# REDES DE ORDENADORES

# 

[**REDES DE ORDENADORES**](#_heading=h.gjdgxs) **[1](#_heading=h.gjdgxs)**

[1.-](#_heading=h.3znysh7)I[NTRODUCCIÓN](#_heading=h.3znysh7)[2](#_heading=h.3znysh7)

[2.- VENTAJAS E INCONVENIENTES EN E](#_heading=h.3znysh7)[L USO DE REDES](#_heading=h.2et92p0) [2](#_heading=h.2et92p0)

[3.- SISTEMAS INFORMÁTICOS EN RED](#_heading=h.tyjcwt) [3](#_heading=h.tyjcwt)

[4.- CLASIFICACIÓN DE LAS REDES DE ORDENADORES](#_heading=h.3dy6vkm) [3](#_heading=h.3dy6vkm)

[4.-1.- REDES SEGÚN LOS SERVICIOS QUE BRINDAN](#_heading=h.1t3h5sf) [4](#_heading=h.1t3h5sf)

[4.2.- REDES SEGÚN EL ÁREA GEOGRÁFICA QUE OCUPAN](#_heading=h.4d34og8) [4](#_heading=h.4d34og8)

[5.- ELEMENTOS DE UNA RED](#_heading=h.2s8eyo1) [5](#_heading=h.2s8eyo1)

[6.- EXPLOTACIÓN DEL CIRCUITO DE DATOS](#_heading=h.17dp8vu) [7](#_heading=h.17dp8vu)

[6.1.- TIPOS DE COMUNICACIONES](#_heading=h.3rdcrjn) [7](#_heading=h.3rdcrjn)

[6.2.- TIPOS DE TRANSMISIONES](#_heading=h.26in1rg) [8](#_heading=h.26in1rg)

[7.- ARQUITECTURA DE UNA RED - TOPOLOGÍA](#_heading=h.lnxbz9) [9](#_heading=h.lnxbz9)

[7.1.- Topología en bus](#_heading=h.35nkun2) [9](#_heading=h.35nkun2)

[7.2.- Topología en estrella](#_heading=h.1ksv4uv) [10](#_heading=h.1ksv4uv)

[7.3.- Topología en anillo](#_heading=h.44sinio) [10](#_heading=h.44sinio)

[7.4.- Topología en malla](#_heading=h.2jxsxqh) [11](#_heading=h.2jxsxqh)

[7.5.- Topología en árbol](#_heading=h.z337ya) [12](#_heading=h.z337ya)

[8.- ELEMENTOS DEL NIVEL FÍSICO](#_heading=h.3j2qqm3) [12](#_heading=h.3j2qqm3)

[8.1.- MEDIOS FÍSICOS GUIADOS](#_heading=h.1y810tw) [13](#_heading=h.1y810tw)

[8.1.1.- Cable par trenzado](#_heading=h.4i7ojhp) [13](#_heading=h.4i7ojhp)

[8.1.2.- Cable coaxial](#_heading=h.2xcytpi) [16](#_heading=h.2xcytpi)

[8.1.3.- Fibra óptica](#_heading=h.1ci93xb) [17](#_heading=h.1ci93xb)

[8.2.- MEDIOS FÍSICOS NO GUIADOS](#_heading=h.3whwml4) [18](#_heading=h.3whwml4)

[9.- Dispositivos hardware de nivel físico](#_heading=h.2bn6wsx) [19](#_heading=h.2bn6wsx)

[10.- Dispositivos hardware de nivel de enlace](#_heading=h.qsh70q) [20](#_heading=h.qsh70q)

[11.- Dispositivos hardware de nivel de red](#_heading=h.3as4poj) [22](#_heading=h.3as4poj)

[12.- REDES DE ÁREA LOCAL](#_heading=h.1pxezwc) [22](#_heading=h.1pxezwc)

[12.1.- Redes ethernet (802.3)](#_heading=h.49x2ik5) [22](#_heading=h.49x2ik5)

[12.2.- Redes fast ethernet](#_heading=h.2p2csry) [23](#_heading=h.2p2csry)

[12.3.- Gigabit ethernet](#_heading=h.147n2zr) [23](#_heading=h.147n2zr)

[12.4.- 10 Gigabit ethernet](#_heading=h.3o7alnk) [23](#_heading=h.3o7alnk)

[12.5.- Redes inalámbricas (802.11)](#_heading=h.23ckvvd) [24](#_heading=h.23ckvvd)

[12.5.1.- Topologías inalámbricas](#_heading=h.ihv636) 24

# 

## 1.- INTRODUCCIÓN

Una red de ordenadores es "**un conjunto de computadoras autónomas interconectadas"**. Efectivamente, al menos dos ordenadores conectados entre sí mediante algún medio, que se comunican y transmiten información forman una red. En la definición usamos dos palabras muy parecidas en significados pero que presentan diferencias a tener en cuenta: **comunicación y transmisión.**

1. **Transmisión:**

Es el transporte de la señal donde **"viajan" los datos.** Así la transmisión solo se encarga de transportar sin importarle la información en sí. Para transportar la información se usan señales de diversos tipos: eléctricas, luminosas, acústicas, etc.

1. **Comunicación:**

Se refiere al **transporte de la información**. Cuando emisor y receptor se comunican no importa mucho la señal por la que lo hagan ni sus características físicas, solo importan los datos que se están proporcionando ambos elementos en la red.

**NOTA:** Si existe comunicación existe transmisión, pero no siempre que se transmite se está comunicando.

## 2.- VENTAJAS E INCONVENIENTES EN EL USO DE REDES

Entre las ventajas que proporciona el uso de redes de ordenador destacamos:

1. **Compartir información. Conectividad.**

Evitamos tener duplicada la información; además el hecho de tener un fichero en varios lugares podría producir incoherencias en la información, ya que alguno de ellos pudiera estar más actualizado que otro.

1. **Abaratamos costes.**

Si tenemos una impresora compartida en un PC podemos acceder a ella desde cualquier lugar de la misma en lugar de comprar una impresora para cada PC. Los recursos se comparten y ahorramos en gastos.

1. **Repartimos el trabajo.**

Una tarea puede dividirse en partes de forma que cada puesto en la red desempeñe una de esas tareas reduciendo la carga de trabajo

1. **Facilita la comunicación.**

El uso de redes ha conseguido que personas alejadas en espacio que antes no podían comunicarse ahora sí lo hagan.

**5.Escalabilidad**

Una red de ordenadores puede ampliar fácilmente sus posibilidades, además

esta red puede conectarse con otras redes, y así dar mayores prestaciones.

Son pocos los inconvenientes que vienen asociados a los sistemas en red, sin embargo, existen algunos relacionados sobre todo con la seguridad del mismo:

1. **Ataques a la información.**

Si los equipos de la red no son suficientemente seguros pueden ser atacados y vulnerada la información.

1. **Mal uso o uso excesivo de la red.**

Al igual que facilita las comunicaciones y relaciones sociales se debe tener especial cuidado en no hacer un uso excesivo de ellas, ya que puede perjudicar al individuo y provocar un aislamiento social.

## 3.- SISTEMAS INFORMÁTICOS EN RED

Vamos a realizar una primera clasificación teniendo en cuenta el estado de aislamiento o conexión de un sistema informático. Distinguimos: **sistemas aislados, sistemas en red y sistemas distribuidos.**

1. **Sistemas aislados.**

Ordenadores que **no se conectan con ningún otro ordenador ni comparten información** con ellos. Se puede considerar como sistema aislado a aquel que se conecta esporádicamente a la red.

1. **Sistemas en red.**

Los sistemas en red son **los más usuales**. Tenemos **varios ordenadores conectados** entre sí gracias al uso de **un medio de conexión concreto**. En este tipo de sistemas, los ordenadores son accesibles a través de su nombre o **dirección IP**, **cada equipo** conoce al resto de equipos que la forman.

1. **Sistemas distribuidos.**

Este tipo de sistemas es similar a los sistemas en red, ya que todos los PC están conectados y compartiendo información; su peculiaridad radica en el nombre del ordenador, el lugar donde se encuentre el mismo, etc., son datos transparentes al usuario. Para entender los sistemas distribuidos hay que comentar que se trata de un sistema de “tolerancia a fallos”. ¿Qué queremos decir con esto? Pues que, al ser una única red, pero con **muchas computadoras** si alguno de los elementos falla, los otros podrán seguir realizando la función correctamente, por lo que los errores se complementan y evitan rápidamente. Por este motivo los sistemas distribuidos suelen **otorgar bastante confianza a la hora de trabajar con ellos**, ya que es **muy raro que falle el sistema por completo**.

## 4.- CLASIFICACIÓN DE LAS REDES DE ORDENADORES

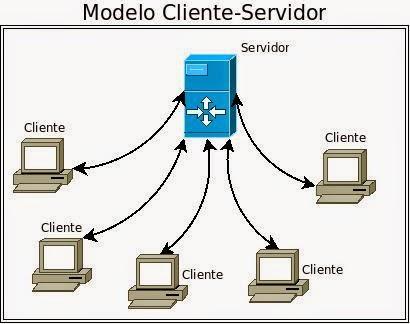
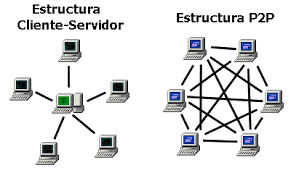
Las redes de ordenadores pueden clasificarse siguiendo diferentes criterios.

### 4.-1.- REDES SEGÚN LOS SERVICIOS QUE BRINDAN

El objeto de una red fundamentalmente es el de compartir información. Según esto podemos distinguir: **redes entre iguales (peer to peer) o redes cliente-servidor.**

1. **Redes cliente-servidor.**

Son aquellas en las que algunos PC de la red tienen el rol de clientede forma que demanda servicios y otros el de **servidor,** es decir, ofrece servicios. Normalmente, los equipos servidores suelen tener mejores prestaciones, aunque esto va en función del tipo de servicio que provea. Un servidor puede ser un ordenador en la red que comparte una simple carpeta. El rol de servidor o cliente va a depender de si comparte alguna información o recurso.

1. **Redes entre iguales (peer to peer).**

En una red entre iguales todos pueden ser clientes y servidores, ya que todos ofertan y demandan información y recursos.

### 4.2.- REDES SEGÚN EL ÁREA GEOGRÁFICA QUE OCUPAN

Según el área geográfica ocupada podemos distinguir los siguientes tipos de redes:

1. **Redes de área personal** (PAN, Personal Área Network).

Red formada por elementos que **no pueden ubicarse a mucha distancia** unos de otros para poder establecer comunicación. No son capaces de conectarse con otro ordenador vía telemática, es decir, si tenemos información en otro ordenador y copiamos ésta en un USB podremos acceder a ella a través de ese medio, pero seguiría siendo un sistema aislado. Es el tipo de red que hoy día es habitual configurar en casa, una red formada por uno o varios PC de escritorio, algún PC portátil, móviles con bluetooth o infrarrojos, consola de videojuegos, etc.

1. **Red de área local** (LAN, Local Area Network).

Red que ocupa una planta de un **edificio** o un edificio completo.

1. **Red de área de campus** (CAN, **Campus** Area Network)

Red cuyos ordenadores están distribuidos por todo un **campo universitario**, el espacio suele ser bastante mayor que el ocupado por una red LAN, **varios edificios.**

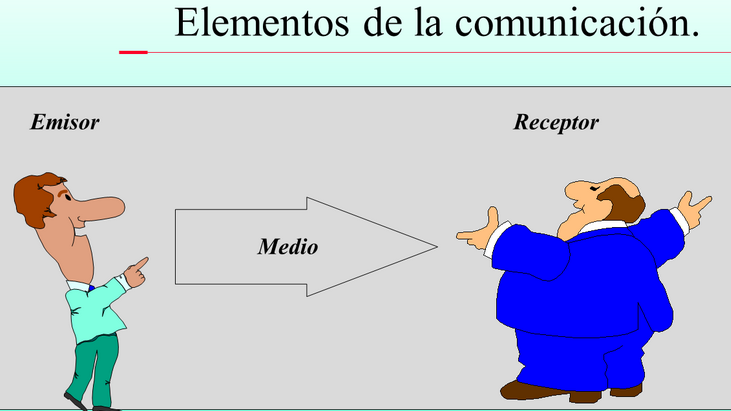
1. **Red de área metropolitana** (MAN, Metropolitan Area Network).

Red que ocupa **municipios** completos, ciudades o localidades completas. Una red MAN está **compuesta por redes LAN** que se interconectan usando determinados componentes de red.

1. **Red de área extensa** (WAN, wide area network).

Red que ocupa **países** y **continentes**

## 5.- ELEMENTOS DE UNA RED

****

Cuando hablamos de redes de ordenadores, teniendo en cuenta su definición de varios ordenadores conectados entre sí formando lo que se denomina circuito de datos, podemos deducir que en la red existen ordenadores que son emisores o receptores, medios por los que circula la información y dispositivos adicionales que permiten dicha comunicación.

1. **Ordenador, PC o Host**.

Elementos finales o iniciales de la transmisión de la información. En la red cualquier ordenador puede enviar un dato, ser emisor de información, o recibir un dato, ser receptor de la información. Existen determinados equipos que según la función que desempeñen sólo puedan ser receptores o emisores. A estos dispositivos se les llama ETD**.** (Equipo Terminal de Datos)

1. **Medio**:

Elemento que se usa para la **transmisión de la señal**. Es el elemento que se encarga del transporte de la señal entre emisor y receptor. Cada tipo de señal se transmite por un medio concreto, por ejemplo, las señales eléctricas por medios metálicos, las señales luminosas por fibras de vidrio, etc.

Las señales electromagnéticas usan multitud de medios en función de la frecuencia de la señal, cable, aire, etc.

.

1. **Transductor:**

Elementos ubicados junto a los ETD cuya misión es la de convertir la naturaleza de la señal para que **pueda ser transmitida por el medio físico.** Se denomina ECD (Equipo de Comunicación de Datos). Es un dispositivo de red que se encarga de convertir la naturaleza de la señal.

Por ejemplo, si tenemos una señal de tipo eléctrica la convierte en lumínica, etc. Ejemplo de transductor sería una bombilla o diodo, a la que le llega una señal eléctrica y la convierte en luminosa; su opuesto sería una célula fotoeléctrica o fotodiodo que se encargará de recoger las señales lumínicas y las convertirá en eléctricas.

1. **Otros elementos del sistema de comunicació**n.

Dispositivos de red que se encargan de **ampliar** la señal que viaja por un medio concreto, **repetir** la misma, etc. Como otros elementos definimos a aquellos que se ubican en algún lugar entre emisor y receptor del circuito de transmisión con un fin concreto.

Por ejemplo, cuando emisor y receptor están muy alejados en espacio y queremos enviar una señal entre ellos por el medio que sea, esta no acabará llegando por mucha potencia que tenga en el emisor, ya que acabará deteriorándose en el camino; para evitar esta pérdida se coloca en el medio un **dispositivo amplificador** que aumentará la señal para que llegue a su destino adecuadamente. Ejemplo de estos dispositivos son: Códec, **Repetidor, Antenas**, etc.

**Diferencia importante:**

**Equipo Terminal de Datos (ETD),** que serán todos los equipos, ya sean emisores o receptores de información.

**Vs**

**Equipo de Comunicación de Datos (ECD)** que es cualquier dispositivo que participa en la comunicación pero que no es ni emisor original ni receptor final.

**ETD:** Equipo Terminal de Datos. Existen diferentes tipos de terminales:

• **En función de la autonomía que poseen:**

1. **Terminal simple o tonto**.

Este terminal está compuesto por un teclado y una pantalla. Pueden introducir y visualizar información, pero **no procesar ésta.**

1. **Terminal autónomo:**

Tiene **capacidad para procesar** de forma independiente la **información**. Está provisto de procesador y memoria para tal fin. Un tipo especial de terminal autónomo es el **Terminal programable.**

**• Según el fin para el que se crean:**

1. **Terminal de propósito general.**

Puede desempeñar una gran variedad de funciones.

1. **Terminal de propósito específico:**

Solo se crea para desarrollar una función concreta. Como ejemplo de este tipo de servidores encontramos las supercomputadoras, por ejemplo, **Mare Nostrum** de Barcelona.

## 6.- EXPLOTACIÓN DEL CIRCUITO DE DATOS

### 6.1.- TIPOS DE COMUNICACIONES

Podemos distinguir tres formas en las que se produce la comunicación entre dos ETD: **Simplex, Half-duplex y Duplex.**



1. **Comunicación simplex**

En este tipo de comunicación existe **un solo emisor y un solo receptor, no pudiendo en ningún momento intercambiar sus papeles**. Cuando comienza la comunicación el emisor empieza a emitir estando el receptor siempre en espera. Ejemplo: Cuando escuchamos música por la radio, nosotros sólo recibimos.

1. **Comunicación half-duplex**

En este tipo de comunicación un extremo y otro de la misma **puede ser emisor y receptor, pero nunca al mismo tiempo.** Cuando uno de los dos extremos emite, el otro espera a recibir la información. Cuando la información llega al receptor este puede optar por convertirse en emisor o no. Así tenemos comunicación bidireccional pero no simultánea. Ejemplo: Hablar por el walkie-talkie.

1. **Comunicación dúplex**

En este tipo de comunicación un extremo y otro actúan como emisor y receptor, y pueden transmitir la información **al mismo tiempo**. Hablamos de una **comunicación** **bidireccional** y **simultánea**. Ejemplo claro de este tipo de comunicación es la comunicación telefónica. En el momento que se establece comunicación entre los dos abonados ambos pueden hablar a la vez sin esperar turno de palabra. Otro ejemplo: redes de ordenadores.

### 6.2.- TIPOS DE TRANSMISIONES

Cuando hablamos de la transmisión en sí, es decir, del transporte de la señal, podemos distinguir varios tipos: **Síncrona y asíncrona o Serie y paralela.**

**Síncrona y asíncrona**

1. **El sincronismo**

Es el procedimiento por el que **emisor y receptor** se **ponen de acuerdo** sobre el **momento concreto en el que va a comenzar y acabará la transmisión**. Si se produce un error de sincronismo, la señal se desplazará del emisor al receptor, pero al no saber dónde empieza la información o dónde acaba, no podrá ser interpretada correctamente.

Cuando hablamos de transmisión **asíncrona,** el proceso de sincronización se hace palabra a palabra de forma que **se indica cuando empezamos a transmitir** y **cuando** **acabamos en cada palabra** mediante el uso de bits **delimitadores**. Por ejemplo, si el canal está en silencio (transmitiendo cero lógicos), se puede indicar que se va a comenzar a transmitir emitiendo un 1 al receptor. De igual modo, cuando acabe la transmisión se pueden agregar varios bits de stop.

En una transmisión síncrona, la transmisión se realiza de forma constante bit a bit existiendo determinados bits de control.

1. **Serie y paralelo**

En una transmisión **serie** la información circula por una **única línea de datos** de forma secuencial, es decir, los bits van uno a uno detrás de otro, por el mismo canal. En la transmisión **paralela** la **información** circula por **varias líneas de comunicación**, es decir, se transmiten simultáneamente varios bits a la vez.

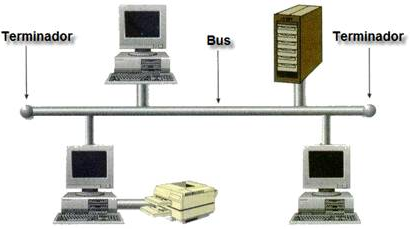
**NOTA:** Puede parecer que la transmisión paralela es la mejor de las opciones; sin embargo, debemos pensar un poco antes de afirmarlo, ya que al existir mayor número de líneas también aumentan las interferencias entre ellas.

## 7.- ARQUITECTURA DE UNA RED - TOPOLOGÍA

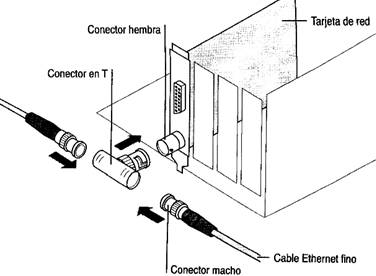
Una arquitectura de red define la forma en la que se conectan los nodos o host de red, qué proceso deben seguir cuando quieran comunicarse con otro host, teniendo en cuenta el medio del que disponen. Así, cuando hablamos de arquitectura de red estamos hablando de: **topología de la red, método de acceso al medio y protocolo o familias de protocolos de comunicación.**

La **topología** de una red refiere la **forma física** de la misma. Normalmente, hablamos de topología cuando trabajamos con redes cableadas, de forma que el dibujo que forman los PC con los cables o medios físicos que los unen constituyen esta. En redes **inalámbricas** también se distinguen topologías, por ejemplo, topología **ad-hoc** en las que existe una comunicación **punto a punto** entre dos elementos de red.

### 7.1.- Topología en bus

****

Todos los ordenadores están conectados a un mismo medio físico: único cable troncal con terminaciones en los extremos. Esta topología era implementada por las primeras redes Ethernet mediante **cable coaxial**, siguiendo el estándar **IEEE 802.3.**

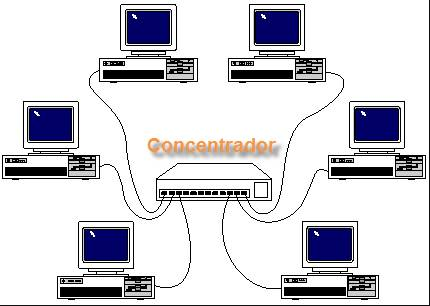


El medio usado tiene múltiples accesos para que los PC puedan conectarse a él y en los extremos, para evitar la producción de ECO o reflexiones (la señal transmitida rebota en un extremo y vuelve al medio), se colocaban unos terminadores que absorbían la señal.

Una de las desventajas de este tipo de redes era la rotura del medio físico usado, dejando inservible toda la red.

### 7.2.- Topología en estrella

En esta topología la red forma una estrella, existiendo un nodo o elemento que centraliza todo el paso de información: que puede ser: un router, un conmutador o switch, o, un concentrador o hub. Cada estación de trabajo se conecta punto a punto con el nodo central, de forma que si quieren transmitir información enviarán esta al nodo central y este se encargará de retransmitir a todos o al PC destino, según el tipo de dispositivo central que tengamos. La usan las redes de área local modernas.



**Ventajas:**

• Son redes **más seguras** ya que toda la información pasa por el nodo central, pudiendo detectarse posibles fallos en la comunicación.

• Si un segmento, de la red deja de funcionar no repercute en el resto (cuando hablamos de segmento nos referimos a la conexión entre una estación de trabajo y el nodo central).

**Inconvenientes:**

• El inconveniente principal de este tipo de redes es el denominado cuello de botella. Si toda la información debe pasar por el **nodo central**, a pequeñas cantidades de información no pasa nada, pero cuando el volumen a transferir aumenta, es posible que el nodo central se convierta en un cuello de botella de modo que la red se vea ralentizada.

• **Mal funcionamiento del nodo central o caída** del mismo. Si el nodo central deja de funcionar, **la red cae** ya que es el elemento principal de la misma.

### 7.3.- Topología en anillo

Los ordenadores que tienen esta topología forman un anillo, de manera que observamos una red en la que de dos en dos se conectan punto a punto los hosts, cerrando el círculo el primer y último PC.

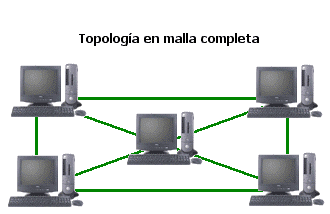


Ejemplo de redes con esta topología son las redes Token Ring, que siguen el estándar **IEEE 802.5.** En las redes en anillo, al igual que ocurría en las redes en bus, la rotura del cable produciría la caída total de la red.

En una red en anillo existe un elemento denominado **MAU** que se encarga de establecer físicamente el anillo. Es un dispositivo parecido al usado en redes en estrellas con la peculiaridad que forma un anillo en lugar de conexiones puntos a punto entre él y cada host.

### 7.4.- Topología en malla

Este tipo de topología dibuja una red en la que **todos los elementos están conectados** punto a punto con uno o más de los componentes de la red. Si cada host se conecta con todos los demás host tenemos una malla completa o una topología de interconexión total, en la que cada PC debe tener varias interfaces de red.



Este tipo de topología tiene la **ventaja** de que **si un host deja de funcionar** los **demás continúan con su actividad normal;** todos pueden seguir comunicándose con todos a excepción del elemento que dejó de funcionar.

### 7.5.- Topología en árbol

Esta topología es una extensión de la topología en bus, donde varias líneas de buses se conectan a un bus central que propaga la señal a estos. Tenemos diferentes niveles a los que se conectan los hosts formando un árbol.



En estas topologías tenemos la ventaja de que, si un bus secundario deja de funcionar, el resto de buses continúan con la transmisión de información; aunque si cae el bus principal la red queda inservible.

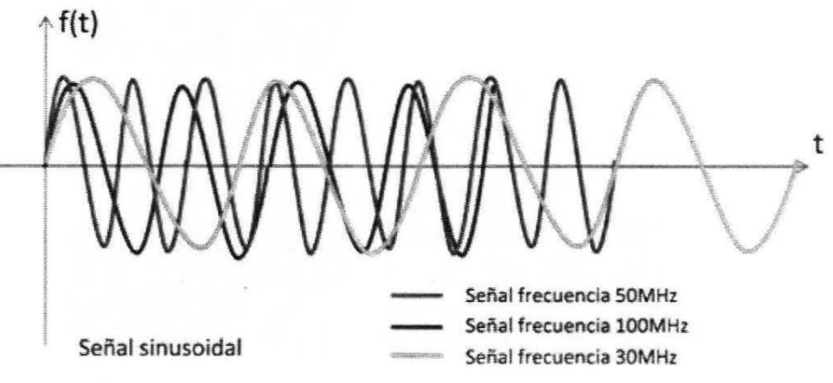
## 8.- ELEMENTOS DEL NIVEL FÍSICO

Según el modelo de referencia OSI, la capa o **nivel físico** es la que establece tipos de **medios** a usar para la **transmisión**, características físicas del medio, niveles de voltaje para representar ceros y unos, etc. El **medio físico** utilizado es de gran importancia, ya que las **características** del mismo **pueden perjudicar o no a la señal**, permitiendo por ejemplo el exceso de ruido (interferencias de señal) o una mayor velocidad. Se pueden transportar señales eléctricas, electromagnéticas, luminosas, etc., con lo que el medio físico se debe adecuar a las mismas. Los medios físicos se clasifican en dos tipos: **medios físicos guiados y medios físicos no guiados.**

Ya hablemos de medios físicos guiados o no guiados, cualquier medio que se use para transmitir una información tendrá una serie de **características** que determinarán su calidad.

• **Velocidad de transmisión de los datos.** Refiere el número de bits que es capaz de transmitir en un segundo. Se mide en Mbps.

• **Ancho de banda que soportan.** Podemos decir que el ancho de banda es la **diferencia entre la mínima y la máxima frecuencia** de señal que puede transmitir el medio físico. Un canal puede ser utilizado por señales de diferentes frecuencias. Así, si puede transmitir muchas señales, la información que atravesará el canal será mayor.

t

Señales que circulan por un canal con diferentes frecuencias. El ancho de banda sería de 70 MHz. (100 -30)

• **Espacio máximo entre dos repetidores.** El medio físico que se utilice dictará la distancia que deben tener como máximo dos nodos de la red para que puedan comunicarse. Además, si debemos configurar una red con muchos ordenadores y bastante extensa probablemente tendremos que hacer uso de repetidores que deben contemplar esta distancia.

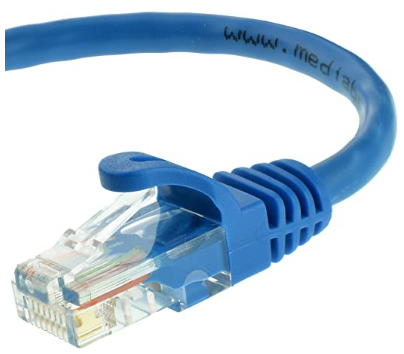
• **Fiabilidad.** La fiabilidad de la red depende en gran medida del medio que se use. Una red cableada será más fiable que una red inalámbrica.

### 8.1.- MEDIOS FÍSICOS GUIADOS

Son aquellos en los que la señal se transmite de forma que **el medio guía ésta**. Existe un elemento, como cable de cobre, fibra de vidrio, etc., que se encarga de establecer un **camino** por el que debe circular la portadora. Entre los medios físicos guiados estudiaremos: **cable par trenzado, cable coaxial y fibra óptica.**

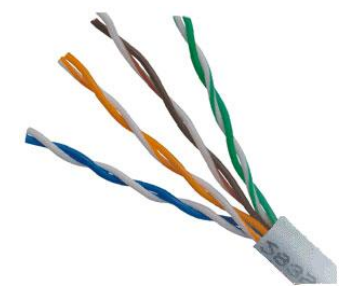
#### 8.1.1.- Cable par trenzado

El cable par trenzado está formado por **pares de cobre**, de forma que cada **par** está **entrelazado** con objeto de evitar o reducir interferencias. El problema de las interferencias es algo a tener muy en cuenta ya que si se produce ruido la información transportada puede quedar ilegible. Las interferencias suelen subsanarse con el uso de una tela metálica que cubre a todos los grupos de pares que forman un cable o a cada par de hilos.

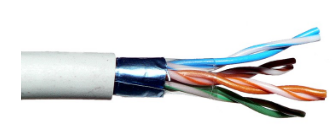


**Cables pares trenzados en función de si están o no apantallados:**

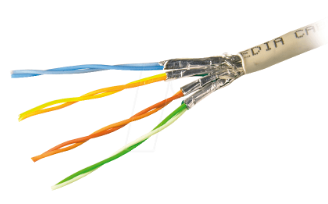
• **UTP (Unshield Twisted Pair, par trenzado sin apantallar).** Son hilos de cobre sin apantallar, es decir, no tienen una malla metálica protectora. Son los más económicos, pero no tienen tanta fiabilidad como el resto, ya que sólo reducen interferencias con el trenzado del cable.



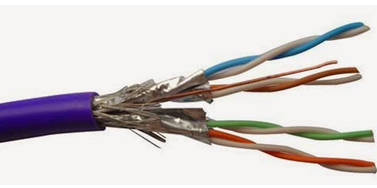
• **FTP (Foiled Twisted Pair, par trenzado con pantalla global).** Este tipo de cable es de nivel intermedio, ya que sí dispone de malla de protección, pero esta malla cubre todos los hilos de cobre.



• **STP {Shielded Twisted Pair, par trenzado apantallado).** Este tipo de cable trenzado es el más fiable ya que cada par de hilos de cobre, además de estar trenzado, dispone de una malla metálica que los recubre. Es más caro que el UTP y más rígido ya que en su interior encontramos "más elementos materiales".



• (**SFTP**) o **par trenzado totalmente blindado** es un tipo especial de cable que utiliza múltiples versiones de protección metálica, estos son blindados y apantallados.



**Tipos de cables par trenzado según categorías.**

• **Categoría 1:** Transmisión telefónica de voz, no de datos. El cable par trenzado telefónico suele estar constituido por cuatro hilos de cobre en lugar de 8 como es habitual en un cable de red.

• **Categoría 2:** Para la transmisión de datos. Velocidad de hasta 4 Mbits/s. Está totalmente desfasado.

• **Categoría** 3: Muy usado tiempo atrás. Para transmisión de datos. Velocidad de hasta 10 Mbits/s.

• **Categoría 4:** Cable que permitía alcanzar hasta los 20 Mbits/s. Poco común y no demasiado útil.

• **Categoría 5:** El más empleado seguido del de categoría 3. Usado para la transmisión de datos, alcanzado velocidades de hasta 100 Mbits/s.

• **Categoría 5e:** Para la transmisión de datos con velocidades de hasta los 1000 Mbits/s (uso en redes Gigabit Ethernet).

• **Categoría 6:** Usado para la transmisión de datos entre puntos bastante distanciados. Se alcanzan velocidades de hasta los 1000 Mbits/s.

• **Categoría 6a y 7:** Como casi todos los anteriores es usado para la transmisión de datos a muy altas velocidades (videoconferencias, redes de almacenamiento, etc.), 10.000 Mbits/s, formando redes 10 Gigabit Ethernet.

El cable par trenzado utiliza **conectores RJ45**. Para cables de dos pares RJ11.

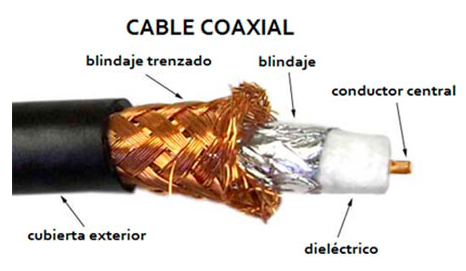
Hoy día, la mayoría de las redes de área local instaladas (LAN) que utilizan medios guiados, usan este tipo de cable, de categoría 5, 6 y 7.

#### 8.1.2.- Cable coaxial

El cable coaxial fue muy usado en las **primeras configuraciones de redes LAN** y poco a poco **ha sido sustituido por el cable par trenzado** estudiado en el apartado anterior. **Hoy día, suele usarse en redes MAN**, para la interconexión de diferentes LAN en un área geográfica no excesivamente extensa. La configuración de una LAN con este tipo de cable conllevaba una topología en bus.

**Las características de un cable coaxial son:**

• El cable puede ser de mayor longitud sin que se produzcan pérdidas de información. • Es menos sensible a interferencias debido a su formato.



Nuevo revestimiento para aislar de interferencias.

Hilo de cobre. Medio por el que se transmite la información.

Este tipo de cable usa un conector BNC.



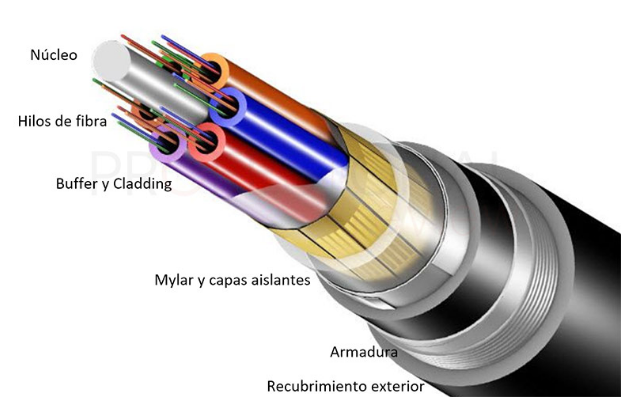
Además, existen otros elementos de conexión, como conector **T** que permite conectar dos extremos del cable y la NICcorrespondiente o terminadores.



#### 8.1.3.- Fibra óptica

Este medio permite la transmisión de señales ópticas que no están sujetas a interferencias electromagnéticas. Como fuente de luz para la transmisión de información se usan rayos láser o diodos LED.





.

Cubierta del conjunto de fibras que aíslan a las mismas de luz externa no deseada. Fibras protectoras.

Cubierta de cada fibra de vidrio.

Revestimiento.

Núcleo.

Existen diferentes tipos de **conectores** para fibra óptica: **SC**, **FC, LC, FDDI, ST,** etc.

Existen dos **tipos** de fibra óptica: **monomodo y multimodo.** En las primeras solo se transmite un haz de luz y este se hace de forma paralela al medio por el que circula. En las fibras multimodo se transportan varias señales luminosas por el mismo canal; las señales rebotan en las paredes y se van transmitiendo de ese modo.

### 8.2.- MEDIOS FÍSICOS NO GUIADOS

La información se envía mediante **señales electromagnéticas** que se propagan en el **medio libre**, con o sin atmósfera. Para que se produzca la transmisión de información deben existir antenas que se encargue de la emisión y recepción de estas ondas.

Las transmisiones no guiadas pueden ser: **direccionales y omnidireccional.**

• **Transmisión direccional.** Es aquella en la que la señal se concentra para ser enviada en una **única dirección**, de forma que no deben existir obstáculos entre antena emisora y receptora que obstaculicen la transmisión.

• **Transmisión omnidireccional.** La información **se envía en todas direcciones** con lo que puede ser recibida por varias antenas.

Cada vez es más común el uso de medios no guiados en la construcción de redes de ordenador, ya no solo en redes personales o LAN, sino en redes MAN. La facilidad de instalación y uso es una de sus ventajas. Sin embargo, cuando no disponemos de cables y es el medio libre el que usamos para transmitir la información, la climatología, la geografía del medio, etc., son inconvenientes a tener en cuenta.

**Son medios físicos no guiados:**

• **Sistemas radio terrestres, radiotransmisión.** Las ondas de radio son fáciles de generar, pueden viajar largas distancias, atraviesan paredes accediendo al interior de los edificios y son omnidireccionales.

• **Sistemas de Microondas.** Este tipo de señal es direccional ya que por encima de los 100 Hz la señal viaja en línea recta y puede orientarse a un receptor concreto. Utilizan este medio la televisión por satélite.

• **Sistemas de Ondas infrarrojas.** Para la comunicación entre dos dispositivos que no estén a demasiada distancia.

## 9.- Dispositivos hardware de nivel físico

1. **MODEM**

Dispositivo encargado de **modular/demodular la señal**. Cuando la información tiene que ser enviada ha de serlo a través de un medio físico concreto con determinadas características, así, **la señal debe ser adaptada al medio físico (debe ser modulada).** Cuando la señal se recibe debe realizarse el proceso inverso (debe ser demodulada). Existen dos tipos: **interno y externo.**

Hoy día, cuando se habla de este dispositivo nos referimos normalmente a aquel que se encarga de conectar nuestra red de casa a la red de área extensa. Son ejemplo de estos adaptadores: **modem RDSI (**conecta nuestra red interna a la red digital RDSI), **modem ADSL** (conexión a través de la línea telefónica), **modem cable** (conexión a través de líneas coaxiales implementadas en un principio para ver televisión) y **modem inalámbrico** (conexión mediante antena a una red pública).

1. **REPETIDORES**

Se encargan de **amplificar la señal digital**, debido a que en **largas distancias** esta se atenúa pudiendo llegar a desvanecerse. Estos dispositivos restauran la señal original permitiendo que alcance el equipo receptor de la información.

Existe otro tipo de dispositivo que realiza la misma función que un repetidor, el amplificador, la diferencia está en que la señal que aumentan es analógica.

1. **CONCENTRADORES DE CABLEADO**

También denominados **repetidores multipuerto.** Es un dispositivo cuya misión es la de repetir la información que recibe por todas sus salidas o puertos, y conectar todos los nodos de la red. Existen dos tipos: **repetidores pasivos** que básicamente se encargan de conectar todos los nodos de la red permitiendo su comunicación y los **repetidores activos** que además de repetir y comunicar la señal, la amplifican y regeneran antes de ser reenviada.

Cuando usamos un concentrador en una red decimos que utiliza topología física en estrella, sin embargo, en función del tipo de repetidor, la topología lógica será en bus o en anillo. Así tenemos repetidores **con topología lógica en bus,** conocidos con el nombre de **HUB** y los repetidores con topología **lógica en anillo,** también denominados **MAU.**

## 10.- Dispositivos hardware de nivel de enlace

El uso de dispositivos de nivel físico para conectar los nodos de una red es una solución sencilla y útil cuando el número de ordenadores de la red es escaso y no esperamos un rendimiento elevado de la misma. En el momento en el que comenzamos a **agregar nuevos nodos, la red se ralentiza** y no es capaz de gestionar redes relativamente grandes.

**NOTA:** Al usar un repetidor (HUB) para conectar una red, cada vez que un nodo quiere enviar una información esta se propagará por todos los puertos del dispositivo, de forma que el dato llega a todas las estaciones, todas rechazan el paquete a excepción del receptor que lo interpreta. De este modo, si la tasa de transferencia de la red es de 1 O

Mbps, al usar todos los canales para retransmitir la información, en un repetidor de 1 O puertos esta tasa se verá dividida entre 1 O, de forma que la tasa de transferencia se reducirá a 1 Mbps para cada puerto. Si el número de puertos aumenta, disminuirá la velocidad a la que transmiten cada uno de ellos y hará que la red deje de rendir.

Además, puede ocurrir que tengamos una única LAN montada en un edificio o varias, y en el caso de que sean varias, estas pueden seguir diferentes estándares, 802.3, 802.11, 802.5, etc., y deben estar conectadas entre sí. Esta casuística solo es capaz de resolverla un dispositivo de nivel de enlace.

Los **dispositivos de nivel de enlace** trabajan con **direcciones MAC** (media access control) o direcciones físicas. Una dirección MAC está compuesta por **48 bits**, 6 bloques de números hexadecimales, e **identifican de forma única a una tarjeta o dispositivo de red**. Los tres primeros octetos (en orden de transmisión) identifican a la organización que publicó el identificador y son conocidas como "identificador de organización único", fabricante (OUI). Los siguientes tres octetos son asignados por esta organización a su discreción para identificar de forma única el producto.



1. **NIC (NETWORK INTERFACE CARD)**

**Tarjeta de Interfaz de Red**, es el elemento que permitirá la conexión del PC a la red, al medio físico. Existen **diferentes tipos** en función de la arquitectura o **cableado** de red que se utilice (tendremos adaptadores para redes Ethernet, Token Ring, inalámbricas, etc.)

1. **PUENTES (BRIDGES)**

Es el dispositivo encargado de **conectar a nivel de enlace redes con topologías y protocolos diferentes**. Como su nombre indica, es un puente o salto a la otra red.

Es un dispositivo que está formando por al menos dos interfaces diferentes, una por cada tipo de red que conecta, por ejemplo, si tenemos una estructura de red LAN con cable par trenzado y otra con cable coaxial, tendrá como mínimo un conector RJ45 y BNC hembras.

Además, este dispositivo no solo se encarga de conectar redes diferentes a nivel de enlace, controla el tráfico de red de forma que no deja pasar a través de él cualquier paquete que no esté remitido a la otra red, es decir, solo "atraviesan el puente" aquellos paquetes cuyo destino sea un ordenador de la otra LAN, a diferencia de los repetidores que retransmitían la información a todos.

1. **PUNTO DE ACCESO INALÁMBRICO (AP)**

Se encarga de **interconectar dispositivos inalámbricos** para formar una red inalámbrica. Normalmente un AP tiene una serie de puertos RJ45 que le permiten conectar con la red cableada pudiendo enviarse información desde la red inalámbrica a la cableada.

Básicamente un punto de acceso es un **repetidor**, ya que en el momento que recibe un dato lo almacena y lo transmite a todos los puestos inalámbricos y cableados.

1. **CONMUTADORES (SWITCH)**

Conectan redes a nivel de enlace de datos, pero a diferencia de los puentes estas redes deben **cumplir los mismos protocolos**. Se usan conmutadores para segmentar la red y mejorar su rendimiento.

Un **switch** es selectivo de forma que **solo enviará la información a través del puerto por el que se llegue al PC receptor** de esta. Así, si la tasa de transferencia de la red es de 1 O Mbps, todos los puertos disfrutarán de esta velocidad porque en el mismo instante la información solo estará transmitiendo por uno de ellos.

Normalmente cuando estudiamos los switch decimos que son **inteligentes**, la verdad es que [**aprenden en función de las peticiones**](https://www.sapalomera.cat/moodlecf/RS/1/course/module5/5.3.1.2/5.3.1.2.html#:~:text=El%20switch%20introduce%20en%20la,trama%20y%20su%20puerto%20asociado.) **de envío que se realicen.** Cuando un equipo en la red quiere transmitir, el switch observa la dirección IP destino del paquete a enviar. En ese momento realiza una petición ARP1 por la que solicita que se busque la dirección MAC asociada a esta dirección IP (ya que es un dispositivo de nivel de enlace). Finalmente, el dispositivo **configura una tabla** en la que encontraremos **(MAC del puerto del switch) -- (MAC del NIC del PC con dirección IP buscada),** de forma que, en los próximos envíos a esa dirección, el switch ya habrá aprendido a donde transmitir los datos.

**NOTA:** Existen dispositivos híbridos, que trabajan a varios niveles, por ejemplo, dispositivos de nivel 2 y 3, es decir, router con varios puertos que permiten la conexión de varios dispositivos formando una red gestionada como un switch.

## 11.- Dispositivos hardware de nivel de red

Estos dispositivos trabajan con direcciones IP, 32 bits agrupados en 4 números decimales. Se encargan de desempeñar las funciones que se indican en el nivel de red.

**ENCAMINADORES O ROUTERS**

Estos dispositivos conectan la red al resto de redes dejando **sólo** pasar la información a través de ellos cuando **va dirigida a un equipo con dirección IP de una red diferente a la del equipo emisor**. Además, a la hora de transmitir la información a otra red se encargan de localizar la ruta más óptima, el camino más corto y seguro por el que puede ser enviada esta.

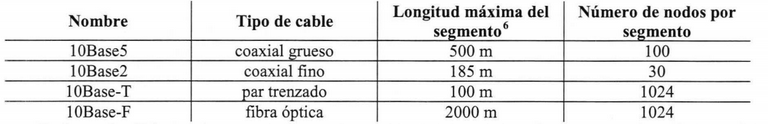
## 12.- REDES DE ÁREA LOCAL

Existen diferentes tipos de redes de área local definidas por el IEEE con el nombre 8025. 802.3 y 802.11 son los estándares más usados actualmente.

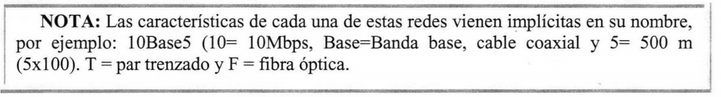
### 12.1.- Redes ethernet (802.3)

Son redes cableadas que utilizan algún tipo de cable de los estudiados en los apartados anteriores. Usan codificación **Manchester o Manchester diferencial** y emplean la técnica de **control de acceso al medio** CSMA/CD (Carrier Sense Multiple Access with Collision Detection), es decir, cuando un ordenador de la red quiere transmitir observa el medio físico antes de hacerlo. Si el medio está libre llevará a cabo la transmisión y si se produce alguna colisión también detectará esta.

La velocidad máxima de transmisión de estas redes es de 10 Mbps. Vemos en la siguiente tabla los tipos más comunes de cableado Ethernet.



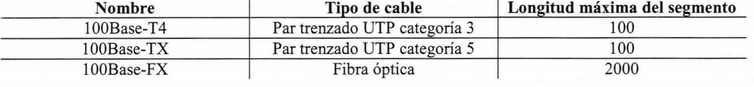
En las redes Ethernet era común la configuración 5-4-3: máximo 5 segmentos de red, 4 repetidores y solo en 3 de estos segmentos conectan PCs.

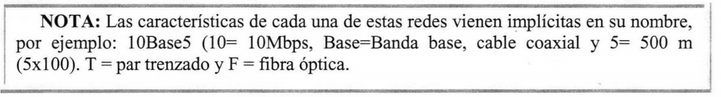
****

### 12.2.- Redes fast ethernet

Al principio, las redes Ethernet con 10 Mbps de velocidad cubrían todas las necesidades de transmisión de la época, sin embargo, según han ido pasando los años, estas velocidades se han ido quedando pequeñas. Finalmente, aparece **802.3u**, más conocido como **Fast Ethernet.**

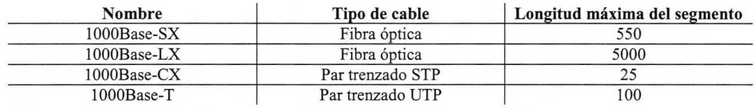
Las redes Fast Ethernet usan cable par trenzado de categoría 3 o 5, en combinación con dispositivos conmutadores (switch) o concentradores (hub). Podemos encontrar alguna combinación con fibra óptica, siendo el cable coaxial descatalogado en esta configuración. La longitud máxima del segmento es 100 m y alcanza velocidades de 100 Mbps.



****

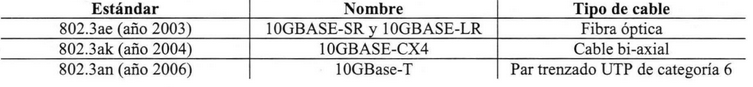
### 12.3.- Gigabit ethernet

Nada más finalizar con el estándar 802.3u se empezó a trabajar en un nuevo estándar que aportara mayor velocidad consiguiendo el **802.3z** conocido como **Gigabit Ethernet.** Se pretendía que la red fuera unas diez veces más rápida que la recién creada Fast Ethernet.



### 12.4.- 10 Gigabit ethernet

La IEEE ha seguido avanzando en el desarrollo de nuevos estándares que aumenten la velocidad de transmisión en redes cableadas, consiguiendo alcanzar los 10 Gbps.



### 12.5.- Redes inalámbricas (802.11)

Son redes que usan radiofrecuencia (parte del espectro electromagnético) o infrarrojos para transmitir la información. Básicamente están compuestas por un AP al que se conectan todos los demás dispositivos inalámbricos clientes. Usan la **banda** ISMde **2,4 GHz**, compartiendo esta con dispositivos como microondas o teléfonos móviles. El estándar 802.11 define una red que alcanza velocidades de **1** o 2 Mbps vía infrarrojos.

Las siguientes revisiones, 802.11a, 802.11b, 802.11g o 802.11n aumenta la velocidad de transmisión, siendo el estándar 802.11 n el más usado en la actualidad.

1. **802.11a.**

Alcanza velocidades de hasta 54 Mbps en la banda ISM de 5 GHz.

1. **802.11b.**

Alcanza velocidades de hasta **11** Mbps en la banda de 2,4 GHz. Las tasas de datos soportadas son 1, 2, 5.5 y 11 Mbps.

1. **802.11g.**

Mejora de 802.11b. Puede operar en la banda de 2,4 GHz alcanzando tasas de hasta 54 Mbps.

1. **802.11n.**

Es en 2009 cuando ratifica el 802.11n con una velocidad de hasta 600 Mbps, **usando simultáneamente las bandas de 2,4 y 5 GHz.**

#### 12.5.1.- Topologías inalámbricas

Existen diferentes topologías de red inalámbrica.

1. **Redes Ad-Hoc**.

Este tipo de redes están formadas por dos ordenadores que se comunican **punto a punto**, no precisan de punto de acceso.

1. **BSS**

(Conjunto de servicios **básicos**). Redes formadas por un **único punto de acceso**. Los PC se conectan como clientes al AP.

1. **ESS**

(Conjunto de servicios **extendido**). Son redes más extensas en espacio que precisan de **varios puntos de acceso.** Los AP se configuran de forma que constituyen una única red, los PC clientes se conectan a ella sin saber a qué punto de acceso lo están haciendo.

#### 12.5.2.- El SSID de una red 802.11

Cuando se instala una red inalámbrica es conveniente asegurarnos de que los ordenadores se conectan con la red apropiada, esto se hace utilizando un **SSID**, que son las siglas en ingles de **Identificador de Conjunto de Servicio**. El SSID es una cadena alfanumérica de 32 caracteres de longitud, donde se distinguen las mayúsculas de las minúsculas, y **sirve para identificar a la red**. Este identificador se emplea para **informar a los dispositivos inalámbricos** de a qué **red pertenecen** y con qué otros dispositivos se pueden comunicar.

#### 12.5.3- Seguridad en 802.11.

Existen varias formas de mantener la seguridad en una red Wi-Fi, nosotros citaremos algunas de las más usuales. Hay que tener en cuenta que las redes Wi-Fi son **muy vulnerables a la interceptación de paquetes,** a los ataques o simplemente a que usuarios no autorizados se aprovechen de la conexión, por tanto, es conveniente implementar medidas de seguridad que prevengan un uso indebido de la red.

Empecemos comentando una medida que no proporciona ningún tipo de seguridad, pero dificulta a los clientes el conectarse, está medida es **ocultar el SSID.**

Otras medidas un poco más eficaces, consisten en encriptar o codificar la información que de la red. Para ello se pueden usar distintos tipos de cifrado:

* **WEP**: Privacidad equivalente a cableado, se encarga de encriptar la información o los datos utilizando claves preconfiguradas para cifrar y descifrar los datos. Puede utilizar claves de 64 bits, 128 bits o 256 bits. Al ser un **método bastante débil,** ya que es fácilmente descifrable, no es muy recomendable utilizarlo.
* **WPA**: Acceso Wi-Fi protegido, utiliza claves de cifrado de entre 64 y 256 bits. Sin embargo, en WPA se generan claves nuevas de manera dinámica con lo que dificulta su descifrado.
* **WPA-PSK** que utiliza un algoritmo complejo de encriptación, utilizando el protocolo TKIP que es el que **cambia la clave dinámicamente**. Por lo que WPA-PSK es vulnerable en la primera conexión al punto de acceso que es donde utiliza la clave preestablecida, después va cambiando las claves de forma dinámica.

El **filtrado de direcciones MAC** es una medida de seguridad adicional y se recomienda utilizarla como complemento de algunos de los métodos de encriptación. Consiste en configurar el **punto de acceso** o router de tal forma que tenga **un listado de direcciones MAC de los equipos autorizados a conectarse** a la red inalámbrica, para que aquellos equipos que no estén en la lista no puedan conectarse.

## 13.- Modelo OSI Vs TCP

#### 13.1 Modelo OSI

El modelo OSI (Modelo para la Interconexión de Sistemas Abiertos), se compone de siete niveles de proceso, mediante el cual los datos se empaquetan y se transmiten **desde una aplicación emisora, viajando a través de medios físicos hasta llegar a una aplicación receptora.**

## https://lh7-us.googleusercontent.com/ma510fvlT6whaQDj3-gWHs_tT4LM2i8o398TB8PFUudIrKeDDvtczfLLHwGHPsF2Pjxwaw9wkbhIUSQ_NodnHXfzoEGIZa51YlfZF9MeSNEnIoANB9nJtGk4V8UHVl1q_9T3bv2_prgB56LQYn_e8Q

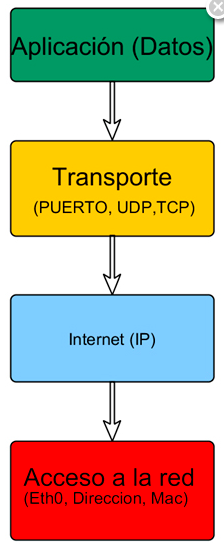
#### 13.2 Modelo TCP

**El Protocolo de Control de Transmisión (TCP)** es un protocolo utilizado para todos los nodos conectados a internet de manera que estos se puedan comunicar entre sí de manera fiable. Se trata de un **protocolo orientado a la conexión que junto con el protocolo IP ha servido de base para el modelo TCP/IP**, utilizado desde antes de que se estableciera el Modelo OSI (Interconexiones de Sistemas Abiertos) y por esta razón el modelo TCP/IP ha sido comparado con el modelo OSI.

Se conoce como ***familia de protocolos*** de Internet al conjunto de protocolos que son implementados por la pila de protocolos sobre los **cuales se fundamenta Internet y que permiten la transmisión de datos entre las redes** de computadoras.

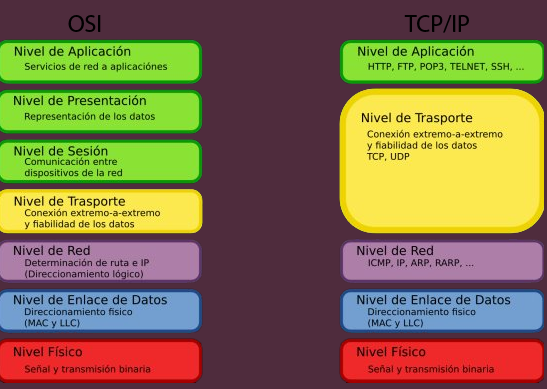
Los **dos protocolos más importantes** y que fueron también los primeros en definirse y en ser utilizados son: **TCP** (Protocolo de Control de Transmisión o Transmission Control Protocol) **e IP** (Protocolo de Internet o Internet Protocol), de ahí que el modelo se denomine **TCP/IP.**

Elmodelo **TCP/IP es un protocolo** dirigido **a la transferencia de información a través de internet,** o, dicho de otra manera, **es un protocolo utilizado por todas las computadoras conectadas a una red, de manera que estos puedan comunicarse entre sí.**

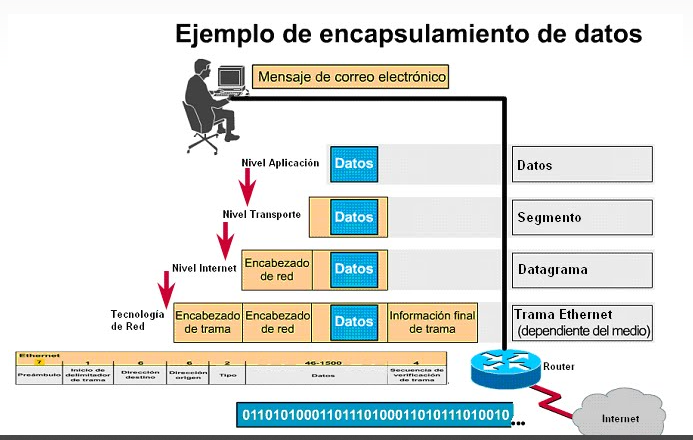


El **modelo** **OSI sirve solo como fundamento teórico** para la interconexión de sistemas abiertos, basándose en un conjunto de siete capas. Cada capa cumple funciones específicas requeridas para comunicar dos sistemas mediante una estructura jerárquica. Cualquiera de sus siete capas se apoya en la capa anterior, realiza su función y ofrece un servicio a la capa superior.

El **modelo TCP/IP (Protocolo para el Control de Transmisión/ Protocolo de Internet)**, Figura 2, **es el usado realmente hoy en día,** está compuesto por cuatro capas, en la que cada una se encarga de determinados aspectos en la comunicación y a su vez cada una brinda un servicio específico a la capa superior.



**Encapsulamiento:** Unidades de información intercambiadas por las distintas capas, según va bajando de capa, cada capa le añade su propia cabecera. Una vez en destino, se desencapsula según sube de capa, para llegar de nuevo a la capa de aplicación del receptor.

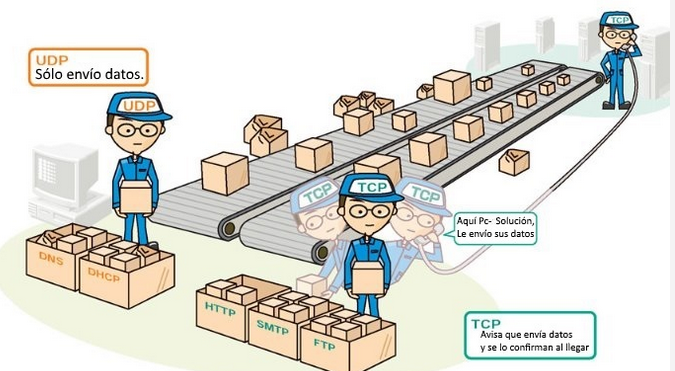


###### *Capa de Transporte*

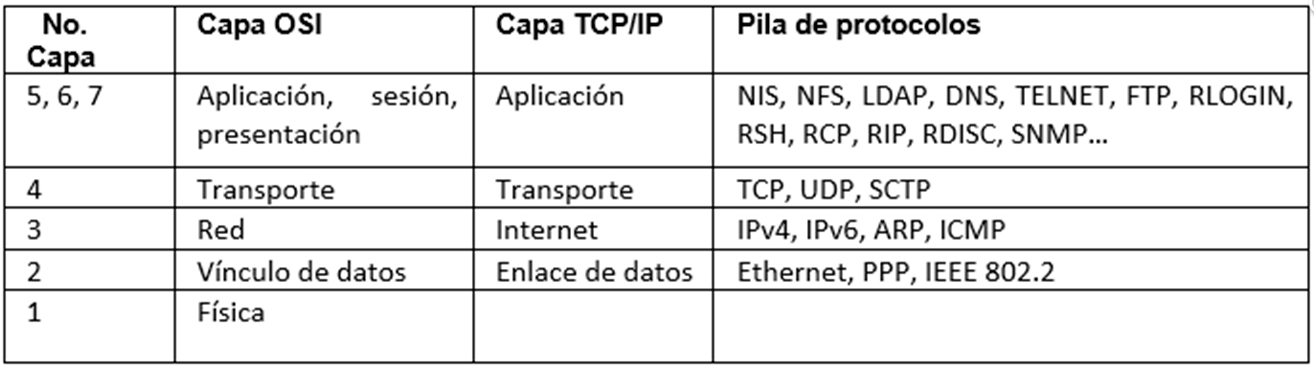
En esta capa se establece **una conexión lógica entre el host transmisor y el host receptor**. Los protocolos de transporte **segmentan los datos en el host origen** para que las capas inferiores realicen el envío y una vez que estos llegan a su **destino**, son **ensamblados** para **recuperar el mensaje original**, brindando de esta manera un transporte de extremo a extremo.

En lo que se refiere al modelo TCP/IP, los protocolos encargados del transporte de datos son dos: **TCP** (Transmission Control Protocol: Protocolo de Control de la Transmisión) **y UDP** (User Datagrama Protocol: Protocolo de Datagramas de Usuario), ambos protocolos trabajan de forma muy diferente y están orientados a distintos usos.

Una de las diferencias es que **TCP es un protocolo orientado a la conexión**, ya que establece una conexión de extremo a extremo entre ordenadores antes de transferir los datos. Por otro lado, **UDP es un protocolo sin conexión** ya que no determina la conexión antes de enviar los datos.



En la Figura 3 se muestra la **comparativa entre las capas del modelo OSI y TCP/IP** en la cual enumera las capas desde la capa superior (Aplicación) hasta la capa inferior (Red física):



*Figura 3. Comparativa de capas de Modelo OSI y TCP/IP*