Tema 5°: INTRODUCCIÓN A LAS REDES DE ÁREA LOCAL

1. *Concepto y características de las LAN.*
2. *Tecnologías de LAN.*
3. *Acceso al medio*
4. *Estándares del IEEE*
5. *Protocolos de nivel superior para LAN*

5.1.- Concepto y características de las LAN.-

Conectar entre sí dos o más ordenadores es permitir compartir la información y los recursos. Las Redes Locales permiten unir físicamente un número indeterminado de ordenadores para compartir recursos (impresoras, discos duros, escáneres, CDROM, etc.) y aplicaciones. El hecho de compartir hardware y software conlleva el consiguiente ahorro del coste total de la instalación.

Análogamente, una Red Local permite la compartición de ficheros y copias de seguridad, ya que se pueden asignar servidores dedicados a estos menesteres y realizar la transferencia a través de la red. Una red facilita las siguientes utilidades:

- Compartir hardware
- Compartir software
- Compartir Datos
- Permitir la comunicación entre usuarios.

Entre los principales argumentos de conveniencia que aconsejan la utilización de una Red de Área Local se encuentran los siguientes:

- **Razones económicas**.- Poder compartir periféricos evita la necesidad de que cada nodo de la red tenga todos los recursos instalados localmente, lo que multiplica su número y encarece significativamente los costes. Cuando alguien necesita imprimir, puede hacerlo por su impresora local, si la tiene, o mediante una impresora corporativa para toda la red, con características apropiadas al tipo de trabajo de impresión.

- **Compartición de datos**.- En el desarrollo de la tarea propia de cualquier organización es imprescindible compartir los datos que se generan en las distintas etapas del proceso. Es preciso, por tanto, un sistema en el que los distintos usuarios de la red intercambien sus datos, con el fin de facilitar la cooperación entre ellos.

- **Creación de sistemas de información distribuidos**.- En ocasiones es imposible, o cuanto menos, no es fácil que toda la información que se debe utilizar resida en el mismo ordenador, ni siquiera en la misma red. Esto lleva a la necesidad de crear sistemas distribuidos de información, que requieren enlaces seguros para el transporte de los datos desde el punto donde residen hasta el lugar donde son utilizados o procesados. Estas técnicas están muy desarrolladas en sistemas relacionales de bases de datos distribuidas.

- **Evitar redundancias inútiles de información**.- En sistemas aislados, cuando distintos usuarios utilizan la misma información, cada uno debe poseer una copia de los datos que utilizará. Al tener entonces el sistema múltiples copias no sincronizadas (una por usuario), pueden producirse desfases con relación a la información original, que impiden precisar cual de todas las copias debe tomarse por correcta. Un sistema en red, en el que únicamente se trabaja con una copia "*on line*" de los datos, impide que haya información redundante e incluso contradictoria. Además, tener múltiples copias incrementa la ocupación de los recursos de almacenamiento en disco de cualquier sistema.

- **Procesos distribuidos**.- Un sistema informático en red permite que el trabajo a desarrollar por el sistema se distribuya entre los distintos nodos que componen la red, de modo que las cargas queden balanceadas (*distribuidas*) entre todos los equipos. Además algunas tareas complejas requieren la cooperación de los distintos equipos o periféricos que pueden estar distribuidos por el sistema. Las redes, por tanto, no sólo permiten la confección de sistemas distribuidos en cuanto a los datos, sino también en cuanto a las tareas que los procesan.

- **Compartición de recursos**.- Una red permite tener recursos a disposición de los usuarios con derechos de acceso sobre aquellos. Ello permite la clasificación de los distintos periféricos por categorías, calidades, costes de utilización, rendimiento, etc. Así, un trabajo de impresión puede desviarse hacia una impresora de calidad fotográfica, de blanco y negro o de color, o de borrador, en función de la calidad requerida para el documento impreso.

- **Simplificación de la gestión de los sistemas**.- Tener la posibilidad de centralizar información o procedimientos facilita la administración y la gestión de los equipos. En la mayor parte de las Redes de Área Local se pueden administrar todos los equipos de la red desde un solo puesto o ***consola de red***, se puede tener un único sistema de cuentas de acceso, un único gestor de derechos de usuarios, etc.

- **Trabajo corporativo**.- La Red de Área Local permite la integración de los procesos y datos de cada uno de los usuarios en un sistema de trabajo corporativo (*workflow*). Esto permite la automatización de las tareas y del flujo de datos en cada una de las fases, así como el control del estado en el que se encuentran cada una de las tareas que lo componen. Se requieren, por tanto, capacidades en los nodos de la red para el intercambio de datos entre los distintos servidores o puestos y entre las distintas tareas que corren en los distintos ordenadores.

Todos los puntos indicados anteriormente redundan en el beneficio económico, aunque ésta no sea la única razón por las que son convenientes las Redes de Área Local.

5.1.1.- Características esenciales de una LAN

Según la IEEE, una Red de Área Local es:

"Una red de área local se distingue de otros tipos de redes de datos en que las comunicaciones están normalmente confinadas a un área geográfica limitada, tal como un

edificio de oficina, un almacén o un campus; utilizando un canal de comunicación de velocidad moderada o alta y una tasa de error baja".

De la definición de LAN, se deduce claramente que sus elementos esenciales son: ***ámbito***, ***seguridad*** y ***velocidad***.

Los componentes de una Red de Área Local dependerán si son componentes software o hardware, según la distribución:

Software de red	Hardware de red
Topología Lógica	Topología Física
Protocolos	Servidor
Sistema de Transporte de Datos	Estaciones
Sistemas Operativos	Medios de transmisión y conectores
Programas de aplicación o de utilidad	Tarjetas Controladoras de red

Siendo estos componentes:

Servidor: Es una computadora de la red que tiene la capacidad de compartir recursos. Los servidores pueden ser clasificados en **dedicados** y **no dedicados**.

- **Servidor no dedicado:** Es aquel que además de compartir recursos o información también puede ser utilizado como una computadora cualquiera. Este tipo de servidores son comunes en redes pequeñas donde el trabajo de los servidores no es extenuante.

- **Servidor dedicado:** Son servidores exclusivamente para la comparición de información y recursos. Suelen ser computadoras grandes y costosas. Suelen utilizarse en redes grandes donde el trabajo de administración de usuarios, aplicaciones, información, recursos, etc., requiere especial atención.

Medio de conexión y conectores: Son los medios físicos que permiten la conectividad, pueden ser: cables metálicos u ópticos, ondas de radio, rayos infrarrojos, etc.

Tarjetas controladoras de red: Son los dispositivos que permiten la transmisión y recepción de datos entre estaciones.

Protocolos: Un protocolo es un conjunto de normas que rigen la comunicación entre las computadoras de una red. Estas normas especifican que tipo de cables se utilizarán, que topología tendrá la red, que velocidad tendrán las comunicaciones y de que forma se accederá al canal de transmisión.

Estación de trabajo: Son aquellas computadoras de la red que no comparten recursos. Muchas veces también reciben el nombre de clientes.

Sistema Operativo: Su función es el manejo de datos, y administrar la capacidad del disco duro, periféricos, memoria y comunicaciones de una computadora.

Programas de aplicación: Son todos aquellos programas que incluye la red tales como: correo electrónico, impresión, administrador de archivos, configuración de la red, etc.

Las características diferenciadoras de una Red de Área Local serán:

- Los canales de transmisión suelen ser de ***multiacceso***. Los nodos utilizan un único canal para comunicarse con el resto de los equipos que componen la red. Todos los paquetes de red, que los nodos ponen en el canal, son enviados indistintamente al conjunto de los nodos de la red o bien a subconjuntos concretos de estos equipos.

- Las líneas de comunicación suelen ser ***multipunto***, a diferencia de las redes WAN en las que la conexión suele ser punto a punto a través de centrales de conmutación o equipamientos de funcionalidad semejante.

- El tipo de red ***depende del tipo de cableado***. El cableado apropiado para redes en el acceso a una red WAN (p.e. cable telefónico) no tiene la calidad requerida para cumplir las especificaciones de velocidad en una Red de Área Local.

- El tipo de red también depende de la ***topología de la red*** y de los ***protocolos utilizados*** (si bien, cada vez las LAN se determinan menos por los protocolos, sobre todo desde la popularización de la tecnología Internet, válida tanto para WAN (*Internet*) como para LAN (*Intranet*)). Las Redes de Área Local admiten cualquier topología, mientras que las redes WAN suelen ser mallas de nodos y centrales conmutadoras. Difícilmente, una red en anillo puede constituir el núcleo de una gran red de área extensa (los anillos mas grandes no pueden superar los 200 kilómetros de diámetro).

En resumen, la topología influye en gran medida en el tipo de red. Aunque existe una gran diversidad de topologías y de protocolos, no se generan todas las combinaciones posibles entre ellas. La conjunción de una topología y un protocolo (o una familia de protocolos) da lugar a una tecnología concreta de red. Tecnologías que se estudiarán a continuación.

5.2.- Tecnologías de LAN.-

Las redes locales LAN son redes pequeñas, caracterizadas por una determinada velocidad de transmisión conocida de antemano. Además tienen una topología y una tecnología de transmisión propia.

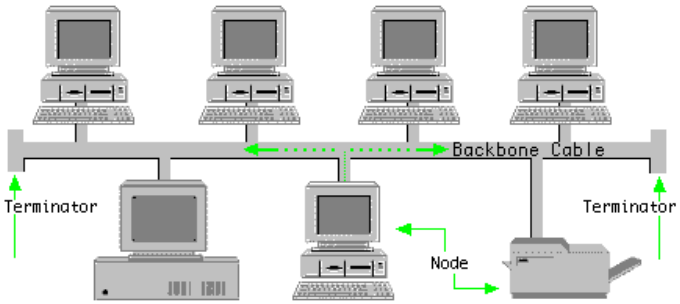
Por **topología de red** se entiende *la forma física de conectarse dos o mas equipos en la red*. Está en función de la forma física en que se realiza el cableado de la red por el que circula la información.

La topología de una red es, pues, el modo en el que se conectan los distintos elementos que configuran la red. Los tipos de topologías que se pueden encontrar en una red local son:

- Topología en bus
- Topología en anillo
- Topología en estrella
- Topología en árbol
- Etc.

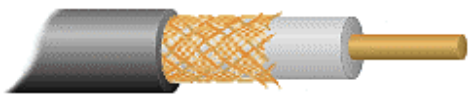
Topología en Bus

La **topología en bus** es la mas sencilla de instalar; está formada por un único cable principal que conecta todos los ordenadores entre sí, permitiéndose la comunicación en ambos sentidos. No se requieren dispositivos altamente especializados para realizar las conexiones físicas entre los nodos y todos los equipos que se conectan a la red lo hacen mediante componentes pasivos o que no necesitan excesiva electrónica.



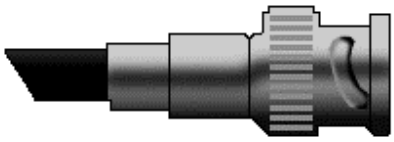
El medio de transmisión que forma la red es un único bus multiacceso compartido por todos los nodos, debiéndose establecer una **contienda** para determinar quien tiene los derechos de acceso a los recursos de comunicación en cada instante. Este sistema de contienda determina el tipo de red. Así, una red en *bus* con sistema de contienda ***CSMA/CD*** es la red IEEE 802.3 o **Ethernet**; una red en *bus*, con sistema de contienda por ***paso de testigo*** es la red IEEE 802.4 o **Token bus**.

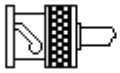
El cable normalmente utilizado para esta topología es el *cable coaxial* RG58U; es un cable de 50 Ω de impedancia característica.



Con el fin de evitar ecos o reflexiones no deseadas que perjudiquen lasa condiciones eléctricas de la transmisión, en los extremos de la red es preciso colocar ***terminadores de red***. Éstos son resistencias de 50 Ω colocadas al final del bus para adaptar las impedancias y así evitar que las reflexiones impliquen pérdida de información.

El bus tiene una estructura lineal, utilizándose ***terminales en T*** y conectores ***BNC*** para establecer la red.



	Macho	Hembra	
BNC			

La distancia entre ordenadores debe ser superior a $\frac{1}{2}$ metro, siendo la longitud máxima de la red 185 metros, y estando formada ésta por 30 ordenadores. Para mayores distancias o para la conexión de mas terminales es preciso utilizar ***repetidores***.

La ruptura del bus impide totalmente la comunicación entre cualesquiera dos nodos de la red. La red en bus no depende de las máquinas conectadas, pero depende totalmente del cableado. Es, pues una topología muy sensible a la ruptura del cable o a problemas de conexiones entre los nodos de la red. Por lo que es conveniente que los cables de datos estén protegidos.

Topología en anillo

Con esta topología se conectan todos los equipos formando un bucle cerrado. La información circula en una única dirección a lo largo del anillo.

El rendimiento de una red en anillo es superior a una red *Ethernet*, porque utiliza protocolos de nivel de enlace para acceso al medio libres de colisiones, en concreto, el método de ***paso por testigo***.

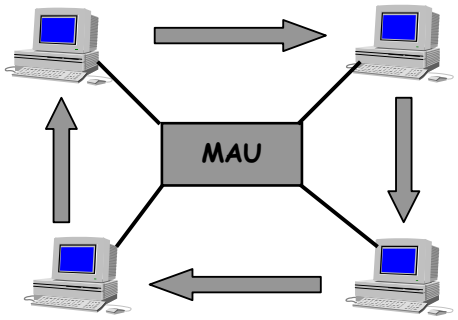
Para conseguir un adecuado funcionamiento del anillo que forma la red, se necesitan elementos electrónicamente activos que encarecen sensiblemente la instalación, frente a otras redes de semejantes prestaciones.

La red en anillo mas extendida es la diseñada por IBM llamada ***Token Ring***. Tiene una estructura muy parecida a la del estándar IEEE 802.5.

Las señales recorren el anillo a la velocidad de la luz en el medio de transporte y requieren ***retardadores*** para evitar que unos bits se superpongan a otros. La transmisión, en una red en anillo es secuencial y, por tanto, es posible que cuando una estación quiera poner en la red el bit siguiente, todavía no se haya terminado de transmitir el anterior. También son necesarios elementos *direccionalmente selectivos* para conseguir que la transmisión de bits se produzca en un único sentido del anillo, ya que si la transmisión se produjera en ambos sentidos del anillo (como ocurre en una red Ethernet en el bus), se producirían interferencias entre cada bit y el siguiente.

Como consecuencia de todo lo expuesto, puede deducirse que el anillo no es simplemente un bus cerrado por sus extremos, sino que requiere una tecnología electrónica completamente diferente, esto es, no existe sólo diferencias topológicas.

El dispositivo encargado de realizar físicamente el anillo se llama **MAU** (*Multistation Access Unit*) y no es mas que un concentrador especializado para este tipo de redes al que se conectan las estaciones.



Este hardware tiene una serie de componentes de conmutación que crean un nuevo anillo cada vez que conecta una nueva estación como segmento de la estrella, como indica la figura.

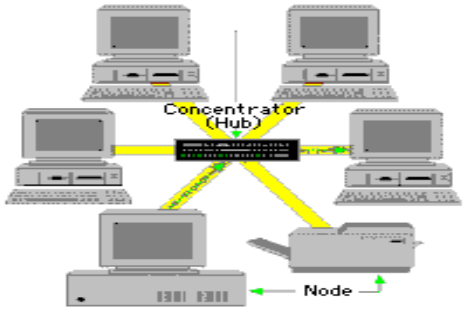
Si el anillo no llega a romperse pero se produce una mala conexión del equipo terminal con el mismo, disminuye considerablemente el rendimiento de la red, debido a problemas de reflexiones de la señal y la modificación de otros parámetros eléctricos.

El cableado típico para una red en anillo *Token Ring* es el par trenzado STP. Otras redes en anillo pueden utilizar otros tipos de cable, por ejemplo, la red FDDI (*Fiber Optics Data Distributed Interface*) utiliza como medio de transmisión un anillo de fibra óptica.

En el caso de la red Token Ring, la longitud máxima de la línea que une la estación con la MAU es de 45 metros para un cable STP.

Topología en estrella

La **topología en estrella** las estaciones se conectan entre sí a través de un nodo especialmente privilegiado que ocupa la posición central de la red formando con el resto de las estaciones una estrella. A este nodo se le denomina **estación concentradora** (***HUB***) de la estrella.



La ventaja fundamental de una red en estrella reside en la seguridad. El **concentrador** tiene funciones tanto de *intercomunicador* entre cualesquiera dos estaciones, como de *aislador* de los problemas que pudieran surgir en algunos segmentos. El fallo en uno de los ordenadores o de su cableado, no afecta al resto de la red, siendo muy sencillo el mantenimiento y la ampliación.

El funcionamiento de una red en estrella se fundamenta en el concentrador. Éste da turnos al resto de los equipos para que puedan utilizar la red. Estos equipos están unidos individualmente con el concentrador, de forma que se requiere gran cantidad de cableado. Así, si se compara con una red en bus, si se incrementa 10 metros la distancia de cada nodo de la red al concentrador, en una red de 50 puestos, se necesitarán 500 metros mas de cable.

Puesto que a cada nodo le llega un único cable de red, las conexiones suelen ser mas limpias que en el cableado en bus. Sin embargo, el problema de la topología en estrella se presenta en el entorno del concentrador, ya que todos los segmentos deben terminar en él, produciendo una importante madeja de cables.

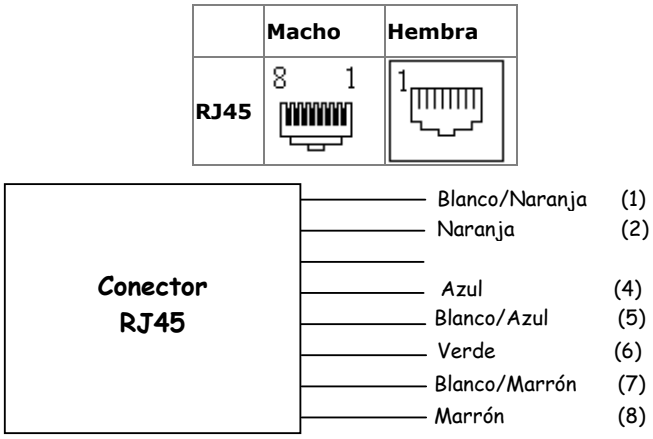
La distancia máxima entre una estación y el concentrador es de unos 100 metros, utilizándose normalmente en los concentradores conectores RJ45, aunque opcionalmente suelen también tener conectores BNC.

Con el concentrador se puede ampliar la red de forma indefinida, siendo las caídas de red puntuales y nunca del sistema.

El cable que normalmente se utiliza para implementar una red en estrella es el par trenzado de cuatro pares de conductores y categoría 5, para así poder prevenir posibles ampliaciones a 100 Mbps. Este tipo de cable UTP tiene ocho colores para identificar los pares de conductores, siendo el segundo conductor el que indica el grupo del par

Pares (Cable Par Trenzado)	
Blanco/Naranja	Naranja
Blanco/Verde	Verde
Blanco/Azul	Azul
Blanco/Marrón	Marrón

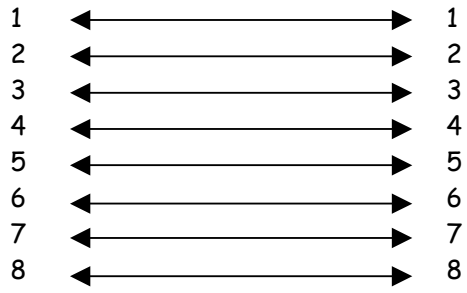
Los hilos se introducen en el conector RJ45 según el siguiente orden:



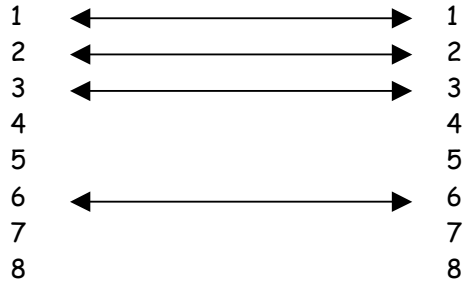
El cable normalmente utilizado suele ser cable par trenzado de 8 hilos y categoría 5, tanto sin apantallar (UTP) como apantallado (STP). Este cable permite una velocidad máxima de 100 Mbps.

Para **tarjetas Ethernet 10 base T**, las conexiones son:

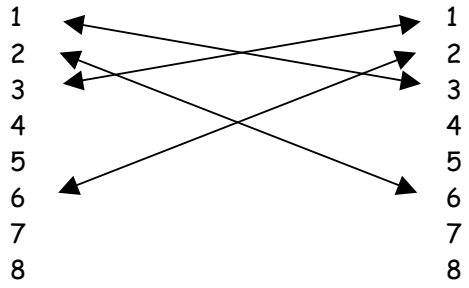
- Si se usa un cable de 8 conductores, la conexión completa es:



- Si se usa una conexión mínima:



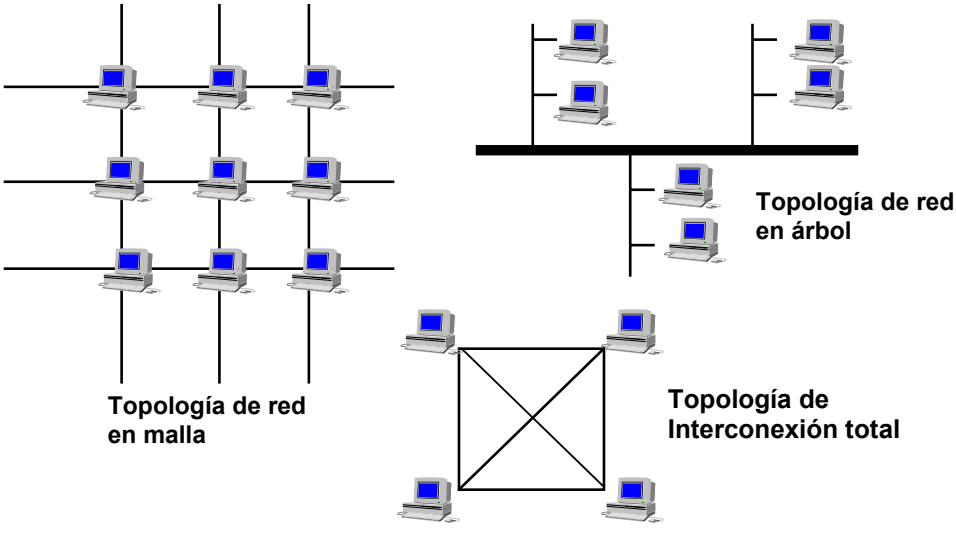
- Si se usa una conexión directa entre dos ordenadores:



Por último, para tarjetas **Ethernet 100 base T**, si se usa un cable de ocho conductores, la conexión completa es:

Otras topologías de red

En ocasiones, y pàra aplicaciones muy específicas, se utilizan topologías mas sofisticadas que permiten conexiones múltiples entre distintos equipos:



- **Topología en malla**.- Se trata de construir una malla de cableado situando los nodos de la red en las intersecciones de la malla. De este modo, cada nodo está siempre conectado mediante líneas punto a punto con cualquier otro nodo abyacente.

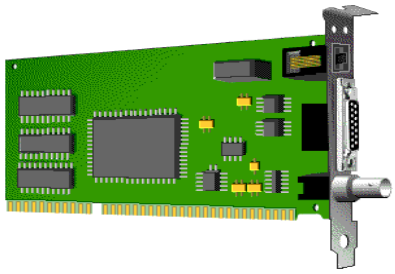
- **Topología en árbol**.- Es una extensión de la topología en bus. Consiste en la conexión de distintos *buses lineales* (ramas) a un nuevo *bus troncal* del que se reparte la señal hacia las ramas. Esta topología es muy utilizada en la distribución de señal de televisión por cable, en donde el troncal suele estar constituido por fibra óptica y las ramas por cables coaxiales.

- **Topología de interconexión total**.- Consiste en conectar todos los ordenadores de una red entre sí a través de líneas punto a punto. Esta topología es muy poco utilizada por la gran cantidad de recursos que son necesarios, aunque se considere la mas segura.

- **Topologías mixtas**.- En este caso, la topología de la red es una mezcla de las topologías básicas estudiadas anteriormente. Es la topología mas común en redes medias y gransdes, debido a que describeel crecimiento natural de una red en una organización.

Tarjetas controladoras de Red (NIC)

La tarjeta de red (NIC) es el dispositivo que conecta físicamente al ordenador a la red. Son tarjetas que se insertan en la computadora como si de una tarjeta de vídeo se tratase o cualquier otra tarjeta. Puesto que todos los accesos a red se realizan a través de ellas se deben utilizar tarjetas rápidas para comunicaciones fluidas.



El tipo de **NIC** conectado en cada computadora determina la topología física que debe ser utilizada.

Por otro lado, la mayor parte de las tarjetas de red requieren la configuración del nivel de interrupción (**IRQ**) y la dirección base, cuyos valores van de acuerdo a la configuración de la computadora donde se coloquen.

Otros dispositivos de red:

Concentradores (HUB).- En una red, dependiendo de sus necesidades de crecimiento y de su topología, es posible a veces encontrar dispositivos especiales que juegan papeles importantes, entre los cuales es posible hallar. Los concentradores son dispositivos que permiten conectar una red de tipo estrella a uno o varios usuarios con cableado UTP 10 base T Ethernet y con conectores RJ-45.

Un concentrador o **Hub** es un elemento que *provee una conexión central para todos los cables de la red*. Los hubs son "cajas" con un número determinado de conectores, habitualmente RJ45 más otro conector adicional de tipo diferente para enlazar con otro tipo de red. Puede ser de tipo **inteligente** que envían la información solo a quien ha de llegar mientras que los normales envían la información a todos los puntos de la red siendo las estaciones de trabajo las que decidirán si se quedan o no con esa información. Están provistos de salidas especiales para conectar otro Hub a uno de los conectores permitiendo así ampliaciones de la red.

Repetidores.- Cuando una señal viaja a lo largo de un cable va perdiendo "fuerza" a medida que avanza. Esta pérdida de fuerza puede desembocar en una pérdida de información.

Los repetidores *amplifican la señal que reciben permitiendo así que la distancia entre dos puntos de la red sea mayor que la que un cable solo permite*. Existen dos tipos de repetidores, que son los pasivos y los activos.

El repetidor activo tiene alimentación externa mientras que el pasivo no la tiene. Un repetidor activo permite que los cables logren mayores distancias que los pasivos. En la gran mayoría de las veces no se recomienda el uso de dos repetidores pasivos de forma simultánea en la trayectoria de un cable.

Módems.- El módem es otro de los periféricos que con el tiempo se ha convertido ya en imprescindible y pocos son los modelos de ordenador que no estén conectados en red que no lo incorporen. Su gran utilización viene dada básicamente por dos motivos: Internet y el fax, aunque también tiene otros usos como son su utilización como contestador automático incluso para conexión con la red local de una oficina específica o con la central de la empresa.

Aún en el caso de estar conectado a una red, ésta tampoco se libra de éstos dispositivos, ya que en este caso será la propia red la que utilizará el módem para poder conectarse a otras redes o a Internet estando en este caso conectado a nuestro servidor o a un router.

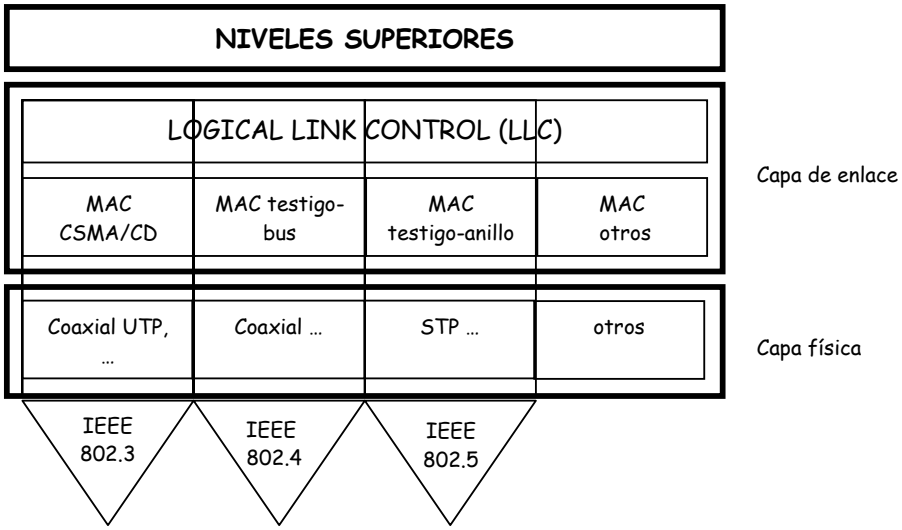
Los módem se utilizan con líneas analógicas, ya que su propio nombre indica su principal función, que es la de modular-demodular la señal digital proveniente de nuestro ordenador y convertirla a una forma de onda que sea asimilable por dicho tipo de líneas. Es cierto que se suelen oír expresiones como módem ADSL o incluso módem RDSI, aunque esto no es cierto en estos casos, ya que estas líneas de tipo digital no necesitan de ningún tipo de conversión de digital a analógico, y su función en este caso es más parecida a la de una tarjeta de red que a la de un módem.

5.3.- Acceso al medio.-

Una Red de Área Local (LAN) puede implementarse según diversas topologías. Para todas ellas es necesario establecer mecanismos para gestionar la información que entra y sale de las líneas de transmisión. El **acceso al medio** consiste pues en el establecimiento de una política o algoritmo que permita a las estaciones acceder y compartir un medio de transmisión (dispositivo MAU, HUB, switch. Etc.) de forma ordenada y coherente.

La IEEE ha propuesto varias normas relativas a Redes de Área Local. El conjunto de estas normas se conoce como las **normas IEEE 802**. Posteriormente han sido aceptadas por otras asociaciones de normas nacionales (ANSI) o internacionales (norma ISO 8802).

Estas normas incluyen varios ***tipos de acceso al medio*** (subcapa inferior del nivel de enlace) como son el **CSMA/CD**, el acceso por **paso de testigo en bus** y el acceso por **paso de testigo en anillo**. Estas tres técnicas de acceso, definidas por los estándares ***IEEE 802.3***, ***IEEE 802.4*** e ***IEEE 802.5*** respectivamente difieren en la capa física y en la subcapa de acceso al medio, sin embargo son totalmente compatibles en la subcapa superior de la capa de enlace, ya que las tres utilizan el protocolo ***LLC*** (Logical Link Control), protocolo derivado del ya conocido HDLC.



La norma IEEE 802.1 define las primitivas del *interface* entre las capas y proporciona una introducción a todo el conjunto de normas IEEE 802.2. Por su parte, IEEE 802.2 hace una descripción de la subcapa superior del nivel de enlace y, por tanto, del protocolo **LLC**.

LLC está construido de modo que su funcionamiento sea independiente del método de acceso que tenga la red al medio de transmisión. Además sirve como *interface* con las capas superiores. Por lo tanto, las principales funciones del protocolo LLC serán las siguientes:

- **Habilitar la transferencia de datos** entre la capa de red (pro ejemplo procedente del protocolo IP) y la subcapa de acceso al medio (MAC)

- **Controlar el flujo de datos**, mediante la utilización de operaciones semejantes a las utilizadas en el protocolo HDLC, utilizando, por ejemplo, tramas RR, RNR, etc.

- **Efectuar conexiones para los servicios orientados a la conexión**, utilizados entre aplicaciones situadas en distintos puntos de la red. Estas conexiones se efectuan poniendo a ,los distintos nodos en el modo *asíncrono balanceado*.

- **Configurarse, de modo mas simple, como un protocolo sin conexión**, utilizando las tramas no numeradas de información (trama **UI** o *Unnumbered Information*)

Los distintos tipos de servicios de la capa de enlace se configuran como *asociaciones de primitivas OSI* (*.request, .indication, .response, . confirm*) considerando cuatro tipos de servicio en el protocolo LLC:

- **Tipo 1**.- *Servicio sin conexión y sin confirmación*. Todas las redes 802 deben proveer este tipo de servicio. Al ser un servicio sin confirmación carece de control de flujo y de control de errores. Este servicio sólo podrá ser utilizado por aplicaciones de red en las que la seguridad no sea crítica.
- **Tipo 2**.- *Servicio orientado a la conexión*. Es un servicio completo, con corrección de errores y con control de flujo.
- **Tipo 3**.- *Servicio sin conexión y con confirmación*. Este tipo de servicio no realiza una conexión , pero provee confirmación de las unidades de datos recibidas. Por tanto, se trata de un servicio rápido en el inicio de la comunicación (al no tener conexión), pero con las debidas garantías de seguridad.
- **Tipo 4**.- *Es la combinación, en un único servicio, de los tipos 1º, 2º y 3º*, dependiendo de las necesidades de comunicación en cada momento. Se trata, pues de un servicio mixto.

La norma 802.2 describe las primitivas de la tabla siguiente:

Servicio	Primitiva	Significado
Sin conexión	DL_UNITDATA.request DL_UNITDATA.indication	Transferencia de datos
Orientado a la conexión	DL_CONNECT.request DL_CONNECT.indication DL_CONNECT.response DL_CONNECT.confirm	Solicitud de conexión
Orientado a la conexión	DL_DAT.request DL_DAT.indication	Transferencia de datos
Orientado a la conexión	DL_CONNECTION_FLOWCONTROL.request DL_CONNECTION_FLOWCONTROL.indication	Acción de control de flujo
Orientado a la conexión	DL_RESET.request DL_RESET.indication DL_RESET.response DL_RESET.confirm	Solicitud de *Reset*
Orientado a la conexión	DL_DISCONNECT.confirm DL_DISCONNECT.indication	Solicitud de desconexión

Además se definen tres primitivas para la comunicación con la capa MAC: ***MA_UNITDATA.request***, ***MA_UNITDATA.indication***, para el paso de datos y la ***MA_UNITDATA_STATUS:indication***, para el análisis del éxito de la transferencia.

5.4.- Estándares del IEEE

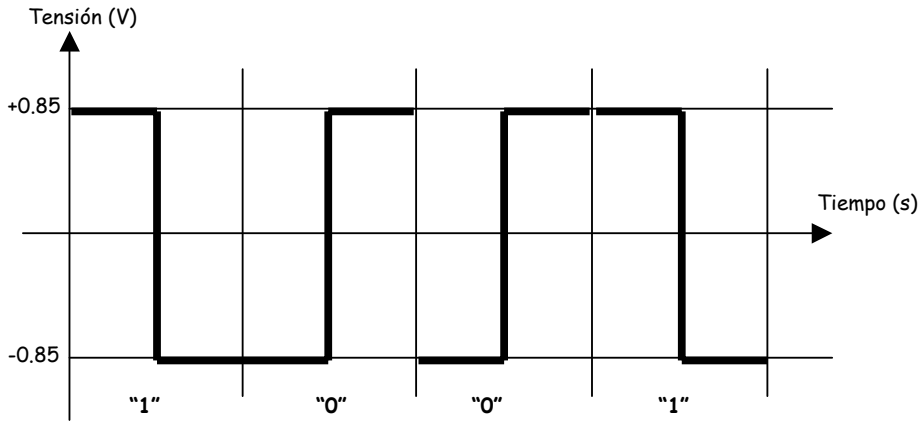
5.4.1.-Estándar IEEE 802.3 (Ethernet)

La norma IEEE 802.3 establece el protocolo **CSMA/CD**. Para la transmisión utiliza el cable coaxial y el par trenzado con velocidades de hasta 100 Mbps. Los estándares propuestos coinciden con las especificaciones de la arquitectura Ethernet.

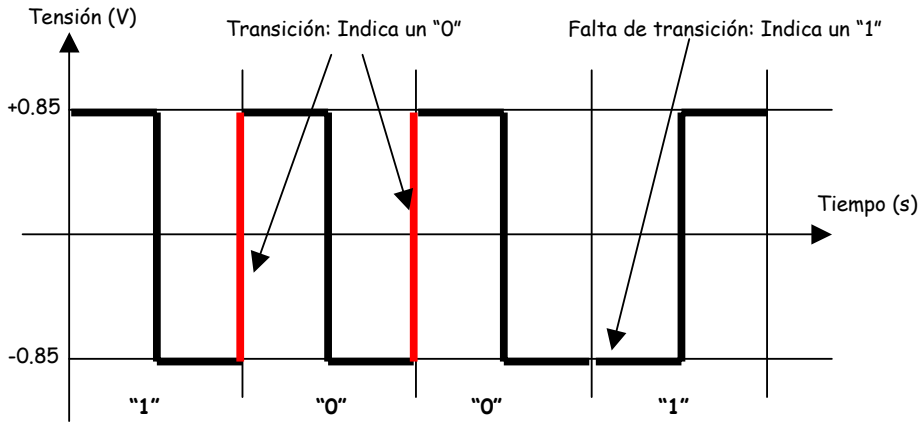
En el nivel físico, ninguna de las versiones de la IEEE 802.3 utilizan codificación binaria directa asignando 0 voltios al bit "0" y 5 voltios al bit "1" ya que conduce a ambigüedades (por ejemplo, si se envía la cadena 0001000 podría interpretarse falsamente como 1000000 o 0100000 dado que no se puede distinguir entre un transmisor inactivo- 0 voltios – y la emisión de un bit "0" – 0 voltios -).

Algunos mecanismos que determinan sin ambigüedades el comienzo, final o la mitad de cada bit sin hacer referencia a un reloj externo son la **codificación Manchester** y la **codificación Manchester diferencial.**

En la codificación Manchester, cada periodo de bit se divide en dos intervalos iguales. Un bit binario "1" se envía teniendo el voltaje alto durante el primer intervalo y bajo durante el segundo. Por su parte, el bit binario "0" es justamente lo inverso: primero bajo y después alto. Este esquema asegura que cada periodo de bit tiene una transición a la mitad facilitando que el emisor se sincronice con el receptor. Una desventaja del código Manchester es que requiere el doble del ancho de banda que la codificación binaria directa



Para evitar este incremento en el ancho de banda se utiliza la codificación **Manchester diferencial**, en ella, un bit "1" se indica mediante la ausencia de una transición en el inicio del intervalo y el bit "0" mediante la presencia de una transición al inicio del intervalo. Em ambos casos también existe una transición a la mitad. El esquema diferencial requiere un equipo mas complejo pero ofrece una mayor inmunidad al ruido.



Para cualquiera de las dos codificaciones, en cualquier instante, el cable puede estar en alguno de los tres estados posibles:

- **Transmisión de un cero lógico**.- Un cero lógico está constituido por una señal de -0.85 voltios seguida de otra señal de +0.85 voltios

- **Transmisión de un uno lógico**.- El uno lógico es la inversión del cero lógico, por tanto es una señal de +0.85 voltios seguida de otra señal de -0.85 voltios.

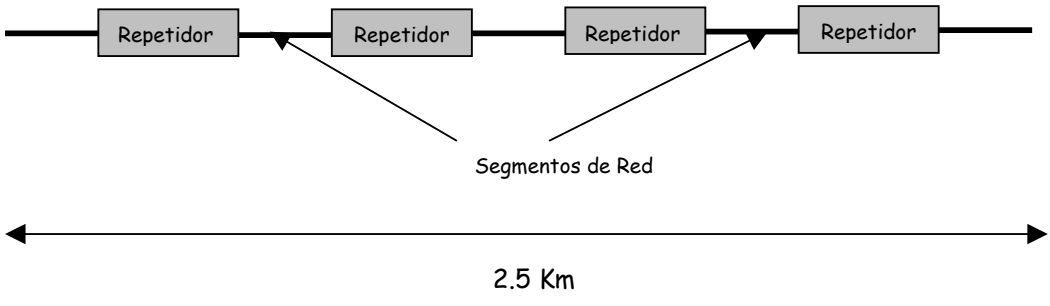
- **Canal inactivo**.- Sin transmisión; se caracteriza por mantener el canal a 0 voltios.

Cualquier estación conectada a una red IEEE 802.3 debe poseer una **tarjeta de red** con los componentes electrónicos y el software adecuado para la confección y recepción de tramas. La tarjeta debe contener un **transceptor** o dispositivo encargado de la detección de la portadora y el gobierno de las colisiones.

La tarjeta de red contiene un **controlador**, encargado de verificar las tramas que llegan desde el canal, así como de ensamblar los datos de información, dándoles la forma de una trama, calculando los códigos de redundancia cíclica, etc.

La tarjeta es también la encargada de negociar los recursos que necesita con el sistema operativo del ordenador en el que se instala.

La longitud máxima para el bus en el que se basa una red IEEE802.3 es de 500 metros, sin embargo, es posible conectar varios segmentos a través de dispositivos especiales llamados repetidores:



El repetidor opera en la capa física y se encarga de *amplificar* (realmente lo que hace es *regenerar*) la señal eléctrica, para que su amplitud sea la adecuada y llegue correctamente a los posibles receptores. Hay una limitación en la longitud total del bus (incluyendo la configuración con repetidores): *dos transceptores no pueden distanciarse mas de 2.500 metros. Además, entre dos transceptores cualesquiera no puede haber un camino de red con mas de cuatro repetidores.*

El modo en que las tramas son puestas en el medio físico de transmisión depende de las especificaciones de hardware y de los requerimientos del tipo de cableado elegido. Se definen entonces distintos subestándares, todos ellos integrados en la IEEE 802.3 que especifican el tipo de conector y de cable que es preciso para alcanzar los rendimientos previstos, utilizando siempre el método CSMA/CD. Algunos de estos subestándares son:

- **10 Base 5 o Ethernet Grueso**.- Es la especificación original de Ethernet y utiliza cable coaxial grueso para transporte de las señales en banda base, utilizando **derivaciones vampiro** para las conexiones.

- **10 Base 2 o Ethernet delgado**.- También es especificación original para Ethernet. Utiliza cable coaxial fino (en concreto RG-58 de 50 Ω de impedancia) y conectores BNC para transmisiones hasta 10 Mbps.

- **10 Broad 36**.- Define un estándar para cable coaxial en banda ancha. Apenas se utiliza en la actualidad.

- **10 Base T**.- Utiliza cable par trenzado UTP para producir transmisiones de hasta 10Mbps. Configura la red Ethernet como una *estrella*.

- **100 Base T**.- Es semejante al 10 Base T, pero con velocidades hasta 100 Mbps utilizando cable UTP de categoría 5.

- **1000 Base T**.- En este caso las comunicaciones siguen la normativa Ethernet, pero con velocidades de 1000 Mbps. Necesita cables superiores al UTP de categoría 5 (por ejemplo categoría 5 mejorada) y las distancias de cable deben ser mucho mas reducidas. Es la base de la tecnología ***Gigabit Ethernet***.

En cuanto a las **tramas**, un marco IEEE 802.3 se compone de los siguientes campos:

- **Preámbulo**.- Este campo tiene una extensión de siete bytes que siguen la secuencia "**10101010**", semejante a la bandera señalizadora del protocolo HDLC. Cuando esta secuencia se codifica en Manchester diferencial, se genera una onda cuadrada (digital y discreta) de 10 MHz de frecuencia que dura 5.6 microsegundos. Este es el tiempo que dispone el receptor para sincronizarse con el reloj del emisor.

- **Inicio**.- Es un campo de un byte con la secuencia "**10101011**" que indica que comienza la trama. En el final de la secuencia aparecen dos unos seguidos, por lo que se genera una

señal cuadrada de 20 MHz de frecuencia. Por tanto un receptor reconoce el comienzo de trama cuando escucha un preámbulo de 10 MHz seguido de una señal de 20 MHz.

- **Dirección de destino**.- Es un campo de 2 o 6 bytes que contiene la dirección del destinatario. Aunque la norma permite las dos longitudes para el tamaño de este campo, la utilizada en la red de 10 Mbps es la de 6 bytes. Esta dirección puede ser **global** o **local**.

  Es ***local*** cuando la dirección sólo tiene sentido dentro de la propia red y suele estar asignada por el administrador de la red.

  Una dirección ***global*** (dirección MAC o dirección Ethernet) es única para cada tarjeta de red, normalmente codifica la *compañía constructora de la tarjeta* y el *número de serie*. El bit de mayor orden de este campo, que ocupa el lugar 47, codifica si la dirección de destino es un único destinatario (bit puesto a 0) o si representa una dirección de grupo (bit puesto a 1).

  Una ***dirección de grupo*** es una dirección a la que varias estaciones tienen derecho de escucha (transmisión de uno a varios). Cuando todos los bits del campo de dirección están a 1, se codifica una ***difusión*** o ***broadcast***, es decir, se codifica una trama para todas las estaciones de la red. El sistema sabe si se trata de una dirección local o global analizando el bit 46.

- **Dirección de origen**.- Es semejante al campo de dirección de destino, pero codifica la dirección MAC de la tarjeta que originó la trama.

- **Longitud**.- Este campo, de 2 bytes, codifica cuantos bytes contiene el campo de datos. Su valor oscila en un rango entre 0 y 1500.

- **Datos**.- Es un campo que puede codificar entre 0 y 1500 bytes, en donde se incluye la información de usuario procedente de la capa de red.

- **Relleno**.- La norma IEEE 802.3 especifica que una trama no puede tener un tamaño inferior a 64 bytes; por lo tanto, cuando la longitud del campo de datos es muy pequeña, se requiere rellenar este campo hasta completar la trama mínima de 64 bytes. Es un campo que puede, por tanto, tener una longitud comprendida entre 0 y 46 bytes, de modo que la suma total de la trama sea 64 bytes.

- **CRC**.- Es el campo, de 4 bytes en donde se codifica el control de errores de la trama, por el método de redundancia cíclica.

Preámbulo (7 bytes)	Inicio (1 byte)	Dir Destino (2o6 bytes)	Dir Origen (2o6 bytes)	Long Datos (2 bytes)	Datos (0 y 1500 bytes)	Relleno (0y46 bytes)	CRC (4 bytes)

La norma IEEE 802.3 resuelve las **colisiones** utilizando el **algoritmo de retroceso exponencial** binario cuya forma de actuación es de la siguiente manera:

Cuando se produce una colisión, las estaciones implicadas en ella interrumpen sus transmisiones, generan una señal de ruido para alertar al resto de las estaciones de la red y esperan un tiempo aleatorio para volver a retransmitir. El sistema de asignación de tiempos de espera consiste en dividir el tiempo en ranuras temporales, con un valor de 51.2 microsegundos, denominado *tiempo de ranura*. En este tiempo la red hubiera podido transmitir 512 bytes, que se hubieran desplazado 2.5 km y que coincide con la distancia máxima permitida de la red.

Después de la colisión, las estaciones generan un número aleatorio, que se resuelve como 0 o 1. Si el resultado es 0, se produce la retransmisión inmediatamente; mientras que si es 1, se espera un tiempo de ranura para efectuar la retransmisión.

Si ambas estaciones eligen el mismo número aleatorio, se producirá de nuevo otra colisión.

Tras la segunda colisión, cada máquina escoge 0, 1, 2, o 3 al azar y espera ese número de tiempos de ranura. Si se produce una tercera colisión (la probabilidad de que ello ocurra es del 25 %), la siguiente vez el intervalo de ranuras a esperar se escogerá al azar del intervalo 0 a 2^3–1.

En general, tras *n* colisiones, se escoge un número aleatorio comprendido entre 0 y 2^n-1, y se salta ese número de ranuras de tiempo. El número máximo de ranuras a esperar es 1023.

Con cada colisión se retarda la transmisión, pero la probabilidad de una nueva colisión se reduce exponencialmente, aunque tras 16 colisiones el controlador de la máquina desconecta ésta y la recuperación posterior es responsabilidad de los niveles superiores de la red .

Las **funciones de la capa MAC** se pueden agrupar del siguiente modo

- *Aceptar datos de la subcapa LLC en emisión (o pasarlos a la subcapa LLC en recepción)*
- *Calcular el CRC e insertarlo al final de la trama en emisión (y comprobarlo en recepción)*
- *Pasar la secuencia de bits que forman la trama a la capa física (o recibirlos en recepción)*
- *Insertar un campo de relleno para garantizar que la trama tiene al menos 64 bytes de longitud*
- *Detener la transmisión y generar una señal de ruido cuando se produzca una colisión*
- *Descargarse de tramas inválidas o incompletas.*
- *Retransmitir las tramas que han sufrido colisión después de aplicar el algoritmo de espera para la contienda*
- *Observar el canal en espera de que se libere, para producir una transmisión.*
- *Aceptar cualquier trama cuya dirección de destino le corresponda*

Debido a que la norma IEEE 802.3 propone un protocolo **no libre de colisiones,** hay que considerar que la probabilidad de colisión depende de muchos factores: la longitud de la trama, el número de estaciones que estén transmitiendo, sus necesidades de transmisión, etc.

Puede definirse el ***rendimiento de una red en transmisión*** *como la proporción entre la cantidad de información enviada y el ancho de banda del canal*. Es decir, si un canal tiene un

ancho de banda de 10 Mbps, un rendimiento del 100 % implica que el receptor está aceptando datos a esa misma velocidad.

5.4.2.-Estándar IEEE 802.4 (Token Bus)

Frente a la facilidad de instalación de las redes Ethernet, se opone el problema que representa, para algunas aplicaciones, el carácter probabilístico en la resolución de las colisiones, que puede producir retardos importantes en las transmisiones (una estación puede esperar un tiempo arbitrariamente largo para enviar una trama, dado que en la red Ethernet el caso mas desfavorable de colisión no está determinado). Algunas aplicaciones no soportan tales retardos, sobre todo aquellas que son críticas en el tiempo (aplicaciones en tiempo real). Por ello, la resolución de las colisiones mediante el método de paso de testigo, asociado a la topología bus dio lugar al estándar IEEE 802.4 que define una red en bus por paso de testigo (*token bus*). El testigo no es mas que una trama de control que informa del permiso que tiene una estación para usar los recursos de la red. Ninguna estación puede transmitir mientras no reciba el testigo que la habilita para hacerlo.

La red 802.4 está físicamente constituida por un bus, semejante a la red IEEE 802.3, aunque *desde el punto de vista lógico la red se organiza como si se tratase de un anillo*. Cada estación tiene un número asociado que la identifica totalmente. Cada estación conoce la dirección de la estación situada a su "izquierda" y la dirección de la estación situada a su "derecha".

El testigo es generado por la unidad con número mayor de dirección cuando se pone en marcha la red, la cual puede enviar la primera trama.

El testigo se pasa a la estación siguiente en orden descendente de numeración. Esta nueva estación recoge el testigo y se reserva el derecho de emisión.

Cuando ha terminado de transmitir lo que necesitaba o cuando ha expirado un tiempo determinado genera otro testigo con la dirección de la estación inmediatamente inferior.

El proceso se repite para cada estación de la red; de este modo todas las estaciones pueden transmitir periódicamente; es pues un sistema mas o menos complejo de multiplexación en el tiempo.

Es importante notar que *no es importante el orden físico* en el que estén conectadas las estaciones al cable. Dado que el cable, de suyo, es un medio de difusión, *todas las estaciones reciben todas las tramas* desechando las que no estén dirigidas a ellas. Cuando una estación envía el testigo, lo hace a la estación vecina *lógica*, sim importar la ubicación física de esta estación en el anillo.

Lógicamente, el protocolo de acceso al medio (MAC) de la IEEE 802.4 debe prever el modo en que las estaciones se incorporan al anillo lógico cuando sean encendidas o, por el contrario, la manera en la que se desconectan, sin interrumpir por ello el procedimiento lógico de paso de testigo.

La capa física de la red IEEE 802.4 utiliza cable coaxial de 75 Ω (cable RG59) por el que viajan señales moduladas, es decir, la red IEEE 802.4 es una red de banda ancha que modula sus señales en el nivel físico.

La norma IEE 802.4 permite la utilización de repetidores con el fin de alargar la longitud de la red, y prevé velocidades de transferencia de datos comprendidas entre 1'5 y 10 Mbps.

Debe tenerse en cuenta que aunque la estructura física de la IEEE 802.3 y de la IEEE 802.4 son semejantes, al menos desde el punto de vista topológico, las normas son ***totalmente incompatibles incluso físicamente***: ni el medio de transmisión es el mismo, ni la codificación de las señales coinciden. Ni siquiera, en un nivel superior, el formato de la trama es directamente compatible.

La trama de una red que sigue el estándar IEEE 802.4 tiene los siguientes campos:

Preámbulo (1 byte)	D.C. (1 byte)	Control (1 byte)	Dir Destino (2o6 bytes)	Dir Origen (2o6 bytes)	Datos (0-8182 bytes)	CRC (4 bytes)	D.F. (1 byte)

- **Preámbulo**.- Este campo es semejante al preámbulo de la norma IEEE 802.3, sin embargo tiene una extensión de un byte para representar la secuencia "**10101010**", semejante a la bandera señalizadora del protocolo HDLC. Cuando esta secuencia se codifica en Manchester diferencial, se genera una onda cuadrada (digital y discreta) de 10 MHz de frecuencia que dura 5.6 microsegundos. Este es el tiempo que dispone el receptor para sincronizarse con el reloj del emisor. En otras palabras, la misión de este campo, como en el caso de Ethernet, es la de sincronizar emisor y receptor aunque tiene una longitud siete veces menor.

- **Delimitador de Comienzo**.- Consiste en la emisión de una señal distinta de "1" o "0" (por tanto, una secuencia prohibida en el código binario) durante el tiempo de emisión de 1 byte. Al ser una configuración prohibida en el código binario, se tiene la garantía absoluta de que no se repite en cualquier otro punto de la trama y, en especial, en el campo de datos. Cualquier estación a la escucha conoce perfectamente que comienza la trama al leer del canal esta señal prohibida.

- **Control de trama**.- Este campo codifica en 1 byte el tipo de trama de que se trata. Así, hay tramas encargadas de transferir datos, otras de transferir el testigoa otra estación, otras cuya misión es mantener el anillo en la incorporación de nuevas estaciones, etc. Los tipos de trama considerados son los siguientes:

Campo de control de marco	Nombre	Significado
00000000	Claim…token	Reclamar el testigo durante la inicialización del anillo
00000001	Solicit…sucesor…1	Permitir que entren estaciones en el anillo
00000010	Solicit…sucesor…2	Permitir que entren estaciones en el anillo
00000011	Who…follows	Recuperación de un testigo perdido
00000100	Resolve…contention	Se utiliza cuando quieren entrar varias estaciones
00001000	Token	Pasar el testigo
00001100	Set…Successor	Permitir que la estación se desconecte del anillo

- **Dirección de destino**.- Es un campo de 2 o 6 bytes que contiene la dirección del destinatario de la trama. El sistema de direccionamiento de la norma IEEE 802.4 es idéntico al de la norma IEEE 802.3. Únicamente hay que asegurarse de que, en la misma red, no convivan estaciones con dirección de 2 bytes con otras con dirección de 6 bytes, ya que no se deben mezclar.

- **Dirección de origen**.- Es semejante al campo de dirección de destino, pero codifica la dirección MAC de la tarjeta que originó la trama.

- **Campo de datos**.- En este campo se codifica la información del usuario. Su longitud varía entre 0 y 8182 bytes para el caso de tramas con 2 bytes de dirección; y entre 0 y 8174 bytes en el caso de tramas con direcciones de 6 bytes.

- **CRC**.- Campo semejante al de la IEEE 802.3 encargado del control de errores por redundancia cíclica

- **Delimitador de fin**.- Es un campo idéntico al delimitador de inicio. Su misión es señalizar el final de la trama.

En su funcionamiento, lo mas complejo del estándar IEEE 802.4 es el procedimiento de mantenimiento del anillo lógico, ya que debe ser capaz de resolver problemas como ls que siguen:

- *Tomar la decisión de qué estación debe generar el testigo en el caso de que se haya perdido o deteriorado el testigo anterior.*
- *Resolver los conflictos provocados por la existencia de dos o más testigos en la red, generados por el mal funcionamiento de ésta en un momento dado.*
- *Determinar quién es la estación sucesora o la estación predecesora de cualquier estación de la red*

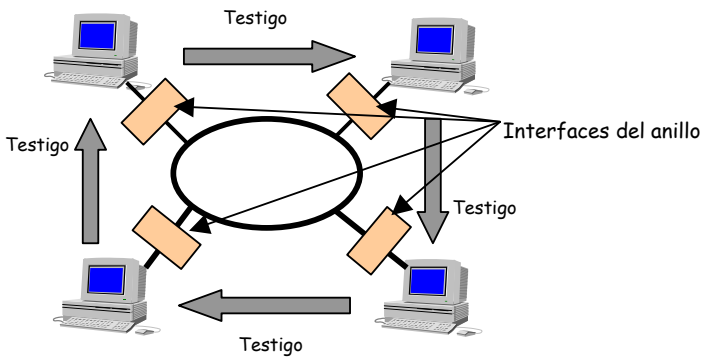
- *Dar de baja en el anillo una estación que desea ser desconectada, lo que supone informar a la estación sucesora y predecesora que deben establecer una relación de continuidad lógica en el anillo.*
- *Dar de alta en el anillo una estación que solicita entrar en la red, lo que implica insertar la estación entre una sucesora y una predecesora, que deben ser informadas de la inserción.*
- *Cuando durante un cierto tiempo no hay actividad en la red , cualquier estación puede emitir tramas de solicitud de testigo estableciendo una contienda determinada (que no es propia del anillo) para determinar si la estación es o no la encargada de generar un testigo que inicie el anillo lógico.*

Por último, como la IEEE 802.4 es un estándar que define protocolos libres de errores, su rendimiento crece con el número de estaciones transmisoras hasta agotar el ancho de banda del medio de transmisión. Es, por tanto, muy eficaz

5.4.3.-Estándar IEEE 802.5 (Token Ring).

La constitución física de un anillo no es una línea circular, como puede parecer por la forma en que se suele representar gráficamente. Mas bien está constituido por un conjunto de interfaces a los que se conecta cada estación del anillo, y una serie de líneas punto a punto entre cada dos interfaces consecutivos en forma cerrada.

Son muchos los tipos de anillos que se pueden construir, pero el mas extendido es el recomendado por la norma IEEE 802.5 que propone una red en anillo con paso de testigo como la que se propone en la figura:



Desde el punto de vista del diseño hay una serie de elementos a considerar, el primero de ellos es la ***longitud física de un bit*** en el anillo. Al ser la topología física la de una estructura cerrada, sólo cabe dentro de ella un número finito de bits simultáneamente.

Cada bit tarda un cierto tiempo en recorrer el anillo y, después de recorrerlo, el bit debe ser retirado por la estación que lo generó. Así, en un anillo cuya velocidad de transferencia es **V** Mbps se emitirá un bit cada **1/V** μs. Si se considera que la velocidad de transmisión de las señales (la velocidad de la luz en el medio de transmisión) es **c**, cuando una estación termine de transmitir un bit, el punto inicial de ese mismo bit habrá viajado **c/V** metros.

Dando valores típicos de una red de este tipo, como puede ser **V** = 1 Mbps y **c** = $3 \cdot 10^8$ m/s (≈ 200 m/μs), cada bit que viaja en la red ocupa 18'75 metros, por lo que si la longitud de la red fuera de 1 km, en el anillo cabrían 5 bits.

El sistema de operación de las redes IEEE 802.5 es el siguiente:

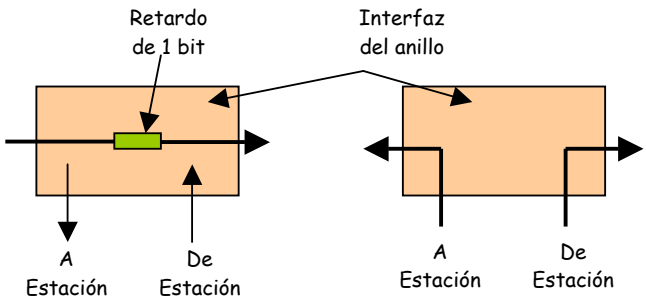
El anillo, en realidad consiste en un conjunto de interfaces de anillo conectadas por líneas punto a punto. Cada bit que llega a un interfaz se copia en un buffer de 1 bit y luego se copia (envia) en el anillo nuevamente. Mientras está en el buffer, el bit puede analizarse y, posiblemente modificar antes de enviarse. Este paso de copiado introduce un retardo de 1 bit en cada interfaz.

En un ***token ring*** (o anillo con testigo), circula por el anillo una trama o *patrón de bit* especial llamado **testigo** (*token*) cuando todas las estaciones están inactivas. Cuando una estación quiere transmitir una trama, debe tomar el testigo y retirarlo del anillo antes de transmitir. Esta acción se lleva a cabo invirtiendo el valor de un solo bit de la trama testigo (de 3 bytes), lo que instantáneamente la convierte en los 3 primeros bytes de una trama de datos normal.

Debido a que sólo hay un testigo, sólo una estación puede transmitir en un instante dado, resolviendo por tanto el problema de acceso al canal de la misma manera que lo hace token bus (norma IEEE 802.4). *No existen, por tanto, posibilidades de colisión*.

El diseño indicado de token ring implica que, al ser el testigo la trama fundamental que controla el acceso al canal, el anillo mismo debe poseer un retardo (***delay***) suficiente (suma del producido por la longitud del anillo y los retardos de 1 bit de cada interface) como para contener un testigo completo que circule cuando todas las estaciones están inactivas. El testigo completo, en el caso de la IEEE 802.5 la longitud de la trama testigo es de 24 bits.

Los interfaces del anillo tienen dos modos de funcionamiento: ***escuchar*** y ***transmitir***. En el modo *escuchar* los bits de entrada simplemente se copian en la salida con un retardo de tiempo de 1 bit En el modo *transmitir*, al que se entra cuando se dispone del testigo, el interfaz rompe la conexión entre la entrada y la salida introduciendo sus propios datos en el anillo, convirtiendo lo que era un testigo en una trama de datos.



Para poder conmutar del modo escuchar al modo transmitir en un tiempo de 1 bit, el interfaz generalmente necesita almacenar en su buffer una o mas tramas, en lugar de obtenerlos de la estación con tan poca anticipación.

A medida que los bits propagados alrededor del anillo regresan, son retirados por el transmisor. La estación transmisora puede guardarlos, para compararlos con los originales y verificar la fiabilidad del anillo, o descartarlos. *Como la trama completa nunca aparece en el anillo en un mismo instante,* ***la arquitectura de anillo no pone límite al tamaño de tramas****.*

Una vez que una estación ha terminado de transmitir el último bit de su último marco, debe regenerar el testigo. Cuando ha regresado el último bit de la trama, debe retirarse, y de inmediato el interfaz debe conmutarse nuevamente al modo escuchar para evitar retirar el testigo que podría seguir si ninguna estación lo ha retirado.

En el protocolo IEEE 802.5 no se necesitan tramas de confirmación especiales. La trama tiene un bit que el receptor pone a uno cuando ha recibido correctamente la trama. Como esta trama llegará necesariamente al emisor, éste detectará, analizando este bit, si la trama llegó correctamente o no al receptor.

Normalmente las redes IEEE 802.5 utilizan cable par trenzado STP operando a velocidades hasta 16 Mbps.

Al igual que en Ethernet, la codificación es Manchester diferencial utilizando +3 voltios para el valor alto de la señal y -4'5 voltios para el valor bajo de la misma. Para marcar el inicio y el final de la trama se utilizan códigos prohibidos en la codificación Manchester.

En ausencia de actividad en la red, el testigo, formado por 3 bytes circula continuamente por el anillo a la espera de que alguna estación lo extraiga de la red y lo convierta en una trama de datos. Cuando una estación quiere transmitir, debe esperar que el testigo pase por su interface, poniendo el bit número 0 del segundo byte a uno. Con esto, la estación convierte los dos primeros bytes del testigo en los *campos delimitador de comienzo y de control de acceso*. Seguidamente se envía el resto de la trama: campos de direcciones y de datos, códigos de errores, etc.

Una estación puede retener el testigo y, por tanto, tener el derecho de transmisión, durante un tiempo previamente establecido que se denomina ***tiempo de retención del testigo*** cuyo valor típico es de 10 ms. Durante este tiempo, la estación poseedora del testigo puede transmitir las tramas que desee. Si antes de ese tiempo ya no tiene nada que transmitir o, aun teniendo tramas que transmitir el tiempo de retención ha expirado, la estación está obligada a generar un nuevo testigo, pasando los derechos de transmisión a la siguiente estación del anillo. Los campos que forman una trama IEEE 802.5 son los siguientes:

Trama Testigo

DC 8 bits	CA 8 bits	DF 8 bits

Trama Datos

DC 8 bits	CA 8 bits	CT 8 bits	Dir Dest 2o6 Bytes	Dir Orig 2o6 Bytes	DATOS Sin limite	CRC 4 bytes	DF 8 bits	ET 8 bits

- **Delimitador de Comienzo de trama (DC)**.- Es un byte q ue actúa como bandera señalizadota de principio de trama. La señalización se produce mediante c ódigos Manchester prohibidos.

- **Control de Acceso (CA)**.- Es un campo de un byte que contiene el bit de testigo (puesto a 0 cuando la trama es testigo y a 1 cuando la trama es de datos. Ademas de este bit contiene el bit de monitor, los de prioridad y los de reserva.

- **Control de Trama (CT)**.- Con una ocupación de un byte, sirve para distinguir las tramas de datos de las de control.

- **Dirección de Destino**.- Codifica con 2 o 6 bytes la dirección de la estación destinataria de la trama. El sistema de direccionamiento es similar al de los estándares IEEE 802.3 y IEEE 802.4.

- **Dirección de Origen**.- Es similar que el campo de dirección de destino, pero codificando la dirección que genera la trama.

- **Campo de datos**.- Es el campo que contiene los datos de usuario. No tiene límite en cuanto a longitud.

- **Control de Errores (CRC)**.- Campo de 4 bytes para el control de errores por redundancia cíclica, de forma análoga a Ethernet y Token bus.

- **Delimitador de Fin de trama (DF)**.- Semejante al campo delimitador de comienzo de trama, de un byte de longitud aunque posee algunos bits codificadores de errores detectados por los interfaces e indicadores de última trama en una secuencia lógica de varias tramas.

- **Estado de la trama (ET)**.- Es un campo de 1 byte en el que se contienen, entre otros, los bits denominados **A** y los denominados **C**.

El bit *A* es puesto a 1 por la estación destinataria por el hecho de que ha pasado por su interface. Sin embargo, si esta trama es aceptada por la estación, además pondrá a 1 el bit *C*.

Por tanto, cuando la trama llega de nuevo a la estación emisora, modificada en sus bits *A* y *C* por la estación receptora, la estación emisora analizará estos bits y podrá determinar que:

- Si *A* = 0 y *C* = 0 el destinatario no ha sido encontrado, bien porque la máquina esté apagada, bien por que esté ausente de la red

- Si *A* = 1 y *C* = 0 el destinatario está activo y presente en la red, pero *no ha aceptado la trama*, porque ésta es errónea, por no tener memoria suficiente para copiar la trama o por cualquier otra causa.

- Si *A* = 1 y *C* = 1 el destinatario está presente y además ha copiado la trama.

- El caso A = 0 y C = 1 es imposible puesto que si se realiza la copia de la trama es por que se ha recibido ésta previamente, esto es, la trama llegó al interface .

5.5.-Protocolos de nivel superior para LAN

El protocolo de red IP (familia TCP/IP)

A diferencia de la mayoría de protocolos de la capa de Red el protocolo IP (***Internet Protocol***) se diseñó considerando previamente la interconexión entre distintas redes.El nivel de red tiene por función proporcionar un medio para el transporte de datagramas desde la máquina origen a la máquina destino, sin importar si estas máquinas están en la misma red o si hay otras redes entre ellas. En la actualidad, el protocolo de red IP es el mas extendido. Es el protocolo de red utilizado en Internet, o interconexión de redes de alcance mundial.

5.5.1.- El datagrama IP

La comunicación en Internet funciona como sigue: La capa de transporte del emisor toma corrientes de datos y los divide en datagramas. En teoría, los datagramas pueden ser de hasta 64 kbytes cada uno, pero en la práctica suelen ser por lo general de unos 1500 bytes. Cada datagrama se transmite a través de Internet, posiblemente fragmentándose en unidades mas pequeñas durante el camino. Cuando todas las piezas llegan finalmente a la máquina destino, son reensambladas por el nivel de Red, dejando el datagrama original. Este datagrama es entonces entregado al nivel de transporte, que lo introduce en la corriente de entrada del proceso receptor.

<table>
<tr><td>Versión</td><td>IHL</td><td>Tipo de servicio</td><td colspan="4">Longitud total del Datagrama</td></tr>
<tr><td colspan="3">Identificación</td><td></td><td>DF</td><td>MF</td><td>Desplazamiento del fragmento</td></tr>
<tr><td colspan="2">Tipo de vida</td><td>Protocolo</td><td colspan="4">Código de Redundancia de Cabecera</td></tr>
<tr><td colspan="7">Dirección IP Origen</td></tr>
<tr><td colspan="7">Dirección IP Destino</td></tr>
<tr><td colspan="7">Opciones</td></tr>
<tr><td colspan="7">DATOS</td></tr>
</table>

Un datagrama IP consiste en una parte de **cabecera** (con un tamaño mínimo de 20 bytes y formada por palabras de 32 bits (5 como mínimo)) y una parte de **texto (Datos)**. La ***cabecera*** tiene una parte fija de 20 bytes y una parte opcional de longitud variable, como se indica en la figura anterior; siendo sus campos los siguientes:

- **VERSION**.- Versión del protocolo IP al que pertenece el datagrama (actualmente en uso la 4 y 6).

- **IHL (Internet Header Length)**.- Longitud de la cabecera expresada en **palabras** de 32 bits (longitud mínima 5 palabras).

- **TIPO de SERVICIO**.- Especifica algunos parámetros de **Calidad del servicio**:

    - La prioridad del datagrama.
    - La rapidez en la entrega.
    - La seguridad en la entrega, etc.

  La gran mayoría de los **enrutadores** (Routers) incorporan estas funciones, por lo que al incluirlas no implica un tratamiento especial.

  Un **router o Encaminador** de la red Internet es un dispositivo que trabaja a nivel IP y que tiene fundamentalmente 2 funciones:

    - Realizar la **traducción de protocolos de los niveles inferiores** entre la red Origen y la red Destino.
    - Proporcionar los **mecanismos de Encaminamiento** necesarios para alcanzar cualquier estación Destino desde cualquier estación Origen, ambas conectadas a Internet, a través de redes y routers intermedios.

- **LONGITUD TOTAL DEL DATAGRAMA**.- Tamaño total expresado en bytes, incluyendo la cabecera y los datos. Dado que el tamaño de este campo es de 16 bits, implica que como máximo el datagrama será de 64 Kbytes.

- **IDENTIFICACION**.- Permite llevar a cabo la fragmentación de los datagramas, junto con los campos MF, DF y Desplazamiento.

  Todos los datagramas llevan un Identificador, de manera que cuando un Datagrama se fragmenta, a cada uno de los fragmentos se le incluye el mismo identificador del datagrama.

- **MF (More Fragments)**.- Si vale 1, significa que hay mas fragmentos del datagrama; Si vale 0 , significa que se trata del ultimo fragmento del datagrama.

- **DF (Don't Fragment.- No fragmentar)**.- DF= 1 El datagrama no se puede fragmentar; DF=0 Si se puede fragmentar.

- **DESPLAZAMIENTO**.- Indica la posicion que ocupa el fragamento dentro del Datagrama original. Cuando se fragmenta un Datagrama todos los fragmentos, excepto quiza el ultimo, deben contener un numero entero de Bloques.

- **TIEMPO DE VIDA**.- Contiene el nº maximo (normalmente medido en nº de Saltos) que el Datagrama puede permanecer circulando por la Red. Cada vez que el Datagrama pasa a traves de un Router, éste le resta 1 al Tiempo de Vida. Cuando llega a 0, el Router descarta el Datagrama.

- **PROTOCOLO**.- Es el protocolo de la Capa Superior al que pertenecen los Datos. La capa IP, se comunica basicamente con 2 protocolos
    - El protocolo **TCP** : Especificado con el valor 6.
    - El protocolo **UDP** : Especificado con el valor 17.

- **CÓDIGO DE REDUNDANCIA DE CABECERA**.- Se utiliza para la Deteccion de Errores en la Cabecera del Datagrama. Calculado al hacer la operación XOR de todas las palabras de 16 bits que forman la cabecera.
- **DIRECCIONES IP Fuente y Destino.-** Identifican a la maquina Emisora y Receptora del Datagrama.

- **OPCIONES**.- Informacion adicional del Datagrama del tipo:
    - ***Encaminamiento de Origen***: Se puede indicar la ruta que puede seguir el Datagrama
    - ***Registro de Ruta***: Se puede registrar la Ruta que ha seguido el Datagrama, es decir, las direcciones de los Routers por los que ha pasado.1

5.5.2.- El protocolo IP de Internet

Es un protocolo diseñado para la interconexión de redes heterogéneas mediante **encaminadores** (*Routers*). Se trata de un *protocolo de conexión no fiable*, es decir, que no garantiza la entrega segura de los paquetes. La información que transmite un equipo hacia la red utilizando el protocolo IP *se divide en partes que pueden seguir caminos diferentes* desde la estación Origen hasta la estación Destino, pudiendo por tanto llegar desordenados e incluso duplicados. Deberá ser la capa de Transporte, o incluso la propia aplicación, es la que, en estos casos, detecte y solucione estas situaciones de error.

Las ***unidades de información*** que se transmiten a nivel del protocolo IP se denominan paquetes IP o **Datagramas.**

El protocolo IP tiene tres funciones básicas:

- **Direccionamiento**. IP debe proporcionar un conjunto global de ***direcciones*** que permitan identificar de forma unívoca a cada una de las maquinas conectadas a Internet. Estas direcciones se conocen con el nombre de **Direcciones IP** y no deben confundirse con las direcciones físicas o MAC que se utilizan a nivel de la subcapa MAC del nivel de Enlace de una LAN.

- **Encaminamiento**. IP debe incorporar mecanismos de ***encaminamiento*** eficientes que permitan a todas las estaciones y routers de Internet encaminar adecuadamente los datagramas en función de su destino. Para poder llevar a cabo todas estas funciones, todos los datagramas que se transmiten a la red deben incluir las **direcciones IP** de las maquinas Origen y Destino.

- **Fragmentación**. Cuando un datagrama tiene que cruzar a través de una o varias redes en el camino hacia su Destino, el protocolo IP se encarga de Dividir el paquete en ***fragmentos*** de

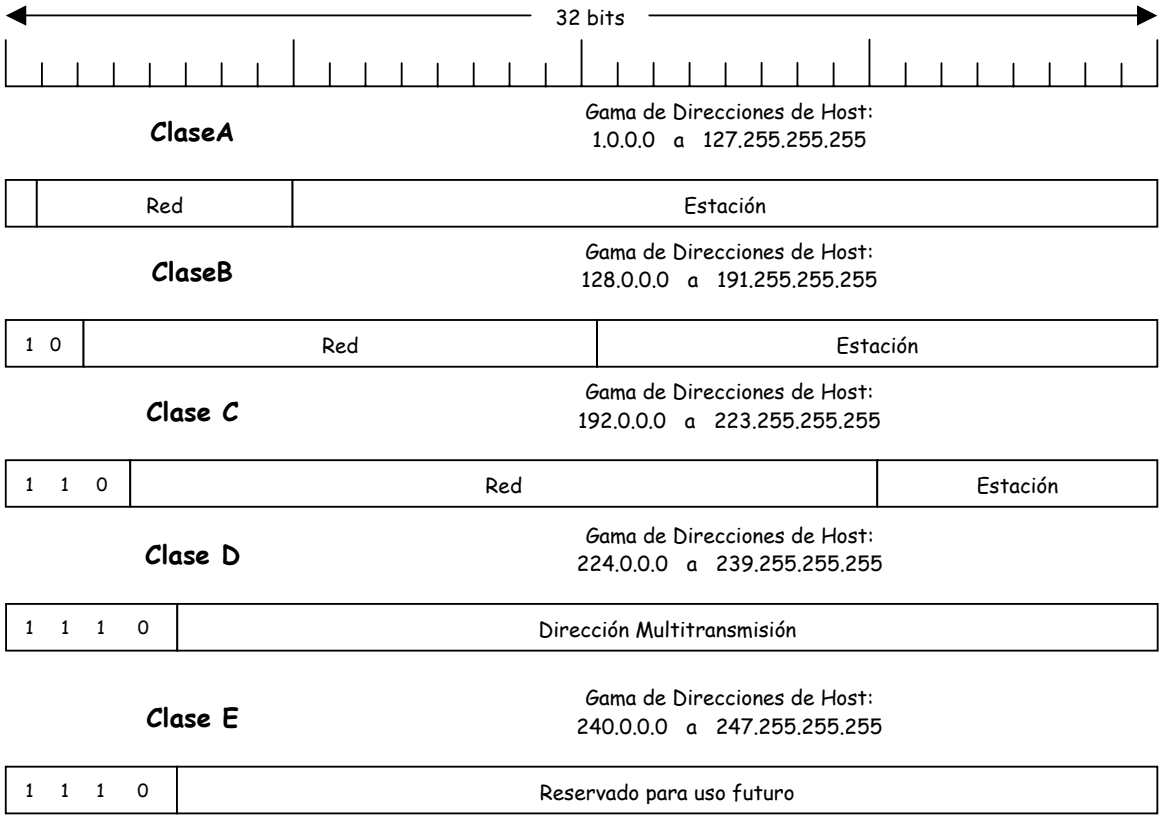
un tamaño aceptable por cada una de las redes que atraviesa. En el destino, el protocolo actuará de forma inversa, reensamblando los distintos fragmentos recibidos para formar el datagrama original.

Actualmente la versión mas extendida de IP es la 4 (**IPv4**), sin embargo, debido sobre todo a las limitaciones en la cantidad de direcciones IP disponibles, se esta implantando poco a poco la versión 6 del protocolo IP (IPv6).

5.5.3.- Direcciones IP

Cada ordenador y cada enrutador de Internet tiene una dirección de IP que codifica su número de red y su número de host. La combinación es única: no hay dos máquinas que tengan la misma dirección IP.

Todas las direcciones IP son de 32 bits de longitud y se usan en los campos *Dirección de Origen* y *Dirección Destino* de los paquetes IP. Los formatos utilizados para las direcciones IP se muestran gráficamente en la figura:

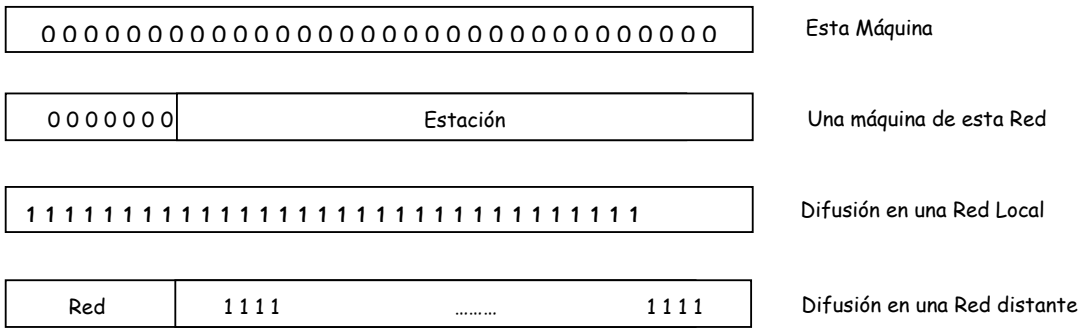


Aquellas máquinas conectadas a varias redes deben tener *diferentes direcciones de IP* en cada red.

Los formatos anteriores permiten respectivamente: hasta 126 redes con 16 millones de máquinas cada una para la clase A; 16382 redes con 64000 maquinas para la clase B; 2 millones de redes de hasta 254 máquinas cada una para la clase C. etc. Las direcciones de red las asigna el **NIC** (Network Information Center).

Las direcciones de red, que son números de 32 bits (4 octetos), generalmente se escriben en **notación decimal con puntos**. En este formato, cada uno de los cuatro bytes se escribe en decimal, de 0 a 255. Así, por ejemplo, la dirección hexadecimal C0290614 se escribe como 192·41·6·20. La dirección IP menor es la 0·0·0·0 y la mayor 255·255·255·255.

Los valores 0 y -1 tienen un significado especial: el valor 0 significa ***esta Red*** o ***esta Estación***. El valor -1 se usa como dirección de difusión para indicar todas las estaciones de la red indicada.



La dirección de IP 0·0·0·0 es usada por las estaciones cuando se arrancan, pero posteriormente no se usan. Las direcciones de IP con 0 como número de red se refieren a la red actual. Estas direcciones permiten que las máquinas se refieran a su propia red sin saber su número (pero tienen que saber su clase para saber cuántos 0 hay que incluir). La dirección formada exclusivamente por unos permite la difusión en la red local y las direcciones con un número de red propio y solamente unos en el campo de identificación de estación permiten que las estaciones envíen paquetes de difusión a LAN distantes desde cualquier parte de Internet.

También, las direcciones 127·XXX·YYY·ZZZ se reservan para pruebas de realimentación, esto es, los paquetes enviados a esa dirección no se ponen en el canal ; se procesan localmente y se tratan como paquetes de entrada. Esto permite que los paquetes se envíen a la red local sin que el emisor conozca su número.

Por último, el NIC ha reservado *tres rangos de direcciones IP que no pueden utilizarse en Internet*. No son direccionables y los encaminadores Internet no las envían. Existe un rango reservado para cada clase de dirección IP:

- Clase A: de 10·0·0·0 a 10·255·255·255
- Clase B: de 172·16·0·0 a 172·16·255·255
- Clase C: de 192·168·0·0 a 192·168·255·255

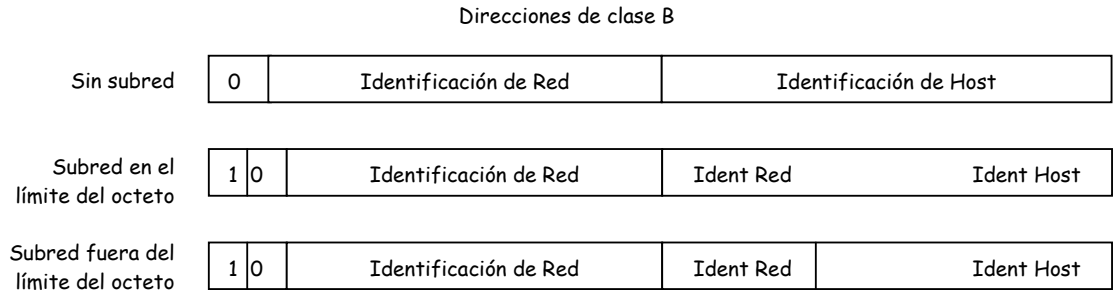
5.5.4.- Subredes

Si una red no va a estar conectada a Internet, los administradores de la red pueden utilizar cualesquiera de las direcciones IP existentes. Sin embargo, al conectar una red a Internet deben utilizarse las direcciones asignadas.

La disponibilidad de direcciones IP está disminuyendo, resultando actualmente muy difícil obtener una dirección, incluso de clase C.

Para paliar esta situación se ha desarrollado un procedimiento de ***subred*** que permite que los administradores distribuyan los identificadores de host de una red en varias subredes

La figura muestra los formatos de las direcciones IP con y sin subredes:



La dirección IP siempre consta de 32 bits . El mecanismo de las subredes utiliza algunos bits de los octetos del identificador del host para identificar la subred. Si no se utilizan subredes, una dirección IP se interpreta en dos campos:

Identificador de Red + Identificador de Host

Si se utilizan subredes la dirección se interpreta en tres campos:

Identificador de Red + Identificador de Subred + Identificador de Host

Máscaras de subred

El identificador de subred se crea utilizando bits del campo del identificador de la máquina mediante la técnica denominada **máscara de subred**.

La máscara de subred es un número de 32 bits en el que los "1" indican que el bit correspondiente de la dirección IP forma parte del identificador de subred y los "0" indican que el bit pertenece al identificador de la máquina.

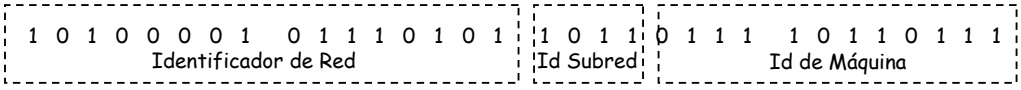
Así, la dirección IP:

1 0 1 0 0 0 0 1 0 1 1 1 0 1 0 1 1 0 1 1 0 1 1 1 1 0 1 1 0 1 1 1

con la máscara de subred:

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0

indica:



El número de bits de la mascara de subred se ajusta en función del número de subredes necesarias, así, en direcciones de clase B la máscara de subred 255·255·255·0 reserva el tercer octeto para el direccionamiento de subredes y permite, consecuentemente, crear 254 identificadores de subred. (nótese que no están permitidas las máscaras de subred en las que los 32 bits son todos "0" o todos "1").

Al configurar una red para que admita direccionamiento de subredes es necesario designar una máscara de subred aunque no se utilicen subredes. Las máscaras de red predeterminadas son las siguientes:

- Clase A: 255·0·0·0
- Clase B: 255·255·0·0
- Clase C: 255·255·255·0

Es necesario configurar la máscara de subred utilizando "1" en los bits que correspondan al campo identificador de red de la clase de dirección. Por ejemplo, una máscara de subred 255·255·0·0 no es válida en una dirección IP de clase C.

El uso de subredes en direcciones de clase C desperdicia muchos identificadores de host potenciales aunque se permite que un NIC represente a varias subredes.

Cálculo de subredes

Es fundamental considerar la forma binaria de las direcciones al planificar las subredes. En caso contrario, la elección de una dirección errónea sería sumamente fácil. Además, si se utiliza una máscara de subred *todos las máquinas deben configurarse con la misma máscara.*

Para determinar el número de subredes que se obtiene a partir de una máscara dada se siguen los siguientes pasos:

- **Calcular el número de subredes**.- Si ***n*** es el número de bits con valor "1" en la porción de la máscara de subred, el número de subredes generadas por la máscara es igual a 2^n-2. Por ejemplo, si hay tres bits con valor "1" en la porción subred de la máscara de subred, pueden existir hasta 2^3-2 = 6 subredes.

- **Calcular los identificadores de red**.- Este método consta de varios pasos:

- Obtener el valor decimal del número binario formado por el último bit de valor "1" de la máscara de subred y los "0" que le siguen:

Así, para la dirección IP de red de clase B:

1 1 0 0 1 0 0 0 0 1 1 0 0 1 0 0 0 0 1 1 0 0 1 0 0 0 0 0 0 0 0 0

de valor decimal **200·100·50·0** con la máscara de subred:

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0

el número bínario formado será: 1 0 0 0 0 0

su número decimal asociado es el 32.

A este número decimal se le denomina **delta**

- Añadir el valor delta al identificador original de la red para obtener el primer identificador de subred:

200·100·50·0 + 0·0·0·32 = 200·100·50·32

- Añadir repetidamente el valor delta para determinar los identificadores restantes:

200·100·50·32 + 0·0·0·32 = 200·100·50·64

200·100·50·64 + 0·0·0·32 = 200·100·50·96

200·100·50·96 + 0·0·0·32 = 200·100·50·128

200·100·50·128 + 0·0·0·32 = 200·100·50·160

200·100·50·160 + 0·0·0·32 = 200·100·50·192

200·100·50·192 + 0·0·0·32 = 200·100·50·224

Como resumen pueden considerarse, para las tres clases principales de direcciones IP las tablas siguientes:

Subredes de clase A

Bits adicionales necesarios (n)	Número máximo de subredes (2^n-2)	Número máximo de máquinas por subred (2^{24-n}-2)	Máscara de subred
0	0	16777214	255.0.0.0
1	No válido	No válido	No válido

2	2	4194302	255.192.0.0
3	6	2097150	255.224.0.0
4	14	1048574	255.240.0.0
5	30	524286	255.248.0.0
6	62	262142	255.252.0.0
7	126	131070	255.254.0.0
8	254	65534	255.255.0.0

Subredes de clase B

Bits adicionales necesarios (n)	Número máximo de subredes (2^n-2)	Número máximo de máquinas por subred (2^{16-n}- 2)	Máscara de subred
0	0	65534	255.255.0.0
1	No válido	No válido	No válido
2	2	16382	255.255.192.0
3	6	8190	255.255.224.0
4	14	4094	255.255.240.0
5	30	2046	255.255.248.0
6	62	1022	255.255.252.0
7	126	510	255.255.254.0
8	254	254	255.255.255.0

Subredes de clase C

Bits adicionales necesarios (n)	Número máximo de subredes (2^n-2)	Número máximo de máquinas por subred (2^{8-n}-2)	Máscara de subred
0	0	254	255.255.255.0
1	No válido	No válido	No válido
2	2	62	255.255.255.192
3	6	30	255.255.255.224
4	14	14	255.255.255.240

5	30	6	255.255.255.248
6	62	2	255.255.255252
7	No válido	No válido	255.255.255254
8	No válido	No válido	255.255.255.255

Protocolos de Encaminamiento en Internet

Existen protocolos de encaminamiento internos empleados por los Routers para el encaminamiento dentro de un sistema autónomo y los protocolos de encaminamiento externos, utilizados por los Routers Frontera para el encaminamiento entre sistemas autónomos distintos.

Protocolos Internos más habituales

- RIP (Routing Information Protocol) o Protocolo de Información de Encaminamiento.
- OSFP (Open Shortest Path First o Protocolo de Apertura del Primer Camino más Corto)

Protocolos Externos más empleados

- EGP (External Gateway Protocol o Protocolo de Pasarela externa).
- BGP (Border Gateway Protocol o Protocolo de Pasarela Frontera).