjeta de red).....	14
3.2. Protocolos de comunicación.....	14
3.2.1. La familia de protocolos TCP/IP. Direcciones IP. Clases de IP. Subnetting .....	14
3.3. Sistema Operativo de red .....	20
3.4. Servicios de red:.....	20
3.4.1. Directorio .....	20
3.4.2. Recursos compartidos.....	21
3.4.3. DNS.....	21
3.4.4. Servidor de archivos (FTP, SMB y NFS) .....	22
3.4.5. Correo electrónico .....	23
3.4.6. Web (HTTP) .....	24
3.4.7. DHCP .....	24
3.4.8. SSH .....	24
4. Topologías en LANs.....	25
5. Cableado estructurado.....	26

## 1. CARACTERÍSTICAS

**LAN** (Local Area Network / redes locales):

- Tienen una extensión muy limitada. Ej: una oficina, una clase...
- Es una red privada (pertenecen a una determinada organización)
- Tienen una velocidad de transmisión elevada.

Ejemplos:

- Ethernet: 10Mb/s
- Fast Ethernet: 100 Mb/s
- Gigabit Ethernet: 1000 Mb/s
- 10 Gigabit Ethernet: 10Gb/s
- Las transmisiones son muy fiables (tienen una tasa de error muy baja)
- Se suelen organizar según cableado estructurado.
- En este tipo también podríamos incluir las **WLAN** (Wireless LAN, es decir, LAN inalámbricas).

## 2. COMPONENTES HARDWARE DE UNA RED

### 2.1. TARJETA DE RED

- Es una tarjeta de expansión que permite a un ordenador o impresora acceder a una red y compartir recursos. Un equipo puede tener una o más tarjetas de red para permitir más configuraciones o atacar distintas redes.
- Existen tarjetas apropiadas para cada tecnología de red: Ethernet, Token Ring, FDDI, redes inalámbricas...
- Actualmente, las más comunes son las de tipo **Ethernet** usando conector **RJ45**.



- Cada tarjeta de red posee un **numero identificador único** de 48 bits en hexadecimal llamado **MAC**.

```
C:\WINDOWS\system32\cmd.exe
Configuración IP de Windows

Nombre del host . . . . . :
Sufijo DNS principal . . . . . :
Tipo de nodo . . . . . : híbrido
Enrutamiento habilitado . . . . . : No
Proxy WINS habilitado . . . . . : No
Lista de búsqueda de sufijo DNS: ujaen.es

Adaptador Ethernet Conexión de área local :
Sufijo de conexión específica DNS : ujaen.es
Descripción . . . . . : Marvell Yukon 88E8053 PCI-E Gigabit Ethernet Controller
Dirección física . . . . . : 00-14-85-C3-CD-F5
DHCP habilitado . . . . . : No
Dirección IP . . . . . : 150.214
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 150.214
Servidores DNS . . . . . : 150.214.170.15
                          150.214.170.21
                          150.214.170.22
Servidor WINS principal . . . . . : 150.214.170.106
```

- Las tarjetas de red necesitan de un software controlador (**driver**) que conduzca sus operaciones desde el Sistema Operativo.
- Se pueden configurar en modo gráfico (Windows desde el panel de control y en Linux desde el administrador de red) y en modo comando o Shell (en Windows con ipconfig y en Linux con ifconfig o iwconfig)

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Mar>ipconfig /all

Configuración IP de Windows

    Nombre del host . . . . . : mareta
    Sufijo DNS principal . . . . . :
    Tipo de nodo . . . . . : desconocido
    Enrutamiento habilitado. . . . . : No
    Proxy WINS habilitado. . . . . : No

Adaptador Ethernet Conexión de área local :

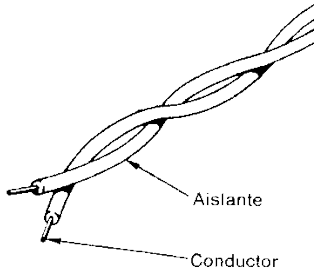
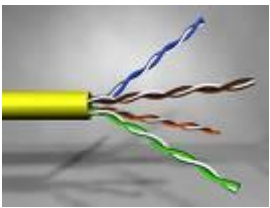

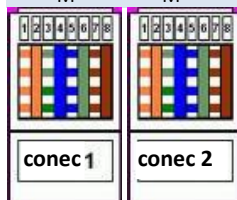
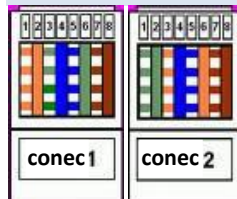
    Sufijo de conexión específica DNS :
    Descripción. . . . . : Adaptador Fast Ethernet compatible U
IA
    Dirección física. . . . . : 00-18-F3-74-22-20
    DHCP habilitado. . . . . : No
    Autoconfiguración habilitada. . . : Sí
    Dirección IP. . . . . : 192.168.0.102
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . : 192.168.0.1
    Servidor DHCP . . . . . : 192.168.0.1
    Servidores DNS . . . . . : 192.168.0.1
    Concesión obtenida . . . . . : martes, 26 de abril de 2011 21:33:45
    Concesión expira . . . . . : martes, 19 de enero de 2038 5:14:07
  
```

## 2.2. MEDIOS DE TRANSMISIÓN

¿Y por dónde pueden viajar los datos?

- Por medios **guiados** → cable
- Por medios **no guiados** → aire

2.2.1. Medios guiados

cable de pares	<div>Estructura</div> <div><p>Aislante</p><p>Conductor</p><p>Formado por pares de hilos de un metal conductor (normalmente cobre), aislados por una cubierta plástica</p><p>Conectores RJ45:</p></div>	<div>Ventajas</div> <ul style="list-style-type: none"><li>- Barato</li><li>- Fácil de instalar (flexible)</li></ul>	<div>Inconvenientes</div> <ul style="list-style-type: none"><li>- Sensible a las interferencias electromagnéticas→ esta sensibilidad se reduce trenzando los pares de cables</li><li>- Cuando se sobrepasan ciertas distancias, hay que usar repetidores para restablecer la señal</li></ul>	<div>Tipos</div> <ul style="list-style-type: none"><li>- <b>UTP:</b><ul style="list-style-type: none"><li>o Sin recubrimiento metálico externo, por lo que es más sensible a las interferencias.</li><li>o Es barato, flexible y fácil de usar.</li></ul></li><li>- <b>STP:</b><ul style="list-style-type: none"><li>- Con un recubrimiento metálico para evitar interferencias.</li><li>- Más difícil de instalar, ya que es menos flexible por lo que solo se usa en entornos eléctricamente hostiles.</li><li>- Más costoso.</li></ul></li></ul>	<div>Clasificación</div> <p>En los cables de pares existen dos clasificaciones:</p> <ul style="list-style-type: none"><li>- Por <b>categorías</b> (1-7): Cada categoría especifica unas características eléctricas para el cable (atenuación, capacidad de la línea e impedancia)</li><li>- Por <b>clases</b> (A-F):Cada clase especifica la distancia permitida, el ancho de banda conseguido y las aplicaciones para las que es útil</li></ul>	<div>Crimpado y conectores</div> <ul style="list-style-type: none"><li>- En LAN sobre cables UTP se usan <b>conectores RJ45</b>.</li><li>- Estos cables se construyen de acuerdo con la <b>norma T568A o T568B</b></li><li>- <b>Norma T568B:</b><ul style="list-style-type: none"><li>- Cable <b>normal</b> o recto:<table><tr><th>conector1</th><th>conector2</th></tr><tr><td>BN</td><td>BN</td></tr><tr><td>N</td><td>N</td></tr><tr><td>BV</td><td>BV</td></tr><tr><td>A</td><td>A</td></tr><tr><td>BA</td><td>BA</td></tr><tr><td>V</td><td>V</td></tr><tr><td>BM</td><td>BM</td></tr><tr><td>M</td><td>M</td></tr></table><p>conec 1      conec 2</p></li><li>- Cable <b>crucado</b>: usado para conectar directamente 2 ordenadores por sus tarjetas de red (sin ningún dispositivo intermedio)<table><tr><th>conector1</th><th>conector2</th></tr><tr><td>BN</td><td>BV</td></tr><tr><td>N</td><td>V</td></tr><tr><td>BV</td><td>BN</td></tr><tr><td>A</td><td>A</td></tr><tr><td>BA</td><td>BA</td></tr><tr><td>V</td><td>N</td></tr><tr><td>BM</td><td>BM</td></tr><tr><td>M</td><td>M</td></tr></table><p>conec 1      conec 2</p></li></ul></li></ul>	conector1	conector2	BN	BN	N	N	BV	BV	A	A	BA	BA	V	V	BM	BM	M	M	conector1	conector2	BN	BV	N	V	BV	BN	A	A	BA	BA	V	N	BM	BM	M	M	<div>Ejemplos</div> <p>Actualmente, lo más frecuente es instalar:</p> <ul style="list-style-type: none"><li>- Categoría <b>5e</b>: usado en Fast Ethernet (100Mbps) y Gigabit Ethernet (1Gbps)</li><li>- Categoría <b>6</b>: usado en Gigabit Ethernet (1Gbps)</li></ul> <p>Se usan por su bajo precio y facilidad de instalación en redes de área local (<b>LAN</b>) con topología en estrella y una <b>longitud máxima</b> por segmento de <b>100m</b>.</p>
	conector1	conector2																																									
BN	BN																																										
N	N																																										
BV	BV																																										
A	A																																										
BA	BA																																										
V	V																																										
BM	BM																																										
M	M																																										
conector1	conector2																																										
BN	BV																																										
N	V																																										
BV	BN																																										
A	A																																										
BA	BA																																										
V	N																																										
BM	BM																																										
M	M																																										

### Estructura

Se necesitan, al menos, 2 dispositivos PLC:

- Un PLC que actúa como transmisor: se conecta al router/switch mediante un cable de red y a un enchufe de corriente cercano.
- El segundo y demás PLC que actúan como receptores: se conectan con un cable de red a los ordenadores y a la toma de corriente.



### Ventajas

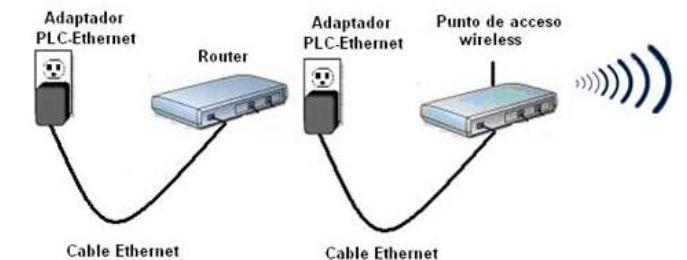
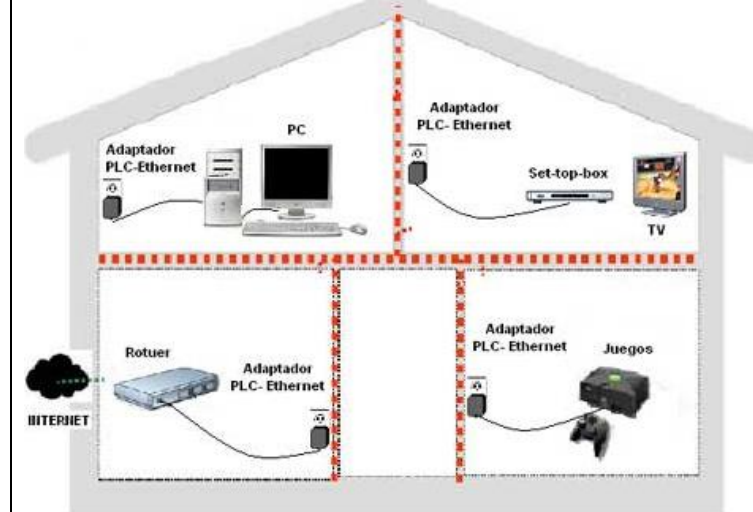
- Utiliza el cableado eléctrico (transmite señales de radio), por lo que podemos conectarnos a la red desde cualquier enchufe de la casa
- Precio asequible
- Alta velocidad
- Fácil conexión

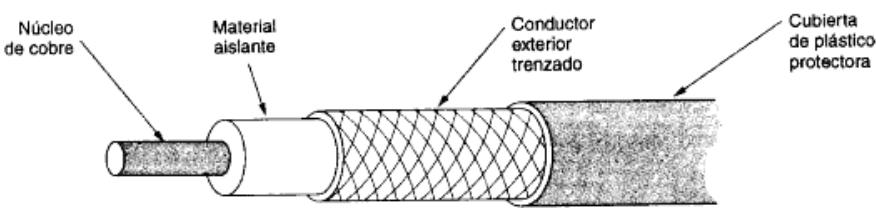
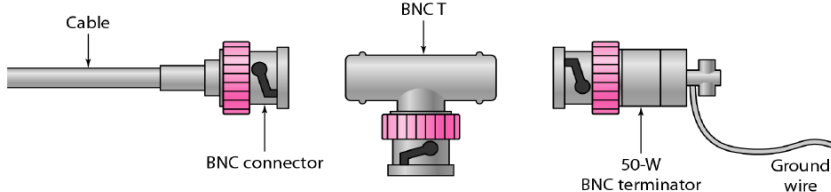
### Inconvenientes

- Genera a su alrededor unas ondas electromagnéticas que pueden interferir en las frecuencias de otra ondas de radio

### Ejemplos

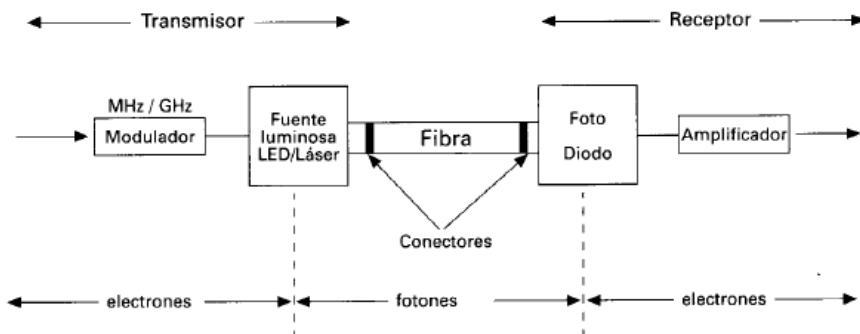
Se usa sobre todo en entornos domésticos:



	Estructura	Ventajas	Inconvenientes	Tipos y ejemplos
coaxial	<div><p>Alambre de metal (cobre) rodeado de material aislante, que a su vez lo rodea por un conductor cilíndrico (malla trenzada). El conjunto se envuelve por una cubierta de plástico protectora.</p><p><b>Conectores BNC usados:</b></p><div><p>Cable BNC connector BNC T 50-W BNC terminator Ground wire</p></div></div>	<ul style="list-style-type: none"><li>- Gran inmunidad frente a interferencias electromagnéticas</li><li>- Fácil de instalar</li><li>- Bastante flexible</li></ul>	<ul style="list-style-type: none"><li>- Más caro que el par trenzado</li></ul>	<p>Hay dos variantes:</p> <ul style="list-style-type: none"><li>- <b>Banda base</b> (<math>50\ \Omega</math>) para transmisiones <b>digitales</b>. Podemos distinguir:<ul style="list-style-type: none"><li>o Coaxial <b>fino</b> (10 Base 2): típico Ethernet, usa <b>conector BNC</b>, <b>longitud máxima de cable de 185m</b>, hasta <b>10Mbps</b></li><li>o Coaxial <b>grueso</b> (10 base 5): longitud máxima de cable de 500m y hasta 10Mbps</li></ul></li><li>- Banda <b>ancha</b> (<math>75\ \Omega</math>) para transmisiones <b>analógicas</b> (TV por cable)</li></ul> <p>Nota: El ohmio u ohm (símbolo <math>\Omega</math>) es una unidad que hace referencia a la resistencia eléctrica de un conductor</p>

## Estructura

Los **sistemas de fibra óptica** se componen de:



- Transmisor de fuente luminosa (el que emite la luz): puede ser un LED o Láser
- Medio de transmisión: la fibra óptica
- Detector de luz: foto diodo

En este sistema, un pulso de luz indica un 1 y la ausencia de luz un 0

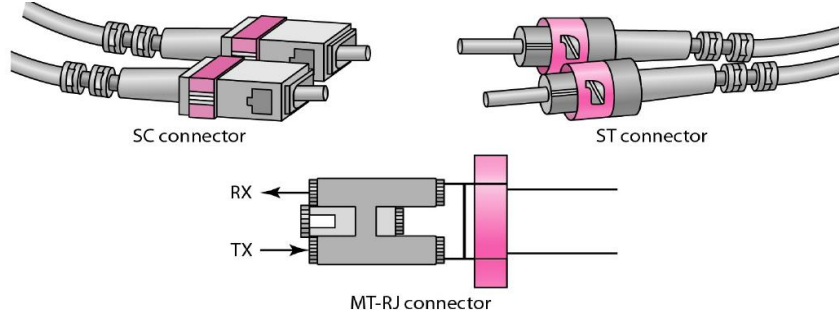
Concretamente, la **fibra** consta de:

- Núcleo conductor de la señal luminosa
- Revestimiento
- Cubierta externa protectora



El índice de refracción del núcleo y el revestimiento son distintos, lo que impide que se escapen los rayos luminosos.

**Conectores** usados:



## Ventajas

- Gran ancho de banda
- Inmunidad electromagnética
- Pérdidas por atenuación muy pequeñas
- Gran fiabilidad
- Ligeras
- Longitud máxima del cable: 2Km

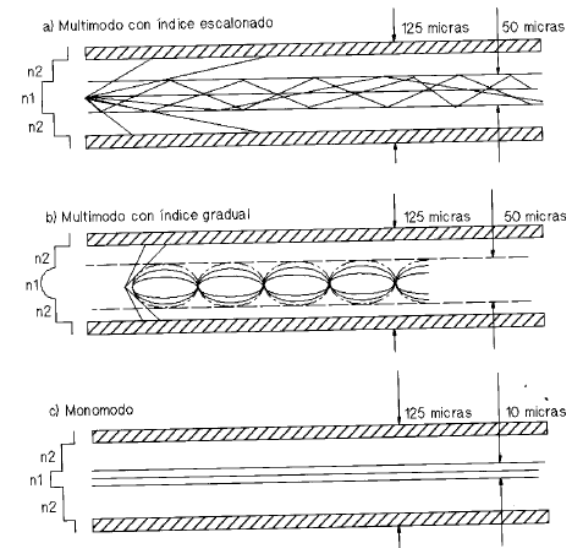
## Inconvenientes

- Difícil manejo y conexionado (difícil de instalar)
- No es flexible
- Más caro que el cable de pares

## Tipos y ejemplos

Actualmente, se utilizan 3 tipos de fibras ópticas para la transmisión de datos:

- Multimodo de índice escalonado: conexiones a otros dispositivos más sencillas.
- Multimodo de índice gradual: esta fibra varía de densidad y tal variación reduce la dispersión de las señales. Tiene un índice de transmisión muy alto.
- Monomodo: diámetro del núcleo muy fino, alto rendimiento, difícil manejo.





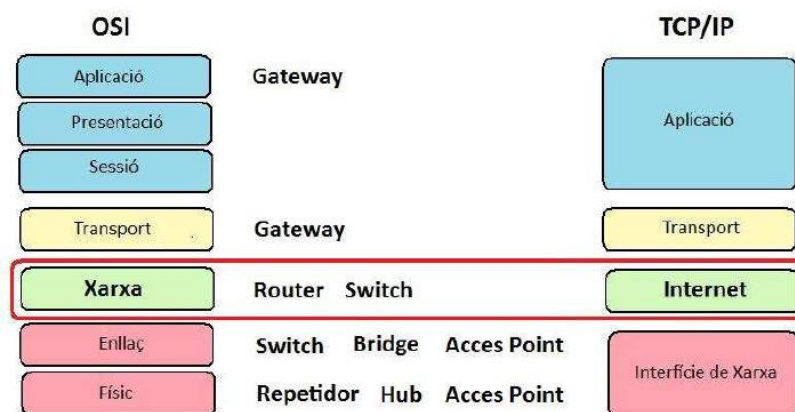
### 2.2.2. Medios no guiados

En el caso de los medios no guiados el envío y recepción de información se hace por el aire a través de antenas, las cuales pueden ser direccionales (requieren alineamiento de emisor y receptor) u omnidireccionales (la señal se expande en todas direcciones).

Tipos:

- **Ondas de radio:**
  - Utilizan las ondas electromagnéticas para transmitir la información.
  - Sistema muy utilizado
  - Inconvenientes:
    - sufren interferencias producidas por la saturación del espectro electromagnético
  - Destacan:
    - Bluetooth: alcanza unos 10m. Es muy usado en telefonía móvil
    - **Wifi**: alcanza unos 100m. Le cuesta atravesar paredes
    - Ambos, en general, usan la banda de 2,4Ghz
- **Infrarrojos (IrDA):**
  - Se utiliza en comunicación de datos a corta distancia.
  - Se basan en la modulación de la señal infrarroja
  - Inconvenientes:
    - Requieren alineación de emisor y receptor
    - No puede atravesar paredes
  - Ventaja:
    - Gran resistencia a las perturbaciones electromagnéticas
- **Microondas terrestres:**
  - Usada en comunicaciones a grandes distancias
  - A mayor frecuencia, mayor velocidad de transmisión
  - Inconvenientes:
    - Requiere alineamiento de antenas
    - Alta sensibilidad a fenómenos meteorológicos
- **Microondas por satélite geoestacionario:**
  - Requiere un satélite en órbita geoestacionaria (retransmite la señal recibida)
  - Inconveniente:
    - retardo de transmisión notable

## 2.3. DISPOSITIVOS DE INTERCONEXIÓN



### 2.3.1. Repetidor

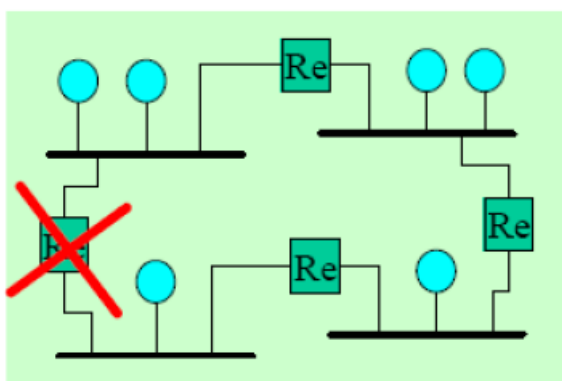
Los repetidores operan en el Nivel 1 (Físico) de OSI, ya que trabajan con señales, a nivel de bits.



Regeneran la señal eléctrica que le llega, con el fin de restituir su nivel original y evitar así los problemas de limitación de distancias por atenuación. Por tanto, permiten alargar distancias máximas de cableado de una red.

Ventaja: se trata de un dispositivo muy sencillo que simplemente copia bits de un segmento de red a otro (sin ningún tipo de configuración).

Desventaja: no aísla de los problemas del tráfico generados en la red en cada uno de los segmentos de la red, por lo que si en un segmento se produce una colisión, ésta se propagará por todos los segmentos de la red.

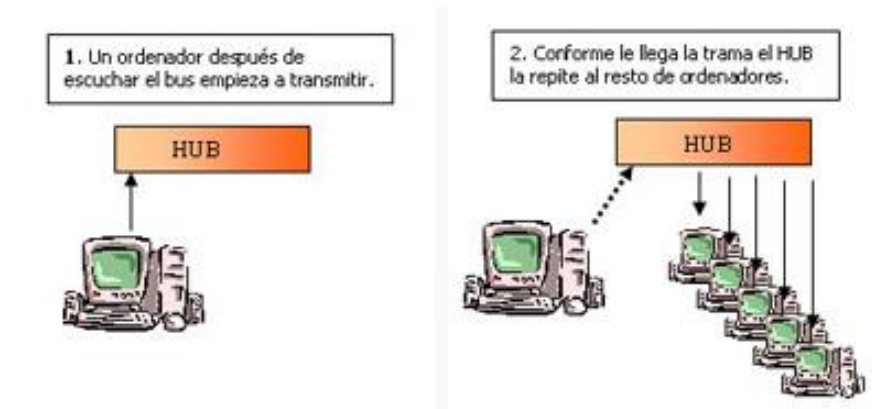


Si intentan transmitir dos equipos a la vez, se produce una colisión y tienen que volver a enviar.

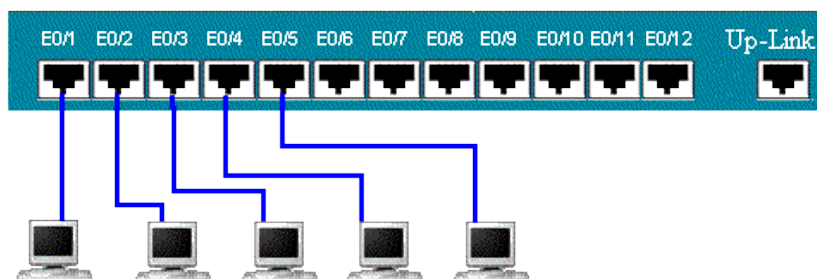
Es por ello que al poner repetidores no debemos hacer "bucles" porque al producirse una colisión, ésta no dejará de propagarse.

### 2.3.2. Hub

Se trata de un repetidor multipuerto que permite comunicar diferentes equipos.



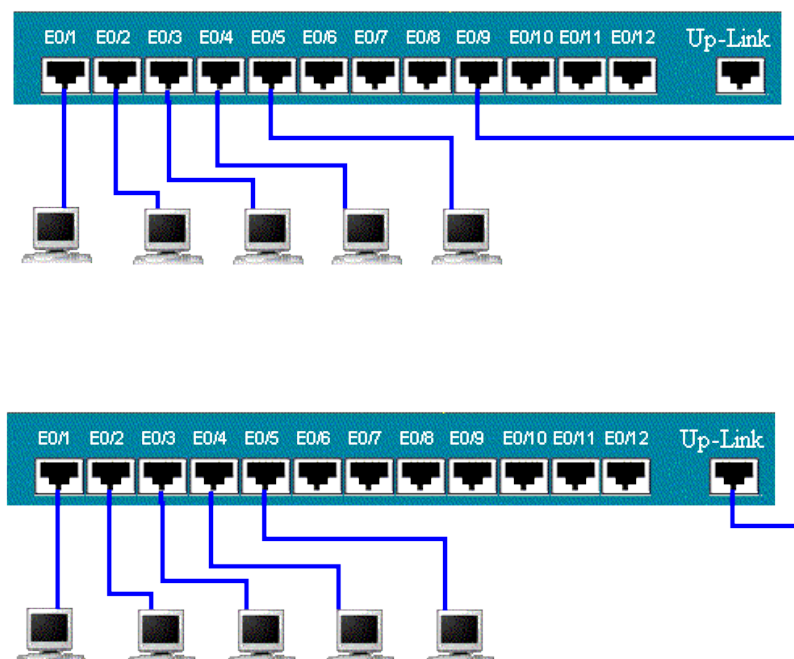
Estos equipos conectados serán miembros del mismo segmento y compiten por el mismo medio, de modo que el ancho de banda es compartido por todos sus puertos de manera que solo una estación puede transmitir de un puerto al resto en cada instante, es decir, envía uno cada vez.



Los cables que van de los ordenadores al Hub son cables de red normales o rectos.

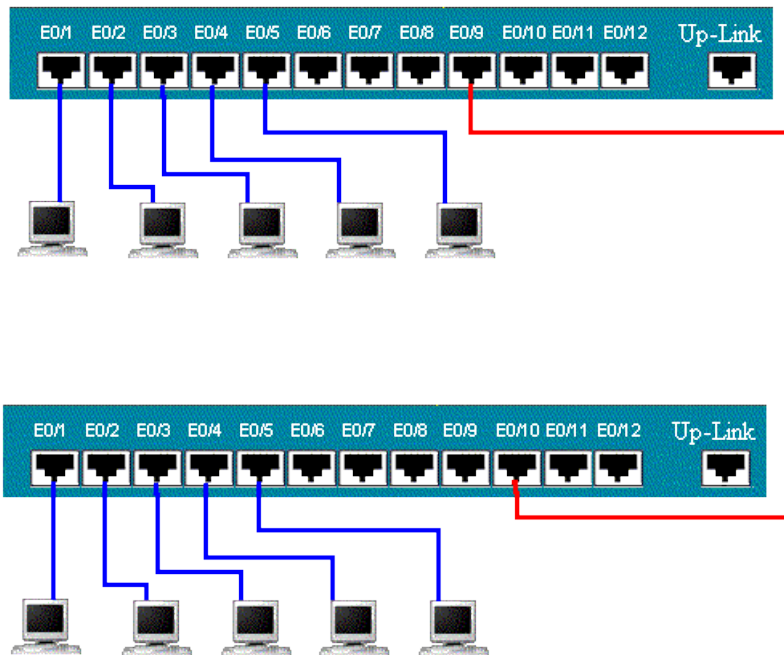
Cuando conectamos dos Hub entre sí, podemos hacerlo de dos formas:

- Forma A:



Conexión de dos Hub mediante cable de red normal o recto.

- Forma B:

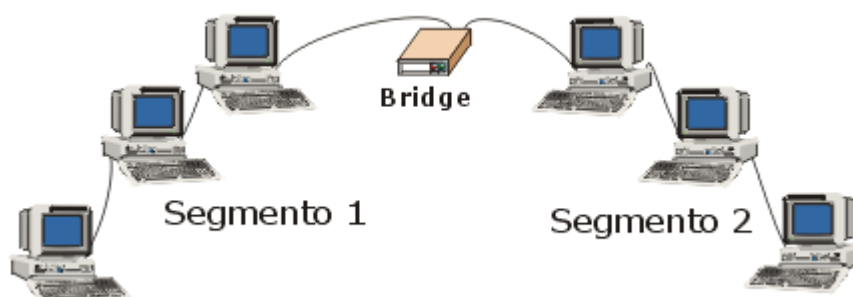


Conexión de dos Hub mediante cable de red cruzado.

### 2.3.3. Puente

- Opera en el nivel 2 (enlace) de OSI, ya que trabaja con tramas (tiene en cuenta la dirección MAC).
- Son un poco más inteligentes.
- Ventaja:
  - Divide la red en dominios de colisión: aísla el tráfico en cada segmento de red. De este modo, la reducción de la carga del tráfico se reduce al impedir que las tramas de un segmento pasen a otros segmentos cuando no esté allí su destinatario.
- Tipos:
  - Transparente: no requiere ninguna configuración para su funcionamiento
  - No transparente: necesitan que la trama lleve información sobre el modo en que va a ser reexpedida. Tienen un mejor rendimiento, pero su compatibilidad en la conexión de redes es menor.

Por otro lado, en función de si las redes a conectar están próximas o no, tenemos puentes locales o remotos.

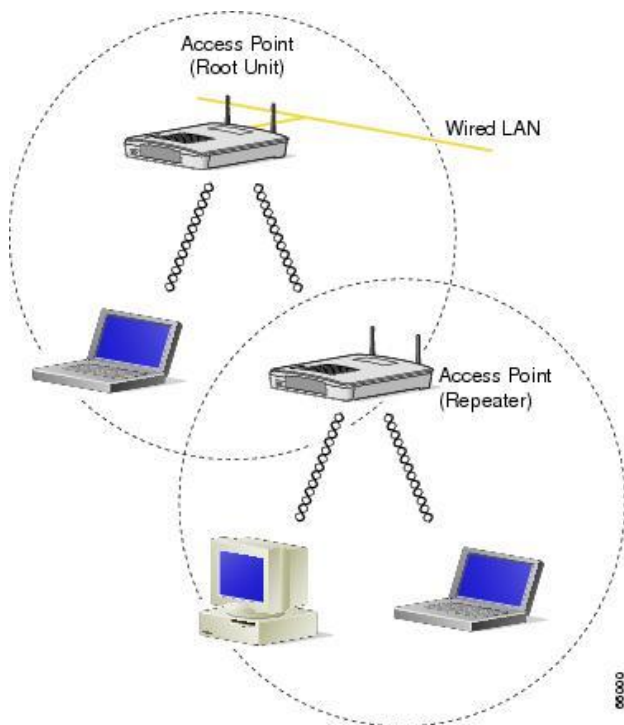


#### 2.3.4. Access Point (punto de acceso)

- Conectan diferentes dispositivos inalámbricos formando una red inalámbrica.
- Se pueden configurar de varias maneras:
  - Como repetidor de la señal para que llegue más lejos
  - Como “hub” para conectar equipos inalámbricos
  - Como punto (LAN + WIFI) haciendo de enlace entre una red inalámbrica y otra cableada



En este caso, la tecnología a nivel de enlace de la red de cable y la red inalámbrica es diferente y el punto de acceso permite que se puedan comunicar entre ellos.



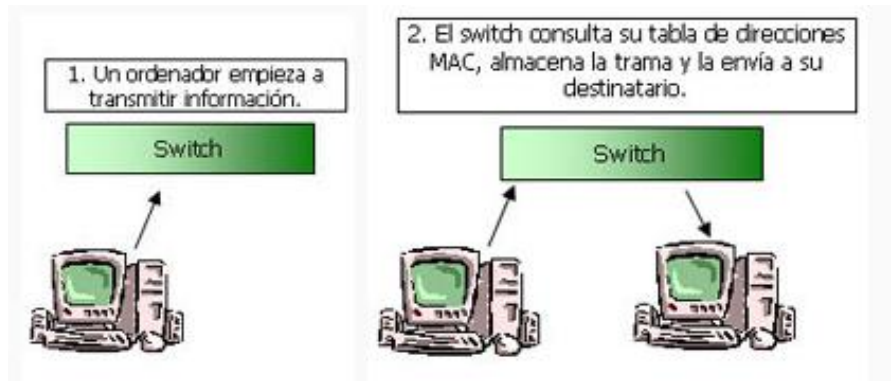
En este caso, el segundo Access Point actúa como repetidor de la señal del primero (y a su vez como hub porque conecta equipos inalámbricos)

### 2.3.5. Switch

Opera en el nivel 2 (enlace) de OSI. Tiene en cuenta las direcciones MAC por lo que es similar al puente.

Características:

- Siempre es local
- Si velocidad de operación es mayor que la del puente
- Filtran y dirigen tramas entre los segmentos de la LAN proporcionando un ancho de banda dedicado (emisor y receptor disponen de todo el ancho de banda durante la transmisión)
- Se pueden apilar y conectar en cascada (que es lo que se hace en el cableado estructurado)



También hay switches de nivel 3. Se usan para crear redes VLAN (conmutadores compatibles con 802.1Q o VLAN Tagging). Una VLAN es una agrupación lógica de nodos de un red que no depende de su ubicación física (evitamos el condicionamiento de la ubicación física).

### 2.3.6. Router

Opera en el nivel 3 de OSI (red). Trabaja con direcciones IP.

Son dispositivos que permiten encaminar paquetes entre sus puertos utilizando la dirección IP.

Permiten unir redes con nivel de enlace de datos (LLC) diferente, por lo que permite conectar LAN con WAN (Internet)

Respecto a su funcionamiento interno, el router sigue una tabla de encaminamiento, en la que se registra qué redes son alcanzables por cada uno de sus puertos. En función de la tabla de encaminamiento, reenvía la información.

Proporciona seguridad (mediante filtrado) y reducen la congestión de la red aislando el tráfico y los dominios de colisión en las distintas subredes que interconecta.

Para realizar su función puede utilizar algoritmos de encaminamiento:

- Estático: requieren que la tabla de encaminamiento sea programada por el administrador de red,
- Adaptativo: capaces de aprender por sí mismos, y por tanto, más flexibles

Respecto a los protocolos de encaminamiento que puede seguir, encontramos:

- RIP: apropiado para encaminamiento en redes pequeñas. Tiene en cuenta el número de saltos de red necesarios para que un paquete dado alcance su destino.
- OSPF: el envío del paquete se realiza por la ruta más corta.
- BGP: protocolo frontera exterior que se ejecuta en los encaminadores que forman el perímetro de la red. Facilitan el intercambio de rutas con los encaminadores exteriores.

En Windows, para gestionar la tabla de rutas se usa la orden "route" y en Linux "iptables" o "ip route".



### 3. COMPONENTES SOFTWARE

#### 3.1. DRIVER DE LA NIC (TARJETA DE RED)

Se trata del software facilitado por el fabricante de las tarjetas de red que hace que el Sistema Operativo pueda comunicarse con la tarjeta de red.

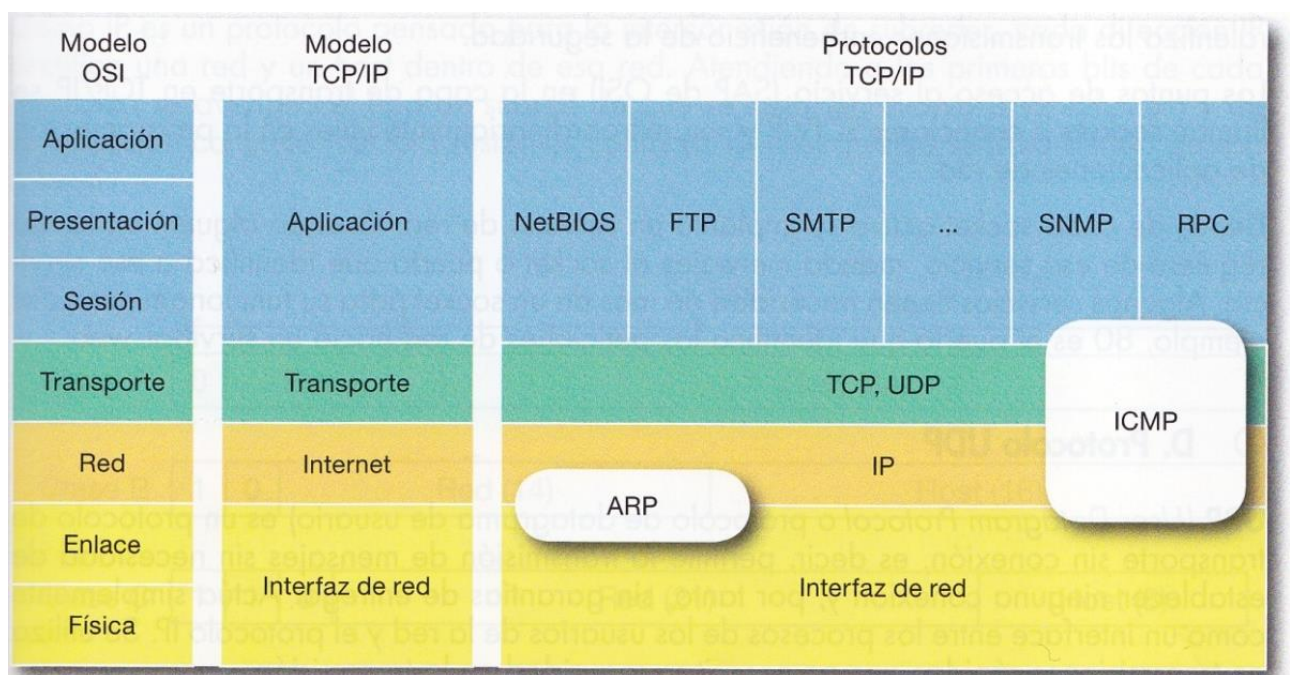
Permite que el equipo pueda utilizar el medio físico (por ejemplo, cable de pares) para la transmisión de información por la red a la que está conectado.

#### 3.2. PROTOCOLOS DE COMUNICACIÓN

En el SO se instalan los protocolos de comunicación necesarios para permitir la comunicación entre equipos a través de internet. Este conjunto de protocolos son usados directamente por el núcleo del SO y por los servicios de red instalados.

Las familias de protocolos más comunes son: TCP/IP, IPX/SPX, Apple Talk y Netbeui.

##### 3.2.1. La familia de protocolos TCP/IP. Direcciones IP. Clases de IP. Subnetting



Podríamos definir **protocolo** como un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red.

En cada capa del modelo TCP/IP encontramos una serie de protocolos. A continuación se describe los más importantes:

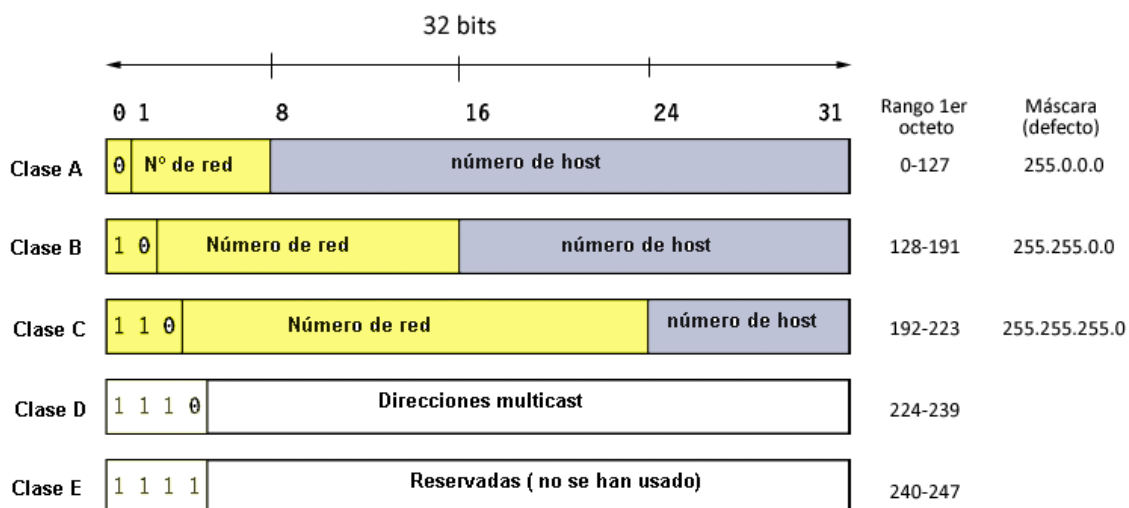
- Protocolo **ARP**: permite averiguar la dirección física (MAC) a partir de la dirección lógica (IP) indicada.
- Protocolo **ICMP**: es el protocolo de mensajes de control entre redes. Expresa eventos que se producen en la red, es decir, se usa para informarnos del estado de la red y saber cómo va todo. Es un protocolo de supervisión.

- Protocolo **IP**: sirve para hacer el encaminamiento. Nos da un servicio sin conexión, es decir, no tenemos garantía de que llegue (de esto ya se encargará TCP).

Este protocolo proporciona un sistema de direcciones para que cada nodo de la red quede identificado por una dirección de 4 números enteros (del 0 al 255) separados por puntos (32 bits binarios en 4 grupos de 8 bits) denominada **dirección IP**.

Una parte de la dirección IP identifica la red y la otra parte sirve para identificar cada host de la red/subred. La **clase** de IP determinará la cantidad de redes posibles de esa clase y el tamaño de las mismas.

**Clases:**



Clase A:

**Formato**

7 bits	24 bits
0	Red Estación

**Características**

- Ejemplo: 112.34.24.230. Identifica una estación dentro de la red 112.
- Sólo puede haber 126 (la 0 y la 127 están reservadas).
- Cada red A admite  $2^{24}=16$  millones de estaciones.
- Organizaciones como IBM, Univ Columbia, DEC, tienen esta clase de redes.

Clase B:

**Formato**

14 bits	16 bits
1 0	Red Estación

**Características**

- Ejemplo: 150.244.28.230. Identifica una estación dentro de la red 150.244.
- Pueden existir  $2^{14}=16$  mil redes de esta clase.
- Cada red B admite  $2^{16}=65536$  estaciones.
- Utilizadas por organizaciones de tipo medio.

Clase C:

**Formato**

21 bits	8 bits
1 1 0	Red Estación

**Características**

- Ejemplo: 200.10.46.90. Identifica una estación dentro de la red 200.10.46
- Pueden existir  $2^{21}=2$  millones de redes de esta clase.
- Cada red C admite  $2^8=256$  estaciones.
- Utilizadas por organizaciones de tipo pequeño.



## Direcciones IP especiales:

- **127.x.x.x** → Dirección de **loopback** (mi propio host)
- Parte de **host** todo **0's** → estamos indicando **la propia red**
- Parte de **host** todo **1's** → estamos indicando la dirección de **broadcast** (para enviar a todas las máquinas de la propia red)

## Direcciones IP públicas y privadas:

- IP **pública**: son visibles en todo internet, es decir, un ordenador con una IP pública es accesible desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener acceso a una IP pública.
- IP **privada**: son visibles únicamente por otros hosts de su propia red. Se usan en las empresas para los lugares de trabajo. Los ordenadores que tienen IPs privadas pueden salir a Internet mediante un router que tenga una dirección IP pública.

Se han reservado los siguientes tres bloques de direcciones IP para redes privadas:

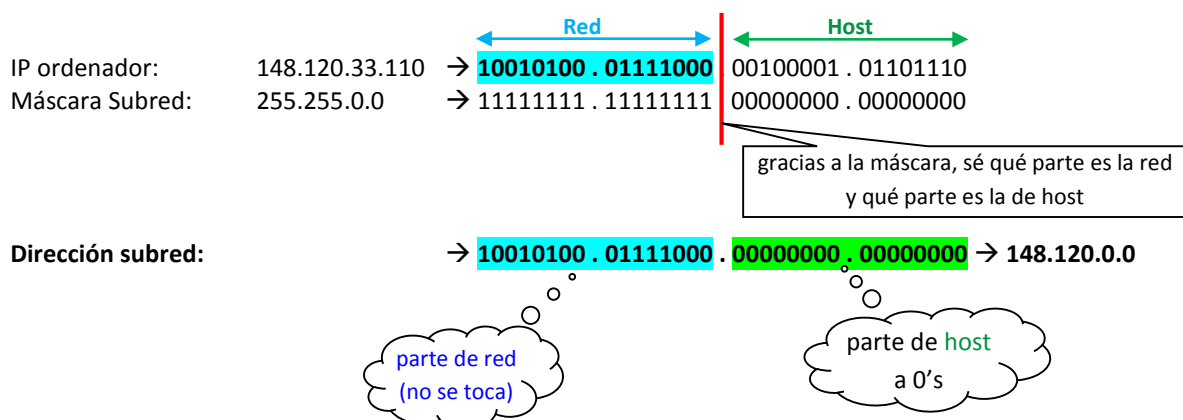
- **10.0.0.0-10.255.255.255** → direcciones IP privadas de clase A
- **172.16.0.0-172.31.255.255** → direcciones IP privadas de clase B
- **192.168.0.0-192.168.255.255** → direcciones IP privadas de clase C

## Máscara:

- En una red de redes TCP/IP no puede haber hosts aislados. Todos pertenecen a alguna red y todos tienen una dirección IP y una **máscara de subred** (si no se especifica se toma la máscara que corresponda a su clase).
- Por medio de esta máscara un ordenador sabe si otro ordenador se encuentra en la misma subred o en otra distinta.
- Las **máscaras por defecto** de clase A, B y C son respectivamente 255.0.0.0, 255.255.0.0 y 255.255.255.0
- Aquellos **bits de la máscara** de red puestos a **0** indican la parte de la dirección que identifica la **estación o host**. Los puestos a **1** identifican la **red**.
- La máscara también se suele representar por el **número de bits a uno**. Por ejemplo de: 255.255.255.0 es /24

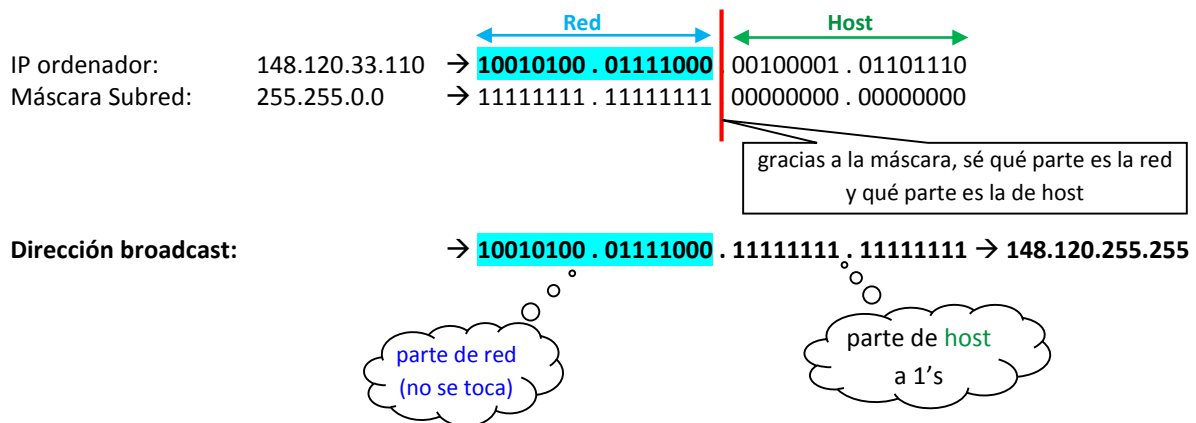
### Ejemplo 1. Cálculo de direcciones de red:

Suponemos una subred con máscara 255.255.0.0, en la que tenemos un ordenador con dirección IP 148.120.33.110. A continuación, indicamos cómo obtener la dirección de la red/subred a la que pertenece ese ordenador:



### Ejemplo 2. Cálculo de direcciones de broadcast:

Suponemos una subred con máscara 255.255.0.0, en la que tenemos un ordenador con dirección IP 148.120.33.110. A continuación, indicamos cómo obtener la dirección de **broadcast**:



### Subnetting:

- Consiste en la división de una red en subredes.
- Lo conseguimos “robando” bits a la parte de host.
- Para calcular el número de **bits** necesarios para representar **subredes** aplicamos la fórmula:  
 $2^{\text{bits robados de la parte de host}} \geq \text{número de subredes}$
- Para calcular el número de **hosts máximo** aplicamos la fórmula:  
 $2^{\text{bits restantes en la parte de host}} - 2 \geq \text{número de hosts posibles}$

### Ejemplo 3. Subnetting:

Nos dan la dirección de red Clase C 192.168.1.0 /24 para realizar mediante subneteo 4 subredes con un mínimo de 50 hosts por subred.

Pasos:

#### a) Adaptar la Máscara de Red por Defecto a Nuestras Subredes

La máscara por defecto para la red 192.168.1.0 es:

Porción de Red			Porción de Host	
255	.	255	.	0
11111111	.	11111111	.	00000000

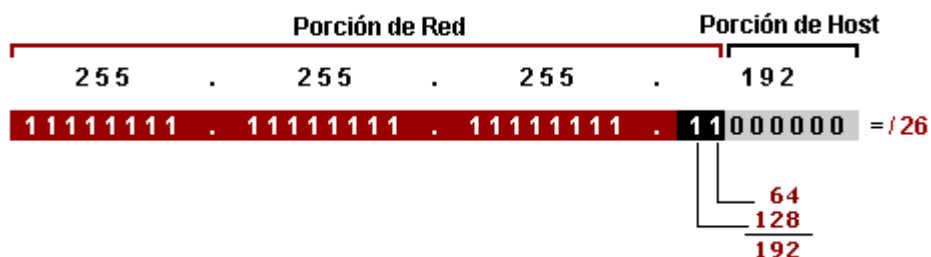
= / 24

Usando la fórmula  $2^N$ , donde **N** es la cantidad de bits que tenemos que robarle a la porción de host, adaptamos la máscara de red por defecto a la subred.

Se nos solicitaron 4 subredes, es decir que el resultado de  $2^N$  tiene que ser mayor o igual a 4.

$2^N$	Redes	Máscara Binario	Máscara Decimal
$2^1$	2	11111111 . 11111111 . 11111111 . 10000000	255 . 255 . 255 . 128
$2^2$	4	11111111 . 11111111 . 11111111 . 11000000	255 . 255 . 255 . 192
$2^3$	8	11111111 . 11111111 . 11111111 . 11100000	255 . 255 . 255 . 224
$2^4$	16	11111111 . 11111111 . 11111111 . 11110000	255 . 255 . 255 . 240
$2^5$	32	11111111 . 11111111 . 11111111 . 11111000	255 . 255 . 255 . 248
$2^6$	64	11111111 . 11111111 . 11111111 . 11111100	255 . 255 . 255 . 252

Como vemos en el gráfico, para hacer 4 subredes debemos robar 2 bits a la porción de host. Agregamos los 2 bits robados reemplazándolos por "1" a la máscara Clase C por defecto y obtenemos la máscara adaptada 255.255.255.192.



## b) Obtener Cantidad de Hosts por Subred

Ya tenemos nuestra máscara de red adaptada que va a ser común a todas las subredes y hosts que componen la red. Ahora queda obtener los hosts. Para esto vamos a trabajar con la dirección IP de red, específicamente con la porción de host (fondo gris).



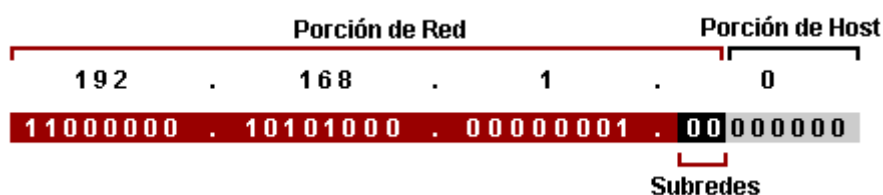
El ejercicio nos pedía un mínimo de 50 hosts por subred. Para esto utilizamos la fórmula  $2^M - 2$ , donde  $M$  es el número de bits "0" disponibles en la porción de host y  $- 2$  porque la primer y última dirección IP de la subred no se utilizan por ser la dirección de la subred y broadcast respectivamente.

$$2^6 - 2 = 62 \text{ hosts por subred.}$$

Los 6 bits "0" de la porción de host (fondo gris) son los vamos a utilizar según vayamos asignando los hosts a las subredes.

## c) Obtener Rango de Subredes

Para obtener el rango subredes utilizamos la porción de red de la dirección IP que fue modificada al adaptar la máscara de red. A la máscara de red se le agregaron 2 bits en el cuarto octeto, entonces van a tener que modificar esos mismos bits pero en la dirección IP (fondo negro).



Los 2 bits "0" de la porción de red (fondo negro) son los que más adelante modificaremos según vayamos asignando las subredes.

Para obtener el rango la forma más sencilla es restarle a 256 el número de la máscara de subred adaptada. En este caso sería:  $256 - 192 = 64$ , entonces 64 va a ser el rango entre cada subred.

N° de Subred	Rango IP *		Hosts Asignables x Subred
	Desde	Hasta	
1	192.168.1.0	192.168.1.63	62
2	192.168.1.64	192.168.1.127	62
3	192.168.1.128	192.168.1.191	62
4	192.168.1.192	192.168.1.255	62

\* La primera y la última dirección IP de cada Subred no se asignan ya que contienen la dirección de red y broadcast de la Subred.

- Protocolo **TCP**: protocolo encargado de la gestión de errores durante el envío de un paquete de información. Proporciona seguridad en la entrega, ya que es el responsable de ensamblar datagramas IP, de modo que si hay algún problema con alguno de ellos, solicita su retransmisión.

Los puntos de acceso a un servicio en la capa de transporte en TCP/IP se llaman **sockets o conectores TCP/IP (dirección IP + puerto)**. Detrás de cada socket activo se implanta un **servicio de red**, de modo que cuando alguien en la red requiere de este servicio, manda mensajes al socket o puerto que identifica a ese servicio. Por ejemplo, 80 es el puerto que identifica las peticiones de red hacia un servidor web. Para este caso, un ejemplo de socket sería: 192.168.0.32:80

- Protocolo **UDP**: protocolo de transporte sin conexión, es decir, permite la transmisión de mensajes sin necesidad de establecer ninguna conexión y, por tanto, sin garantías de entrega. Se usa para transmisiones rápidas que no necesitan seguridad en la transmisión. Por tanto, tiene un mayor rendimiento que TCP, pero también es más inseguro.
- **Protocolos TCP/IP de nivel superior:**
  - **FTP**: protocolo usado para la descarga (bajada) o carga (subida) de ficheros en Internet.
  - **HTTP**: protocolo usado por la web, concretamente, es usado por los navegadores de internet para el acceso a las páginas web.
  - **SNMP**: protocolo usado para la gestión de la red
  - **SMTP**: protocolo para el intercambio de mensajes de correo electrónico entre servidores de correo o el que usa la aplicación cliente de correo para enviar mensajes al servidor al que se conecta.
  - **POP**: protocolo encargado de descargar mensajes de correo desde el servidor de correo en donde se encuentra el buzón o la bandeja de entrada del cliente de correo. La versión actual del protocolo es la 3 (POP3)
  - **IMAP**: protocolo semejante a POP, pero con funcionalidades añadidas que lo hacen recomendable en situaciones de congestión.

La mayor parte de los protocolos de nivel superior tienen asociado uno o más números de **puerto** en sus **sockets** de comunicación, por ejemplo: el 21 y 20 para FTP, HTTP el 80, SMTP el 25, POP el 110.

Servicio	Función	No. De Puerto
<b>MTP</b>	Protocolo de Transferencia Multimedia.	---
<b>FTP</b>	Protocolo de Transferencia de Archivos.	20-21
<b>TELNET</b>	Protocolo cliente/servidor.	23
<b>SMTP</b>	Envío de mensajes de correo electrónico.	25
<b>DNS</b>	Resolución de nombres de dominio.	53
<b>HTTP</b>	Transferencia de hipertexto.	80
<b>POP3</b>	Obtención de mensajes de correo electrónico en clientes locales.	110
<b>IMAP</b>	Acceso a correo electrónico.	143
<b>HTTPS</b>	Transferencia segura de hipertexto.	443
<b>DHCP</b>	Configuración automática de parámetros de red.	67-68
<b>UDP</b>	Intercambio de datagramas a través de una red.	113

### 3.3. SISTEMA OPERATIVO DE RED

Un SO de red es el software que hace que un Sistema Informático pueda comunicarse con otros equipos construyendo una red.

Podemos destacar:

- Grupos de trabajo (peer-to-peer) → Sistemas Operativos cliente. Ej: Windows 7/10/11...
- Dominios (cliente-servidor) → Sistemas Operativos servidor y Sistemas Operativos cliente. Ej: Windows Server

### 3.4. SERVICIOS DE RED:

A continuación, se describe los servicios más clásicos en una red. La mayoría de estos servicios corresponden a la capa de aplicación en TCP/IP.

#### 3.4.1. Directorio

Para centralizar la seguridad de un sistema en red, se usan servicios de directorio, que son aplicaciones software que permiten **organizar, controlar y administrar centralizadamente los usuarios y recursos** de una red.

De este modo, un directorio es una base de datos jerárquica que almacena información sobre los objetos de la red.

Por otro lado, definimos **dominio** como un conjunto de equipos interconectados que comparten información administrativa centralizada (usuarios, grupos, contraseñas...). En este caso, comparten la misma base de datos de directorio. Se identifica unívocamente por un nombre de dominio DNS.

Usando un servicio de directorio se va a centralizar el proceso de autenticación de usuarios y se concede o deniega permisos a los usuarios sobre los recursos de forma centralizada. Por ejemplo, se puede permitir iniciar sesión en determinados equipos del dominio con un determinado horario o denegar la impresión en determinadas impresoras.

En algunas implementaciones, como Active Directory de Windows Server, se pueden usar perfiles móviles, permitiendo que los usuarios tengan sus archivos y configuraciones, sea cual sea el ordenador en el que inicien sesión.

Los servicios de directorio suelen basarse en los estándares DNS, LDAP, Kerberos y Certificados x.509.

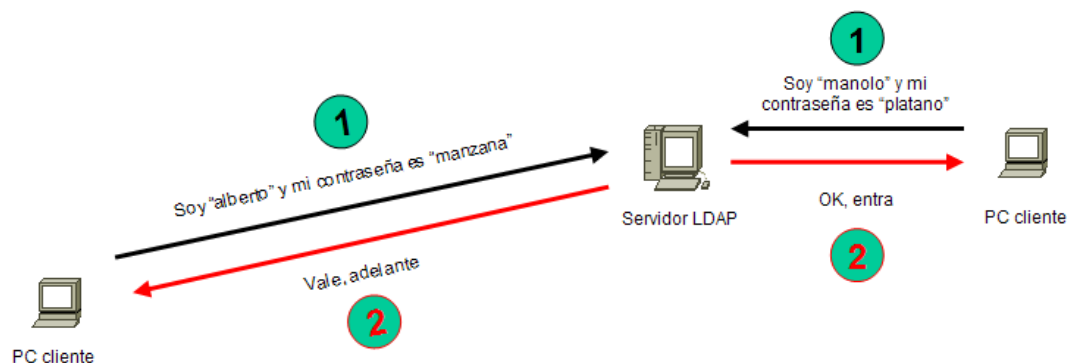
Existen multitud de implementaciones de servicios de directorio. Los más conocidos son: Active Directory de Microsoft, Open LDAP (implementación libre y de código abierto), eDirectory de Novell y Sun Directory Server de Sun.

- **Active Directory:**

- Implementación de Microsoft de servicios de directorio lanzado a la vez que Windows 2000.
- Necesita un Windows Server para convertirlo en DC (controlador de dominio).
- Deberá existir al menos un DC por cada dominio que almacenará las cuentas, grupos, equipos, impresoras, carpetas compartidas, perfiles de usuarios, directivas de seguridad, servicios de red, etc. Si existen varios DC, se replicará la información de unos a otros.
- Requiere la instalación de un servidor DNS (que puede instalarse en el propio DC) que se utilizará para la resolución de nombres y localizar equipos y DC.
- Utiliza los estándares DNS, LDAP, Kerberos y Certificados x.509.

- **Open LDAP:**

- En Linux se consigue un efecto similar a los servicios de directorio usando un servicio que actúe como servidor de cuentas y grupos (openLDAP) y otro que permita la exportación de directorios a maquinas remotas (NFS).
- Open LDAP permite el acceso a la información del directorio mediante un esquema cliente-servidor, donde uno o varios servidores mantienen la misma información de directorio y los clientes realizan consultas a cualquiera de ellos.
- Define una estructura jerárquica de objetos en forma de árbol donde cada objeto posee un conjunto de atributos y viene identificado unívocamente mediante un atributo especial llamado nombre distinguido o DN.



### 3.4.2. Recursos compartidos

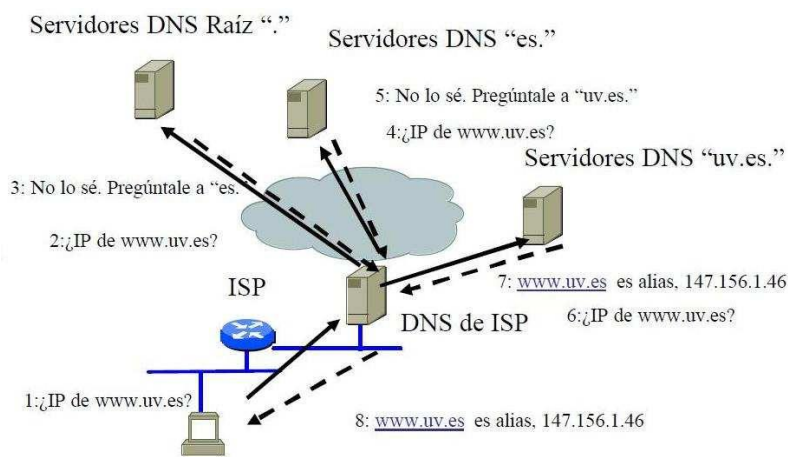
Se trata de servicios ofrecidos a los usuarios por uno o más servidores. El usuario que los usa los ve como local, usándolos de modo transparente:

- **Almacenamiento:**
  - En el caso de servidores, interesan interfaces rápidas como discos SCSI (Ultra/Wide SCSI)
  - En las estaciones cliente de trabajo, basta con interfaces IDE o SATA.
  - Fibre Channel: para conexión de discos con unas velocidades extremas. Es usada en la creación de redes SAN (redes de área de almacenamiento)
- **Impresión:**
  - Los servidores de impresión gestionan todas las tareas de impresión ajustando sus parámetros: velocidad o calidad de impresión, privilegios, prioridades, costes, etc.
  - De este modo, si el sistema de impresiones está centralizado en los servidores, el administrador tienen mayor control sobre los recursos de impresión, ya que puede controlar las impresoras remotas, las colas de impresión, etc.
- **Servidores de aplicaciones y bases de datos**

### 3.4.3. DNS

Se basa en un esquema jerárquico de nombrado de nodos de la red basado en el concepto de dominio (esquema cliente-servidor) que permite a los usuarios de una red TCP/IP usar nombres descriptivos para localizar fácilmente ordenadores y otros recursos en la red, evitando tener que recordar las direcciones IP.

Existen varias implementaciones, como el DNS de Windows Server o BIND de Linux.



### 3.4.4. Servidor de archivos (FTP, SMB y NFS)

Su función es permitir el acceso remoto a archivos almacenados en él o accesibles por este. El acceso a los archivos será transparente a los clientes.

Algunos protocolos usados son:

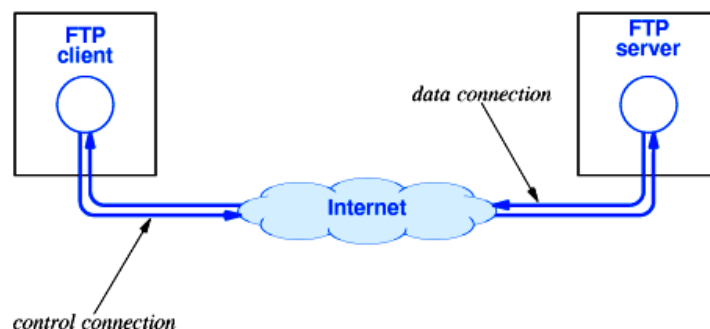
- **FTP** (estándar de Internet):

Proporciona un mecanismo de transferencia de archivos entre sistemas a través de redes TCP/IP. Para utilizarlo hay que disponer de una cuenta en la maquina en la que se quiere cargar o descargar archivos, aunque hay servidores que permiten el uso de una cuenta anónima.

Se trata de un servicio basado en la arquitectura cliente-servidor:

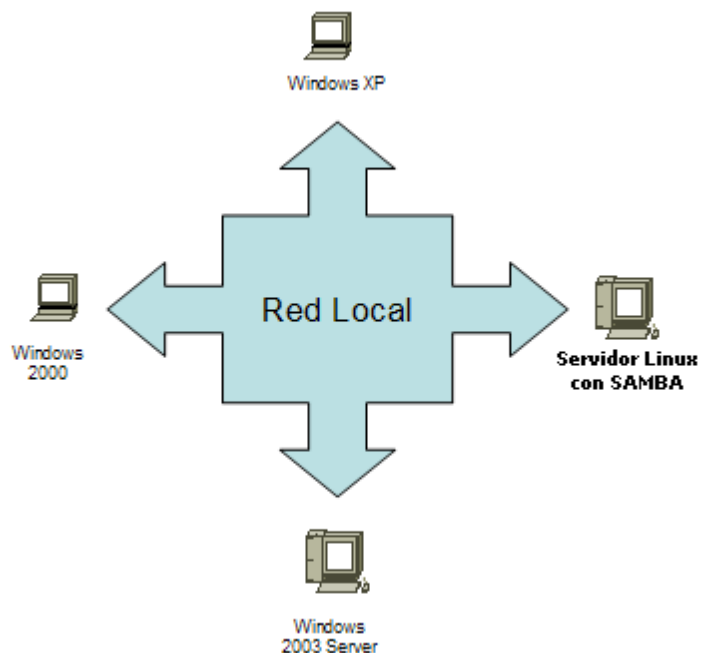
- Hay un servidor FTP que proporciona el servicio y usa 2 puertos:
  - 20: para transferencia de datos
  - 21: para transferencia de la orden de control
- El cliente se conecta al servidor usando un puerto local (origen) y tomando como destino el puerto 21 del servidor. Una vez ya ha establecido la conexión, ya se puede transferir archivos a través del puerto 20.

No proporciona seguridad ya que todo el intercambio de información se realiza sin cifrado. Esto se puede solucionar con aplicaciones como SCP o SFTP, incluidas en el paquete SSH, que permiten transferir ficheros pero cifrando el tráfico.



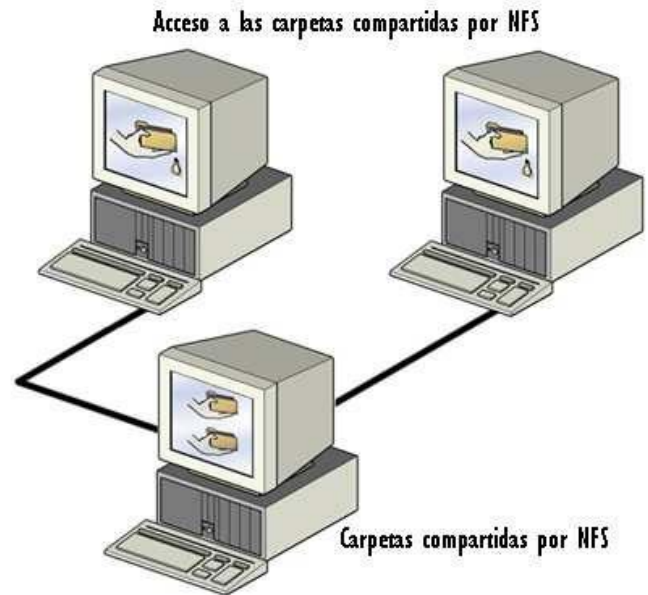
- **SMB** de Microsoft:

Samba son un conjunto de aplicaciones libres para Linux que implementan el protocolo SMB usado por SO para compartir carpetas e impresoras. Permite a PCs que usan Linux conectarse a carpetas compartidas en PCs con Windows y compartir carpetas como si se tratara de un Windows.



- **NFS** en Linux/Unix:

Sistema que usa Linux para compartir y acceder a carpetas compartidas entre sí en una red.



### 3.4.5. Correo electrónico

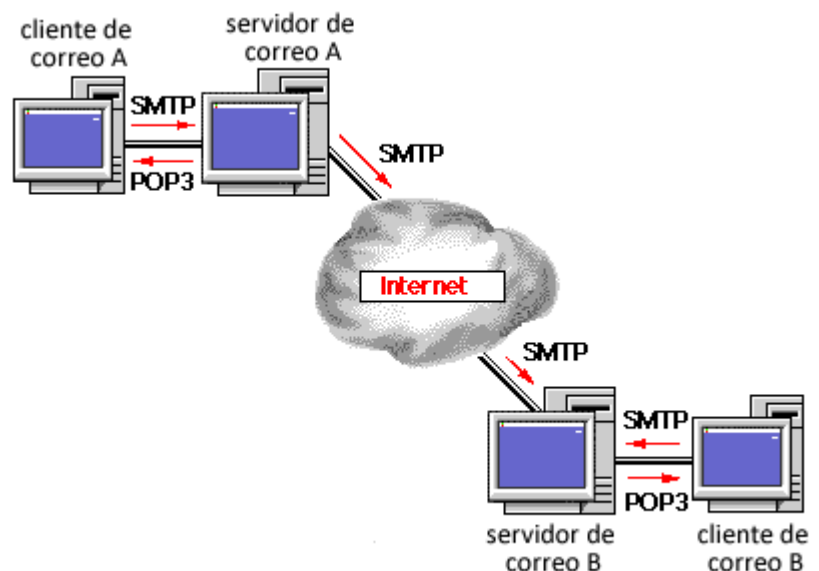
Un servidor de correo permite enviar mensajes de unos usuarios a otros con independencia de la red que estén usando.

Un servidor de correo consta de 2 servidores:

- Servidor **SMTP** encargado de enviar y recibir mensajes
- Servidor **POP/IMAP** que permite a los usuarios obtener sus mensajes

Para lograrlo, se definen una serie de protocolos:

- **SMTP** (simple mail transfer protocol): se utiliza para que dos servidores de correo intercambien mensajes. Su puerto es el 25.
- **POP** (post office protocol): permite al usuario obtener los mensajes guardados en el servidor. Su puerto es el 110.
- **IMAP**: usado también para recogida de correo, pero más potente que el pop. Generalmente, su puerto es el 143.



El estándar MIME permite incluir en el mensaje de correo electrónico cualquier información binaria: voz, vídeo, imagen...

Ejemplos de servidores de correo son Microsoft Exchange Server y Mail Marshall

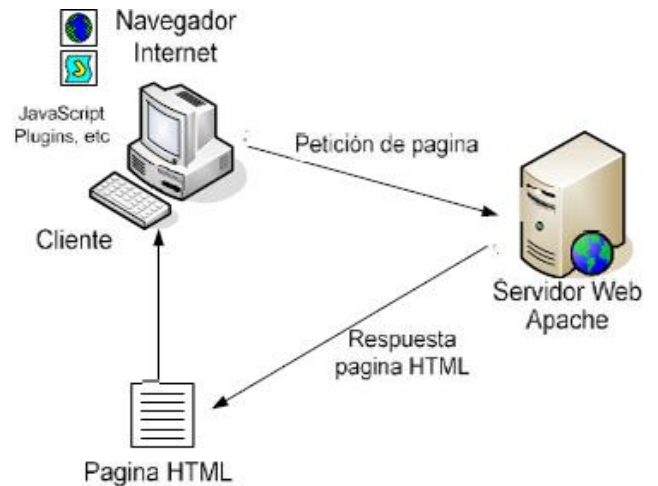


### 3.4.6. Web (HTTP)

Es el método más común de intercambio de información en la world wide web (www) el cual sigue un modelo cliente-servidor mediante el protocolo de transferencia de hipertexto HTTP.

Así, un cliente HTTP (navegador web) establece una conexión TCP con el puerto 80 del servidor y le realiza una petición HTTP. El servidor le responde con el contenido que el cliente solicita (página HTML).

Ejemplos de servidores web son IIS y Apache.

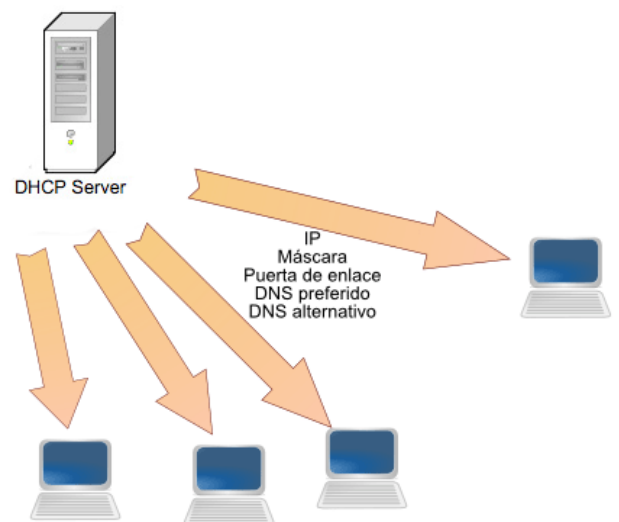


### 3.4.7. DHCP

DHCP es un protocolo de red cliente/servidor que permite a los nodos de una red IP obtener sus parámetros de configuración IP automáticamente (dirección IP, máscara de red, puerta de enlace, servidores DNS).

Funcionamiento: un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes.

Las peticiones se realizan en el puerto UDP 68 y el servidor responde a través del UDP 67.



### 3.4.8. SSH

Servicio semejante al telnet (conexión remota no segura en el puerto 23), ya que permite que un usuario acceda de forma remota a un sistema Linux pero, en el caso de SSH las comunicaciones entre cliente y servidor viajan encriptadas, es decir, SSH ofrece conexión remota de manera segura.

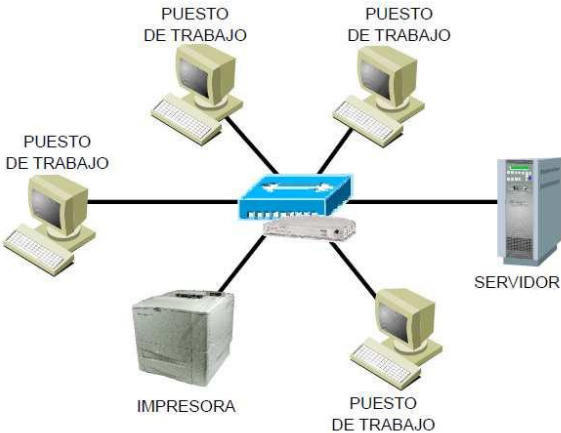
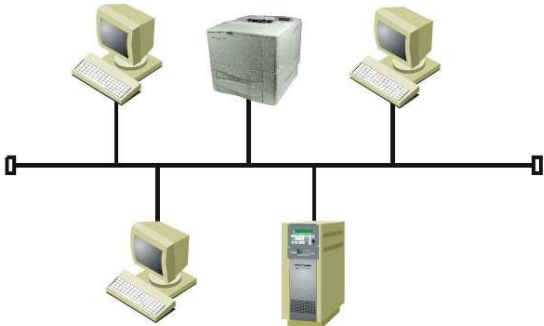
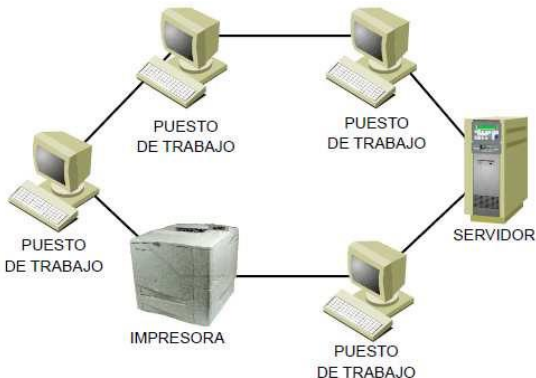
Usa el puerto 22.



## 4. TOPOLOGÍAS EN LANS

La **topología** es la forma en la que están conectados físicamente los distintos elementos (nodos) de una red.

Tipos de topologías usadas en **LANs**:

<ul style="list-style-type: none"><li>- <b>Estrella:</b><ul style="list-style-type: none"><li>○ todos los nodos se conectan a un nodo central que asume las tareas de conmutación de la red.</li><li>○ Es la más usada en la actualidad.</li><li>○ Ventajas:<ul style="list-style-type: none"><li>▪ Fácil administración</li><li>▪ Sencillo añadir o desconectar nodos</li></ul></li><li>○ Inconvenientes:<ul style="list-style-type: none"><li>▪ Si falla el nodo central, deja de funcionar la red</li><li>▪ Requiere una línea (cable) para cada equipo</li></ul></li><li>○ Ej: LAN</li></ul></li></ul>	 <p>Diagrama de topología Estrella: Seis nodos (tres puestos de trabajo, una impresora y un servidor) están conectados individualmente a un switch central.</p>
<ul style="list-style-type: none"><li>- <b>Bus:</b><ul style="list-style-type: none"><li>○ Todas las estaciones se conectan a un único medio de transmisión (cable coaxial) mediante conectores en T</li><li>○ Ventajas:<ul style="list-style-type: none"><li>▪ Sencillez</li><li>▪ Bajo coste</li></ul></li><li>○ Inconvenientes:<ul style="list-style-type: none"><li>▪ La rotura del cable principal dejaría sin servicio a todos los equipos de la red</li></ul></li><li>○ Ejemplo: antiguas redes Ethernet sobre cable coaxial</li></ul></li></ul>	 <p>Diagrama de topología Bus: Tres puestos de trabajo, una impresora y un servidor están conectados a una única línea horizontal central.</p>
<ul style="list-style-type: none"><li>- <b>Anillo:</b><ul style="list-style-type: none"><li>○ La red consta de una serie de repetidores que reciben y retransmiten la información conectados unos a otros como en un anillo.</li><li>○ Ventajas:<ul style="list-style-type: none"><li>▪ Localización de errores fácil</li><li>▪ El software es sencillo</li></ul></li><li>○ Inconvenientes:<ul style="list-style-type: none"><li>▪ El fallo de un enlace implica el fallo del anillo</li><li>▪ Difícil adición de nuevos nodos</li><li>▪ El repetidor de cada nodo ralentiza la velocidad de transmisión</li><li>▪ Instalación de cableado compleja</li></ul></li></ul></li></ul>	 <p>Diagrama de topología Anillo: Seis nodos (tres puestos de trabajo, una impresora y un servidor) están conectados en un círculo cerrado.</p>

## 5. CABLEADO ESTRUCTURADO

Es una técnica de diseño de un sistema de cableado caracterizada por la modularidad y flexibilidad. De este modo, permite cambiar, identificar y mover periféricos o equipos de una red con flexibilidad y sencillez.

Sigue una organización jerarquizada por niveles:

- **Localización de cada puesto de trabajo:** cable que conecta las rosetas que tienen conectores RJ45 con la tarjeta de red del equipo
- **Subsistema horizontal o de planta:** soporta el tráfico de una planta
- **Subsistema administrador o distribuidor:** conecta el horizontal con el vertical. Suelen tratarse de racks con los paneles de distribución, hubs y switches de cada planta.
- **Subsistema vertical o backbone:** encargado de comunicar todos los subsistemas horizontales. Requiere medios de transmisión de gran ancho de banda.
- La distribución vertical se conecta con la red pública de comunicación o con el subsistema de campus (extiende la LAN a varios edificios) en el **cuadro de entrada de servicios**.

