TEMA 4: REDES LOCALES

INDICE TEMA 4

1. LA SUBCAPA DE ACCESO AL MEDIO

Este capítulo trata de la llamada subcapa de control de acceso al medio (MAC). Esta capa es especialmente importante en las redes de área local (LAN), ya que utilizan un canal de acceso múltiple.

Una LAN es una red en la que los ordenadores conectados a ella están, normalmente, situados dentro de un mismo edificio. Las características particulares de una red de este tipo van a ser:

- Un campo de acción cuyo tamaño no es mayor de unos cuantos kilómetros.
- Una velocidad total de datos mínima de varios Mbps.
- Pertenencia a una sola organización.

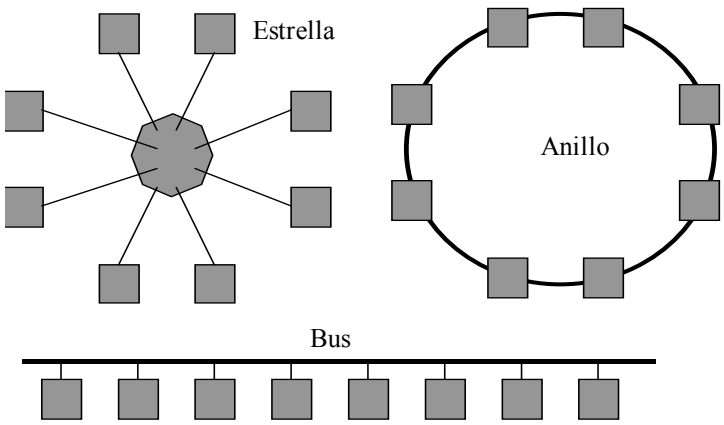
Las redes locales utilizan medios de transmisión muy simples:

- Cable coaxial.
- Par trenzado con o sin apantallamiento.
- Fibra óptica.
- Radio.

Proporcionan una elevada interconectividad entre los elementos de la red a la vez que permiten a cada elemento trabajar de forma independiente. Está interconectividad se logra mediante unas determinadas topologías.

1.1 Topologías de las redes locales

Las topologías empleadas en las LAN son en la mayoría de las ocasiones de uno de los siguientes tres tipos: en Estrella, en Anillo y en Bus. En las comunicaciones en entornos industriales se tiende a utilizar mayoritariamente la última. En las aplicaciones ofimáticas la tendencia actual es hacia las topologías en estrella. Pero las otras topologías también están presentes en cada caso e incluso a veces en una misma red local pueden coexistir varias topologías diferentes.



1.1.1 Topología en Estrella

En la topología en Estrella todo el tráfico pasa a través de un concentrador o nodo central que puede ser activo o pasivo. La conexión entre sí de estos concentradores da lugar a que la ampliación de la red se realice jerarquizadamente en forma de árbol.

Si el nodo central es pasivo, simplemente actúa como repetidor de las señales que recibe por cada uno de los segmentos a él conectados bit a bit.

Si es activo, almacena y retransmite tramas hacia cada nodo en función del direccionamiento de la trama. De esta manera el nodo central realiza un control centralizado en el que puede tener como funciones el interrogar a los nodos periféricos, procesar la información y encaminar toda la información.

Las principales ventajas de esta topología son:

- Fácil inserción de nuevos elementos.
- Alta seguridad ante intentos de entradas de intrusos.
- Fácil detección de nodos con fallos.
- Se pueden conectar elementos con distintos protocolos de comunicación y distintas velocidades de transmisión si el nodo central es activo.
- El direccionamiento nodo a nodo es muy sencillo.
- Un nodo central activo puede establecer prioridades entre las tramas.

Como inconvenientes presenta los siguientes:

- El fallo del concentrador bloquea el funcionamiento de las comunicaciones.
- El nodo central si es activo está dedicado casi exclusivamente a las comunicaciones.
- La actividad de un nodo central activo retrasa el tráfico.
- Si se han de añadir nuevos puertos de E/S al concentrador, la ampliación suele ser cara.

1.1.2 Topología en Anillo

En las topologías en anillo cada estación está unida físicamente a una anterior y otra posterior. La estación siempre recibe los mensajes de la anterior y, cuando no están dirigidos a ella, la interfaz de la estación los transmite sin modificarlos a la estación siguiente. Por lo tanto, la información circula siempre en el mismo sentido dentro del anillo.

Como principales ventajas:

- El acceso a la red esta asegurado en un período de tiempo máximo limitado.
- Simplifican los mecanismos de acuse de recibo, por ejemplo haciendo que la estación que transmite una trama sea la encargada de retirarla.
- Proporcionan velocidades de transmisión altas con tasas de errores muy bajas.
- Este tipo de redes se comporta bastante bien en condiciones de tráfico intenso en la red.
- Todos los nodos tienen acceso a la información que circula por el anillo, lo que permite la priorización de las tramas.

La topología en anillo presentan los siguientes inconvenientes:

- El fallo de una de las estaciones puede suponer el bloqueo de las comunicaciones del resto. Hay que buscar la forma de puentear estaciones averiadas o inactivas.

- La incorporación de nuevas estaciones a la red o la ampliación del alcance de la red es complicada si no existe un diseño de conexión adecuado.

1.1.3 Topología en Bus

En las topologías en bus, todas las estaciones se conectan a un mismo tramo de cable (aunque se pueden crear estructuras en árbol mediante el uso de repetidores) y todas escuchan los paquetes que se difunden por el canal de transmisión.

En este caso, las ventajas son:

- El fallo de la interfaz de una estación no afecta, por lo general, al funcionamiento del resto de la red.
- La inserción de nuevas estaciones es sencilla.
- Se consiguen altas velocidades de transmisión con tasas de errores muy bajas.
- El acceso al medio y la transmisión es muy rápida si la carga de trabajo de la red es baja.

Presenta los siguientes inconvenientes:

- El mecanismo de control de acceso al medio (MAC) ha de ser más elaborado si se desea asegurar un límite para el tiempo de acceso al canal de transmisión.
- Al añadir un nuevo nodo al bus puede que se interrumpa el tráfico.
- La rotura del bus puede bloquear el tráfico de todas las estaciones.
- Bajo cargas de trabajo altas las prestaciones de la red caen drásticamente.

1.2 Asignación Estática del Canal

Una forma tradicional de resolver el problema de cómo se asigna un único canal de comunicación entre varios usuarios, consiste en hacer una multiplexación por división de frecuencia (FDM). Si hay N usuarios, el ancho de banda se divide en N partes del mismo tamaño, asignándole a cada usuario una de esas partes. Dado que cada usuario tiene su propio canal de frecuencias, ya no existirá el problema del acceso simultáneo al medio. Este mecanismo resulta simple y eficiente cuando el número de usuarios es bajo y todos ellos tienen una carga elevada de tráfico. En otras circunstancias, la FDM presenta algunos problemas. El hecho de dividir un canal en N subcanales estáticos es inherentemente ineficiente, ya que cuando algunos usuarios estén inactivos se estará desperdiciando parte de la capacidad total del canal. Además es un esquema muy rígido ante variaciones en el número de usuarios de la red. En redes de ordenadores, el tráfico suele ser a ráfagas, y en consecuencia, la mayor parte de los canales están inactivos durante un gran tiempo.

La misma argumentación puede hacerse para el caso de una multiplexación por división de tiempo (TDM). Cada usuario tiene asignada estáticamente la ranura de tiempo i-ésima, y si no la usa, simplemente se pierde. Resulta evidente que son necesarios mecanismos de asignación dinámica del canal.

1.3 Asignación Dinámica del Canal

En esta sección se estudiarán diferentes mecanismos para la asignación dinámica de canal entre distintas estaciones. Todos estos mecanismos se basan en el siguiente modelo de red:

- **Modelo de estación**: Hay N estaciones independientes, cada una de las cuales tiene un programa o un usuario que genera tramas para su transmisión.
- **Hipótesis de un sólo canal**: En este caso, sólo hay un único canal disponible para llevar todas las comunicaciones entre las N estaciones. Todas las estaciones son capaces de recibir y transmitir a través de él, y todas las estaciones son equivalentes desde el punto de vista de acceso al canal.
- **Hipótesis de colisión**: Si dos tramas se transmiten de forma simultánea, se superpondrán en el tiempo y se tendrá como resultado una señal no válida. Este evento se conoce como colisión. Una trama que haya sufrido colisión podrá ser retransmitida posteriormente.
- **Tiempo**: Se admite un modelo de tiempo continuo en le que la transmisión de una trama puede comenzar en cualquier instante. También puede considerarse la alternativa de tiempo ranurado. En este caso, el tiempo de discretiza en intervalos, de manera que las transmisiones sólo pueden comenzar con el intervalo.

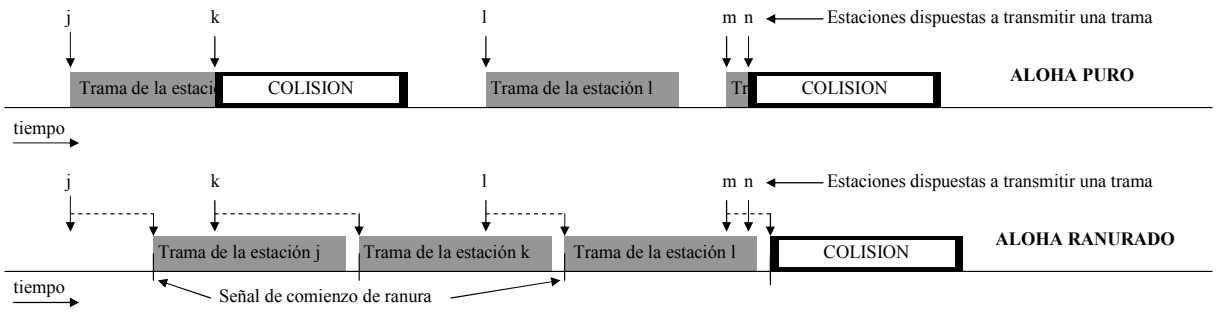
1.3.1 Protocolos con Colisión

Estos protocolos pueden aplicarse a cualquier sistema en el que se tengan usuarios no coordinados que estén compitiendo por el uso de un sólo canal. Este tipo de sistemas se conocen también como sistemas de contienda.

1.3.1.1 Protocolos sin detección de portadora

En la década de 1970, Norman Abramson y sus colegas de la Universidad de Hawai inventaron dos nuevos métodos para la asignación de un sólo canal de transmisión para varias estaciones.

- **Protocolo ALOHA puro**: En la red había un nodo principal y una serie de nodos secundarios repartidos por varias islas del archipiélago. Debido a que la información a transmitir no es continua, sino a ráfagas, no se puede rentabilizar el ancho de banda y el coste de asignar un canal a cada usuario es muy alto. Entonces se pensó en que las diferentes estaciones compartiesen la misma frecuencia sin preocuparse de si está libre o no. La eficiencia de este método depende del número de estaciones y del tráfico que soporte la red, ya que si dos estaciones transmiten simultáneamente hay colisiones y la información se pierde, por lo que habrá que retransmitirla. Se realizó un estudio sobre la eficiencia de este protocolo y se determinó que era de un 18%.



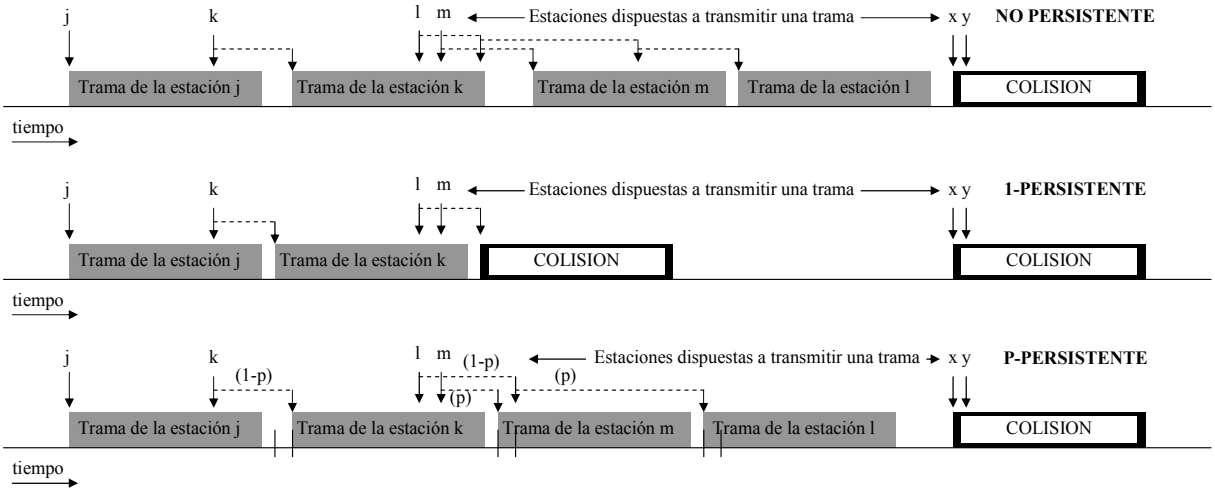
- **Protocolo ALOHA ranurado**: En 1972 se publicó un método que permitió duplicar la capacidad y eficiencia del sistema anterior. La mejora se consiguió dividiendo el tiempo en intervalos discretos denominados ranuras. La transmisión de tramas siempre se realiza al comienzo de una ranura. La sincronización entre los usuarios se consigue teniendo una estación especial que emite una señal al inicio de cada uno de dichos intervalos. A una estación no se le permite que transmita una trama información siempre que quiera, sino que ha de esperar hasta que comience la siguiente ranura. De esta forma se disminuyó el intervalo de vulnerabilidad, o tiempo en que una señal podía ser destruida por el intento de transmisión de otra estación. La eficiencia subió hasta un 37%.

1.3.1.2 Protocolos con detección de portadora

En los mecanismos de acceso al medio con detección de portadora como los CSMA (Carrier Sense Multiple Access), el control del acceso al medio de transmisión se distribuye completamente entre todas las estaciones. Una estación que quiere transmitir escucha la línea para detectar si otra está transmitiendo. Si el canal está vacío la estación transmite, pero si esta ocupado debe esperar un cierto tiempo antes de intentarlo de nuevo.

El empleo del protocolo CSMA evita las colisiones si una estación ya se ha apoderado del canal. Sin embargo, si pueden producirse durante el periodo de contienda (dos estaciones detectan el canal vació e intentan transmitir simultáneamente o antes de que la señal de una llegue hasta la otra). Estas colisiones afectan en forma desfavorable el rendimiento del sistema, en especial cuando la longitud del cable es significativa y las tramas son muy cortas.

Hay tres algoritmos para determinar cuando se vuelve a intentar la transmisión tras encontrar ocupado el canal:



- **No persistente**: La estación tras encontrar el canal ocupado, espera un tiempo aleatorio antes de volver a escuchar el canal para ver si ya está libre. Este tiempo suele ser distinto para dos estaciones lo que evitará las colisiones, pero se produce una pérdida de tiempo al final de cada transmisión.

- **1-Persistente**: La estación escucha el medio ocupado hasta que queda libre y a continuación comunica. Se evita así la pérdida de tiempo tras una transmisión,

pero si más de una estación está esperando a que el medio quede libre para transmitir se produce una colisión.

- ***p*-Persistente**: La estación escucha hasta que el canal queda libre y con probabilidad *p* transmite. Con probabilidad (1-*p*) espera un tiempo fijo (un slot), escucha el canal de nuevo y si está libre transmite. Si no, escucha hasta que el canal queda libre y repite el algoritmo. Este método trata de minimizar colisiones y tiempo de desocupación del canal.

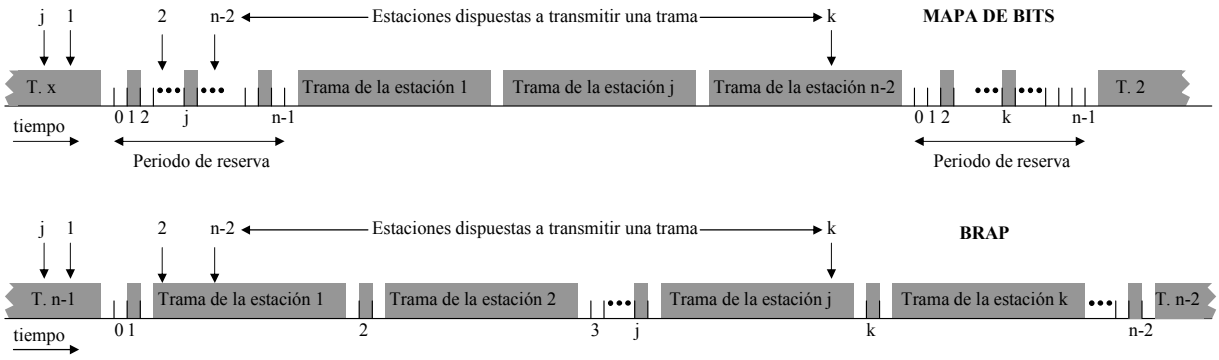
El problema es que ningún algoritmo evita las colisiones completamente. Si se produce una colisión el canal esta desaprovechado durante el tiempo en que se transmiten los mensajes que colisionan y el emisor no sabrá que su mensaje se ha perdido a no ser que espere recibir un acuse de recibo del mensaje y se agote el tiempo de espera por el acuse de recibo.

1.3.2 Protocolos sin Colisión

A continuación se estudiarán algunos protocolos que eliminan totalmente el problema de las colisiones. En todos los casos, se supondrá que hay N estaciones, cada una de ellas con una dirección única. Las direcciones pueden variar entre 0 y N-1.

1.3.2.1 Método del mapa de bits

El protocolo sin colisión más simple es el llamado *método del mapa de bits*. En este caso, cada periodo de contienda tiene exactamente N ranuras. Si la estación 0 no quiere emitir una trama, ésta transmite un bit 0 en la primera ranura, ninguna otra estación está autorizada a transmitir durante esta ranura. Independientemente de lo que haga la estación 0, la estación 1 tiene la oportunidad de transmitir un 1 durante la ranura 1, solamente en caso de que tenga una trama en la lista de espera. En general, la estación j puede avisar que tiene una trama para transmitir mediante la inclusión de un 1 en la ranura j. Después de que hayan pasado las N ranuras, cada estación tiene pleno conocimiento sobre qué estaciones desean transmitir. En este momento, empiezan a transmitir siguiendo la secuencia numérica. Dado que todas están de acuerdo sobre quién es la siguiente que puede transmitir su trama, nunca podrá llegar a presentarse una colisión. Después de que la última estación haya transmitido su trama, un evento que todas las estaciones pueden vigilar, empezará un nuevo periodo de contienda de N bits. Si una estación llegara a estar lista para transmitir después de que haya pasado su bit, ésta simplemente tendrá que permanecer en silencio hasta que todas hayan dicho lo que tenían que decir, y esperar hasta que el mapa de bits vuelva otra vez.



1.3.2.2 Método BRAP: Reconocimiento de difusión por prioridades alternas

El protocolo fundamental del mapa de bits tiene varias desventajas, una de las más evidentes es la asimetría con respecto al número de estación. Las estaciones con baja numeración suelen obtener un servicio mejor que las estaciones con numeración alta. La otra es que ante situaciones de baja carga, la estación siempre tendrá que esperar a que termine el período de muestreo actual (por lo menos) antes de que pueda comenzar a transmitir. El presente método elimina ambos problemas.

En este caso, tan pronto como una estación inserta un bit 1 en su ranura, comienza a transmitir inmediatamente su trama. Además, en lugar de comenzar el mapa de bit cada vez con la estación 0, lo hará con la estación que sigue a la que acaba de transmitir. De esta forma, la autorización para transmitir rota entre las estaciones de forma secuencial. Si la estación desea transmitir, lo hará sin problemas y en caso de que no disponga de ninguna trama para ser enviada dejará vacía su ranura, cediendo así el turno a la siguiente estación.

1.3.3 Protocolos de Contienda Limitada

Hemos considerado dos estrategias básicas para la adquisición de canal en una red que transmite por cable: el método de contienda (por ejemplo los CSMA) y los métodos libres de colisión. Cada estrategia puede calificarse de acuerdo con su rendimiento con respecto al comportamiento de los dos parámetros más importantes, es decir, el retardo en la transmisión de la trama para situaciones de poca carga (pocas estaciones y/o pocas tramas a transmitir) y la eficiencia del canal para el caso de carga alta (muchas estaciones y/o muchas tramas a transmitir). Para condiciones de carga baja, es preferible utilizar el protocolo de contienda (sistemas ALOHA puro o ranurado), debido a que su retardo es mínimo. A medida que la carga se incrementa, la contienda es cada vez menos atractiva, debido a que la sobrecarga asociada a las colisiones en el canal es mayor. Lo contrario es válido para el caso de los protocolos libres de colisión. Estos tienen un gran retardo para condiciones de carga baja, pero a medida que la carga se incrementa, la eficiencia del canal mejora, más que tender a empeorar.

Sería interesante combinar las mejores propiedades de los protocolos de contienda y libre de colisión, para dar lugar a uno nuevo que utilizara el de contienda para condiciones de baja carga, con objeto de tener un retardo pequeño, y que al mismo tiempo, utilizara un técnica libre de colisión para el caso de cargas elevadas y así obtener una buena eficiencia en el canal. Estos protocolos se denominan *protocolos de contienda limitada*.

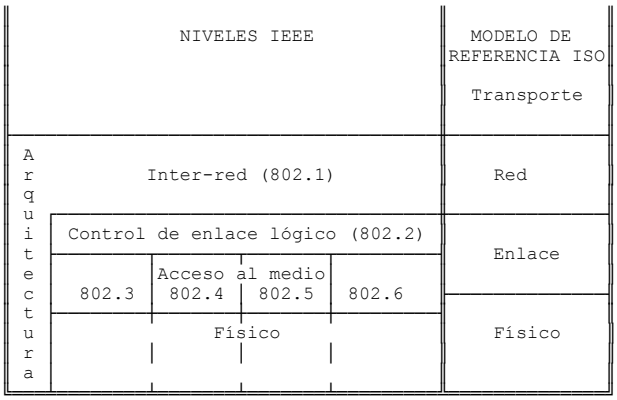
Para que pueda incrementarse la probabilidad de que alguna estación que está tratando de adquirir un canal lo consiga, solamente se logrará mediante la disminución de las que compiten por él. Los protocolos de contienda limitada se encargan precisamente de llevar a cabo esto. Primero dividen las estaciones en grupos. Sólo los miembros del grupo 0 están autorizados a competir por la ranura 0; si alguno de ellos tiene éxito, tomará posesión del canal y transmitirá su trama. Pero si la ranura 0 queda inactiva o si hay una colisión, los miembros del grupo 1 compiten por la ranura 1, etc. El hecho de hacer una división en grupos, hace que la probabilidad de colisión para cada una de las ranuras se reduzca.

El problema consiste en cómo asignar las estaciones a las ranuras. Consideremos algunos casos especiales. En un extremo, por ejemplo, cada grupo estará constituido exclusivamente por un miembro, lo que garantiza que no habrá colisiones porque sólo una estación estará compitiendo por una ranura. Este caso es el protocolo BRAP. El siguiente caso especial, consiste en asignar dos estaciones por grupo, en donde la probabilidad de que traten

de transmitir durante una ranura es p^2 (p es la probabilidad de que una estación quiera transmitir), y si p es pequeño, la probabilidad de colisión es despreciable. Además, la asignación de dos estaciones por ranura reduce el número de ranuras en el mapa de bits del BRAP, disminuyendo así el retardo a la mitad. A medida que se asignan más y más estaciones a la misma ranura, la probabilidad de que se tenga una colisión aumenta, pero la longitud del mapa de bit necesario para dar una oportunidad a todas ellas disminuye. El caso límite será, por consiguiente, tener un solo grupo que contenga todas las estaciones (es decir, un sistema ALOHA ranurado). Lo que se necesita es una forma efectiva de asignar las estaciones a las ranuras dinámicamente, con muchas estaciones por ranura, cuando la carga sea baja y sólo unas cuantas a medida que la carga aumenta.

1.4 Norma IEEE 802 para Redes Locales

La mayor parte del trabajo de estandarización de las redes de área local (LANs), lo ha llevado a cabo el comité de 802 del IEEE. Estos estándares de redes locales recogen las funciones de los dos primeros niveles del modelo de referencia ISO/OSI. Se han definido una serie de estándares para varias redes locales con topologías en anillo y en bus. Hay un estándar separado para cada tipo de control de acceso al medio (MAC) que también cubre algunos aspectos que normalmente son considerados parte del nivel Físico. Al subnivel de control del enlace lógico (LLC), le corresponden tareas de gestión de tramas de enlace y de control de errores entre un par de estaciones y es independiente del tipo de control de acceso al medio. El estándar IEEE 802.1 cubre la descripción formal tanto de la arquitectura de la red como de los mecanismos de interconexión entre redes.



802.3 = CSMA/CD
802.4 = Bus con paso de testigo
802.5 = Anillo con paso de testigo
802.6 = Redes de área metropolitana o bus de banda ancha

En la Figura, también se recoge la relación de los subniveles IEEE con el modelo de referencia ISO/OSI. Como se puede ver, el nivel de Enlace queda prácticamente dividido en dos subniveles: el MAC, encargado del control del acceso al medio físico y los formatos de trama, y el LLC, con las misiones propias del enlace de datos, como la gestión de tramas y el control de errores.

2. ETHERNET Y EL IEEE 802.3

Ethernet es una especificación para redes de área local que comprende el nivel físico y el nivel de enlace del modelo de referencia ISO/OSI. Se implementa en principio sobre una topología bus serie con mecanismo CSMA/CD para el acceso al medio.

Fue desarrollada inicialmente por Xerox Corporation con el apoyo de Intel Corporation y Digital Equipment Corporation, y ha sido la base para el desarrollo del estándar IEEE 802.3 que difiere ligeramente de la especificación Ethernet.

PARAMETRO	10-BASE-5	10-BASE-2	10-BASE-T	10-BASE-F
Velocidad	10 Mbps.	10 Mbps.	10 Mbps.	10 Mbps.
Longitud del Segmento	500 m. máximo	185 m. máximo	100 m. máximo	1 km. máximo
Longitud de la Red	2.500 m. máx.	925 m. máximo	500 m. máximo	5 km. máximo
Nodos por Segmento	100 máximo	30 máximo	1 máximo	1 máximo
Longitud entre Nodos	2.5 m. mínimo	0.5 m. mínimo	-	-
Capacidad por Nodo	4 pF. máximo	8 pF. máximo	-	-
Cable	Coaxial ϕ 0.4 in. 50 Ω Malla doble Rígido	Coaxial ϕ 0.2 in. 50 Ω Malla simple Flexible	Par trenzado Sin o con malla Flexible	Fibra óptica Flexible

Ethernet se ha convertido rápidamente en un estándar “de facto” por el gran número de equipos que existen en el mercado y la gran cantidad de software desarrollado para esta red.

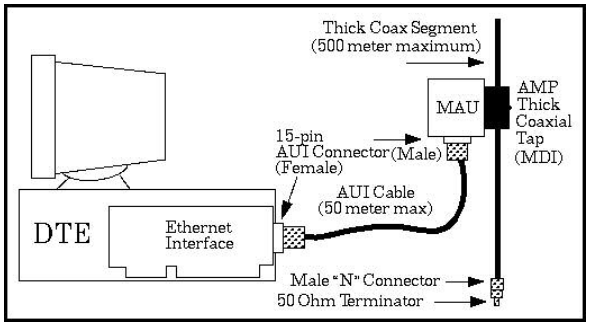
Se implementaba originalmente sobre cable coaxial, codificándose la señal en banda base mediante el código Manchester. Sin embargo se han desarrollado especificaciones para que la red Ethernet se pueda implementar sobre otros soportes físicos: par trenzado, fibra óptica, etc. y soportando mayores velocidades de transmisión.

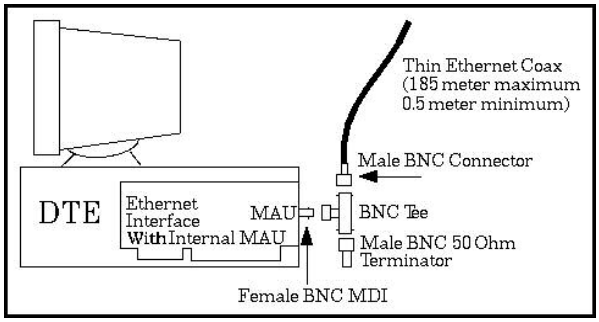
2.1 Topologías de la red Ethernet

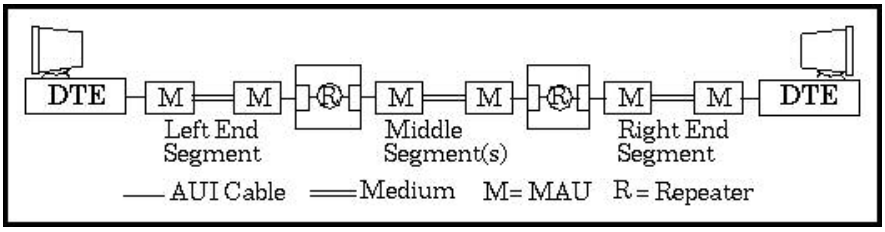
2.1.1 Topología en bus

La topología en bus de la red Ethernet facilita la utilización de repetidores uniendo segmentos que permiten extender la red hasta una longitud total de 2.5 kilómetros y la combinación de segmentos con distintos tipos de cableado. Como limitaciones a esta estructura arborescente, entre dos estaciones no puede existir más de una ruta posible y no puede haber más de dos repetidores de señal entre dos estaciones (Si un tramo de red entre dos repetidores no tiene estaciones ni otros repetidores conectados, se considera al conjunto de los

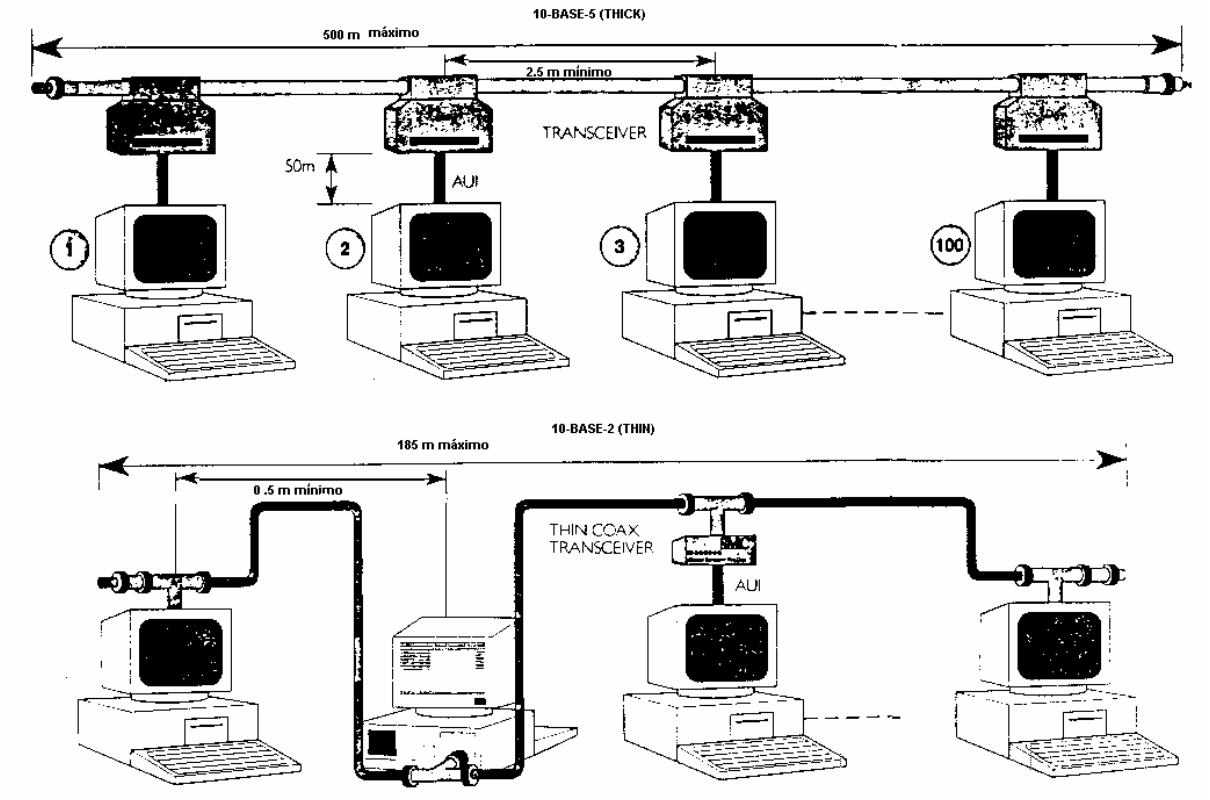
dos repetidores y el cable que los une como un solo repetidor). El número máximo de estaciones de la red se fija en 1024.







Originalmente, una red Ethernet consiste en un cable coaxial de un ancho de media pulgada y hasta 500 metros de longitud (10-BASE-5). El cable central está rodeado por un relleno de polietileno. Rodeando al polietileno hay un escudo de metal, y finalmente, en el exterior, una capa aislante. El cable en sí mismo, es completamente pasivo; todas los elementos electrónicos activos que hacen funcionar a la red están asociados a las computadoras conectadas a la misma. Las redes Ethernet pueden extenderse por medio de unos dispositivos denominados repetidores, que transmiten las señales eléctricas de unos cables a otros.



Las conexiones de las estaciones al cable 10-BASE-5 se hacen por medio de los llamados transceptores o transceivers. En cada conexión de un transceptor al cable, un pequeño agujero en las capas externas del cable permite a pequeñas clavijas tocar el centro del cable y el escudo metálico. El transceptor, también conocido como MAU, se conecta a un conector en "D" de 15 pines, llamado AUI, de la interfaz de la estación (tarjeta de red) por medio de un cable que puede tener hasta 50 metros de longitud. A su vez, la interfaz se comunica con la computadora, normalmente a través del bus de la misma.

Para el sistema operativo, la interfaz aparece como un dispositivo input/output que acepta instrucciones de transferencia de datos de la computadora, controla el transceptor para llevar la transferencia a cabo, envía una señal de interrupción cuando una tarea se ha llevado a cabo e informa sobre el estado de las operaciones.

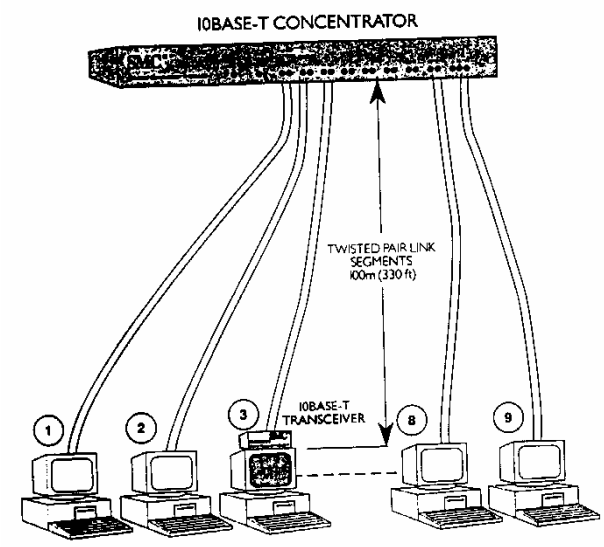
Mientras que el transceptor es un dispositivo hardware sencillo, la interfaz puede ser compleja, incluso llevar un microprocesador para controlar las transferencias.

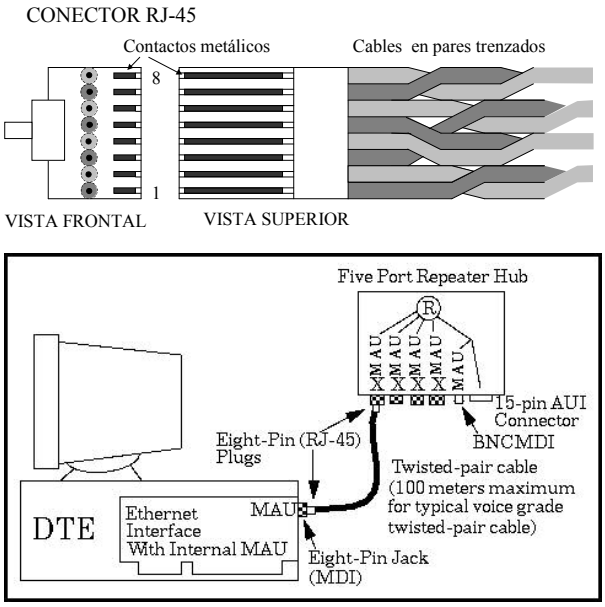
Para la conexión al cable 10-BASE-2 es necesario cortar el cable e insertar conectores BNC para cable coaxial. Para unir una computadora a la red se utiliza un conector BNC en "T" que se conecta directamente a la interfaz de la computadora o a un transceptor que, aunque no es imprescindible, a veces se utilizan con este tipo de cable por razones de flexibilidad. Este tipo de cable coaxial es más fino, flexible y barato que el 10-BASE-5, pero la longitud máxima de un segmento es de 185 metros.

Tanto en el caso del 10-BASE-2 como en el 10-BASE-5 los extremos del cable se coloca un terminador que consiste en una resistencia de 50 ohmios (impedancia característica de los cables coaxiales utilizados) entre la malla y el conductor central del cable coaxial. A veces este terminador no existe en alguno de los extremos si este se conecta directamente a un repetidor.

2.1.2 Topología en estrella

El principal problema que se le achaca a la topología en bus de la red Ethernet es que cualquier fallo en un segmento (una rotura en la continuidad del cable) impide la comunicación a las estaciones conectadas a ese segmento (y esto es habitual en los conectores utilizados con el cable coaxial fino 10-BASE-2). Por ello se desarrolló la 10-BASE-T, que es una red Ethernet con topología en estrella utilizando cables de par trenzado. En esta topología, las estaciones se conectan a un concentrador pasivo o *hub* con un determinado número de bases de conexión (de 8 a 32 generalmente), una para cada estación. En las bases de conexión se insertan conectores del tipo RJ-45, similares a los utilizados en las instalaciones telefónicas, instalados previamente en ambos extremos del cable de par trenzado. Si el número de estaciones supera al de bases de conexión del *hub*, es necesario incorporar un nuevo *hub* que se interconecta con el anterior. El cableado que se utiliza entre las estaciones y el concentrador es del tipo de par trenzado, para aprovechar los cables telefónicos existentes en las instalaciones de los edificios de oficinas. El *hub* también se puede conectar a un bus o líneas de fibra óptica para facilitar la expansión de la red.





Por lo general el cableado se realiza con cuatro pares trenzados, aunque solo dos de ellos se utilizan, uno para transmisión y otro para recepción. La correspondencia entre los pines cableados en la tarjeta adaptadora de la computadora y el *hub* es directa (el 1 con el 1, el 2 con el 2, etc.). En algunas ocasiones se utilizan cables cruzados, donde los pines de recepción de un extremo se unen mediante un par a los de transmisión del otro. Las aplicaciones de este cable cruzado suelen ser la unión directa de dos ordenadores sin utilizar un *hub* para formas una red con sólo dos estaciones, o el entrelazado de *hubs* utilizando un puerto convencional de cada uno para ampliar la red. En este último caso, a veces no es necesario emplear un cable especial cruzado, ya que los *hubs* suelen disponer de algún puerto especial para estas funciones, que cruza internamente las líneas de transmisión y recepción.

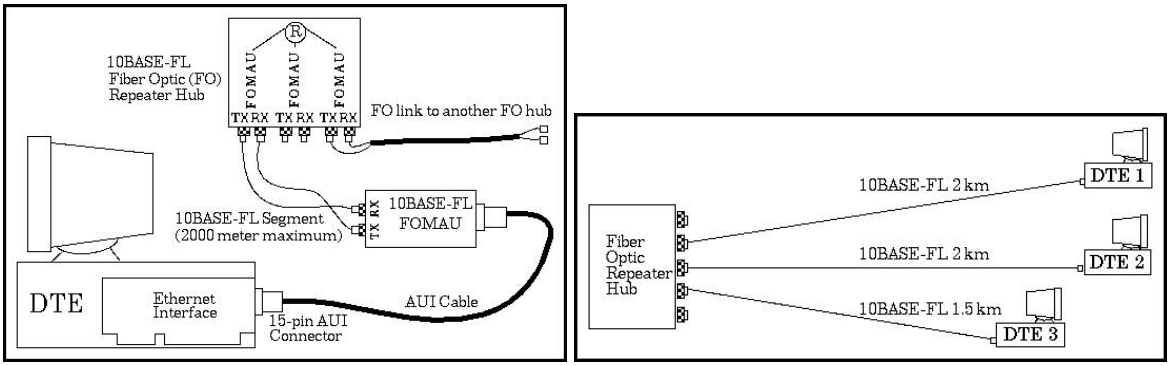
Computador		HUB
TD+	1	1
TD-	2	2
RD+	3	3
	4	4
	5	5
RD-	6	6
	7	7
	8	8

Cable cruzado

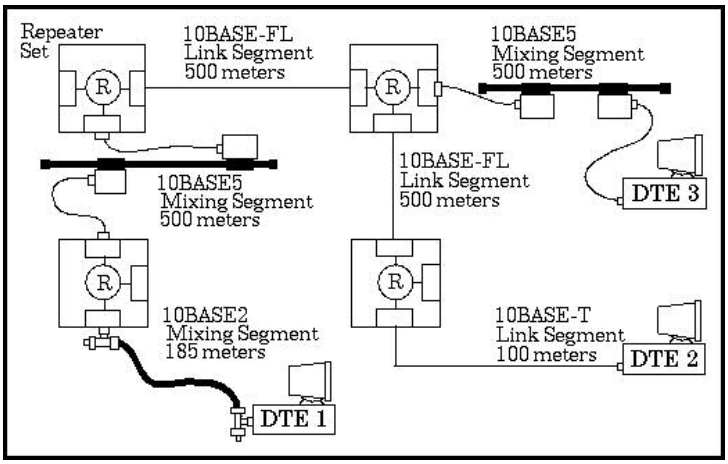
TD+	1	1	TD+
TD-	2	2	TD-
RD+	3	3	RD+
	4	4	
	5	5	
RD-	6	6	RD-
	7	7	
	8	8	

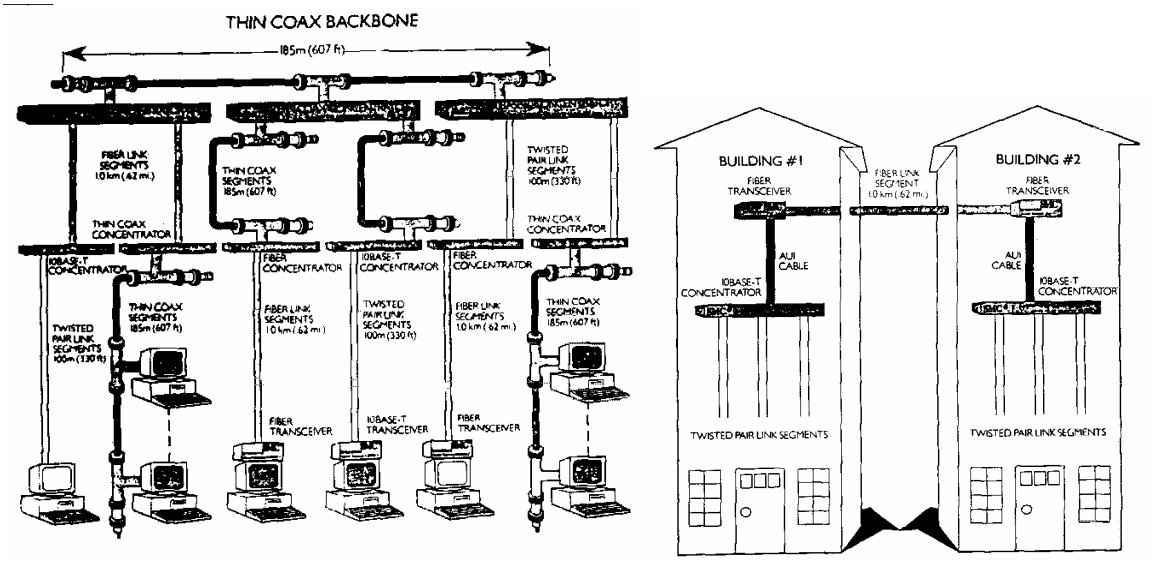
También existen *hubs* para cableado con fibra óptica, 10-BASE-F. Con ello la distancia entre la estación y el *hub* puede pasar de 100 metros, que es el máximo para el cable 10-BASE-T, a uno o dos kilómetros. En este caso el acoplamiento al ordenador se

realiza con un transceptor para fibra óptica conectado al conector AUI de 15 pines de la tarjeta adaptadora de red.



Utilizando los diferentes sistemas de cableado que admite la red Ethernet, esta se puede extender con una gran variedad de posibilidades entre las que se encuentra la conexión de redes de edificios próximos mediante el uso también de fibra óptica. En estos casos se habrán de observar las reglas de extensión de la red mediante repetidores que se mencionaban anteriormente.





2.2 Formato de las tramas Ethernet e IEEE 802.3

Por ser una red broadcast los mensajes enviados por una estación se difunden por todo el árbol de la red formado por los repetidores y segmentos, llegando a todas las estaciones de la red. Esto permite la emisión de mensajes destinados a todas las estaciones (Broadcast) o a un grupo de ellas (Multicast).

El paquete de un mensaje Ethernet consta de los siguientes campos:

Preambulo	Dir. destino	Dir. origen	Tipo	Datos	CRC
8	6	6	2	46-1500	4

- **Preámbulo** (8 bytes): Es una cadena de bits empleada para la sincronización de la codificación de fase y para determinar el comienzo de la trama. Consta de siete bytes (10101010) de preámbulo y un delimitador de comienzo de la trama (10101011).

- **Dirección de destino** (6 bytes)

- **Dirección de origen** (6 bytes): Las direcciones Ethernet tienen 48 bits, de manera que cada estación tiene una dirección única grabada en el hardware con lo que no puede haber coincidencias de dirección entre dos estaciones distintas. Los rangos de direcciones Ethernet son otorgados como parte de la licencia de Xerox a los fabricantes de tarjetas de interfaz Ethernet. Cada fabricante se puede identificar mediante los 3 primeros octetos de la dirección Ethernet, y los otros 3 numeran de forma única cada interfaz, de tal manera que nunca puedan existir dos tarjetas de interfaz Ethernet con la misma dirección.
- **Tipo** (2 bytes): En este campo se indica cual es el protocolo del nivel inmediatamente superior (el de RED) encapsulado en el campo de datos.

Este valor ha de ser superior al valor 05EE en hexadecimal, si es inferior, se trata de un campo de longitud utilizado en tramas de tipo IEEE 802.3.

- **Datos** (46 a 1500 bytes): Contiene los datos de nivel de enlace transmitidos por la trama.
- **CRC** (4 bytes): Código de redundancia cíclica para detección de errores en la trama.

Tras la transmisión de cada trama el medio se mantiene siempre en silencio al menos 9,6 microsegundos con el objeto de facilitar la detección del final de la trama.

La especificación IEEE 802.3 define un formato ligeramente diferente donde las direcciones pueden ser de 16 ó 48 bits y un campo de longitud del mensaje de 16 bits reemplaza al campo del tipo de mensaje. En una red se ha de usar el campo de dirección de 16 o de 48 bits pero no una mezcla de tramas con campo de dirección de diferente tamaño en el mismo cable. A pesar de estas diferencias, en una misma red local pueden transmitirse simultáneamente tramas de tipo Ethernet y de tipo IEEE 802.3 con campo de dirección de 48 bits sin problemas, ya que si en el campo Tipo de 2 bytes el valor es inferior a 0x05EE la trama se interpreta como IEEE 802.3 y si es superior como Ethernet.

La red Ethernet proporciona a nivel de Enlace un servicio de datagramas, en el que los mensajes pueden perderse o llegar duplicados sin que este nivel pueda recuperar este tipo de errores. Por lo tanto, hay que implementar algún tipo de control de secuenciamiento y de detección de errores en los niveles superiores.

El mecanismo de acceso al medio empleado por Ethernet es el CSMA/CD (Carrier Sense Multiple Access with Collision Detection) que se describe brevemente a continuación. Es sobradamente conocido y está recogido en una abundante bibliografía y por las normas Ethernet e IEEE 802.3.

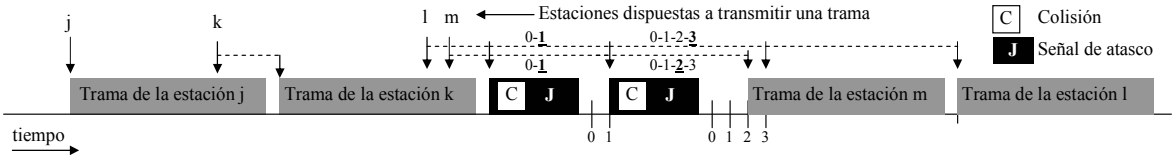
La base del mecanismo CSMA/CD es el CSMA 1-Persistente que se utiliza en topologías en bus. Una estación que quiere transmitir escucha para ver si está en curso otra transmisión, si es así espera a que esta transmisión termine antes de comenzar a transmitir, si no es así trasmite inmediatamente.

El mecanismo CSMA/CD añade una nueva característica al mecanismo CSMA 1-Persistente, la detección de colisión (CD), con el fin de aumentar el aprovechamiento del canal. Es posible que dos o más estaciones encuentren el bus libre y transmitan simultáneamente, se produce entonces una colisión. El transceptor de cada estación escucha la línea mientras transmite y compara la señal con el mensaje a transmitir o detecta niveles elevados de tensión. Si se detecta colisión se aborta la transmisión y se emite una señal de "jamming" (atasco) para asegurarse de que las demás estaciones detectan la colisión y dejan de transmitir. Este método puede detectar también errores en la transmisión producidos por ruido en el canal de transmisión sin necesidad de esperar un acuse de recibo por parte de la estación receptora.

Después de que ocurre una colisión, el tiempo se divide en ranuras discretas llamadas "ventanas de colisión". La duración de una ventana de colisión se define como el tiempo máximo en el que se puede producir una colisión después de que la línea queda en silencio tras la transmisión de una trama, si dos o más estaciones están a la espera para transmitir. Se estima que esta duración es igual a dos veces el tiempo máximo de propagación de la señal a lo largo de todo el bus más el tiempo que dura la señal de jamming (48 bits). El

estándar Ethernet establece, para una red a 10 Mbps, el valor de la "ventana de colisión" en 512 bits (51.2 μs).

Con el fin de facilitar la distinción entre las tramas "basura" resultantes de una colisión y las válidas, se establece que la longitud mínima de una trama válida ha de ser de 64 octetos, por lo cual si la parte de datos de la trama tiene menos de 46 octetos, se completa el campo con octetos de relleno para alcanzar la longitud mínima requerida.



Tras la primera colisión cada una de las estaciones selecciona aleatoriamente esperar 0 ó 1 ranuras antes de intentar de nuevo la transmisión. Si los dos eligen el mismo número de ranuras, tendrá lugar una nueva colisión. Después de esta segunda colisión, cada estación selecciona un número de ranuras que puede ser 0, 1, 2 ó 3, de forma aleatoria y espera dicho número de ranuras. Si ocurriera una tercera colisión, el número de ranuras que tendrá que esperar para la próxima ocasión, será elegido de forma aleatoria entre 0 y 2^3-1.

En general, tras i colisiones se seleccionará un número aleatorio cuyo valor oscilará entre 0 y 2^i-1, y se esperará ese mismo número de ranuras. Sin embargo, si se han producido 10 colisiones seguidas, el intervalo de aleatoriedad se congela a un valor de 0 a 2^{10}-1=1023 ranuras. Si llegasen a producirse 16 colisiones, el controlador desiste de intentar enviar la trama e informa a la estación del fallo, dejando la recuperación del error en manos de las capas superiores. Como el algoritmo que calcula el tiempo aleatorio es función del número de colisiones que ha producido la trama, cuanto más sobrecargada esté la red, más colisiones habrá y mayores serán los intervalos de espera. Este algoritmo se conoce como **disminución exponencial binaria**, y se diseñó con el objetivo de adaptarse dinámicamente al número de estaciones que intentan emitir.

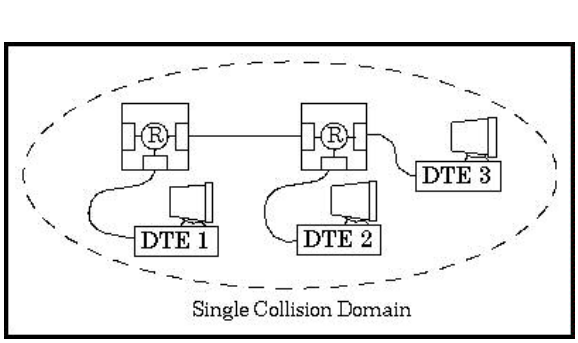
La principal desventaja de Ethernet, sobre todo en lo que se refiere a su utilización en entornos que trabajan en tiempo real, es que no se puede garantizar que una trama se va a enviar en un tiempo máximo conocido, como en el caso de las redes en anillo, el bus con paso de testigo o los sistemas con un único maestro. Ha de tenerse en cuenta que esto sólo es cierto cuando el canal de transmisión está libre de errores, ya que los errores convierten cualquier sistema de comunicación en probabilístico. Con bajas cargas, la probabilidad de errores en una red Ethernet es similar a la de que se produzcan colisiones. Otro inconveniente es que no se puede establecer prioridad alguna entre las tramas, característica que es muy apreciada para sistemas en tiempo real.

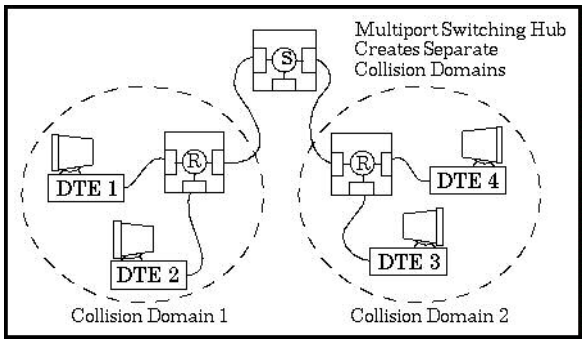
2.3 Red Ethernet conmutada

A medida que se añaden más estaciones a una red Ethernet, el tráfico aumentará, pudiendo llegar a saturar la red. Una solución a este problema consiste en ir a velocidades mayores. Este tipo de solución requiere perder toda la inversión inicial en tarjetas de interfaz. Una solución menos drástica consiste en emplear una red conmutada. En este

modelo, la configuración típica de la parte central del sistema es un conmutador (*switch*) de tráfico con espacio para varias tarjetas de conexión (de 4 a 16). Cada tarjeta está conectada en un *backplane* de alta velocidad y tiene hasta 48 conectores, habitualmente para cableado 10-Base-T, a través de los que se unen las estaciones al sistema. En otros casos cada tarjeta es un equipo independiente, interconectados entre si, cuando proceda, por algún sistema de cableado externo que hace las funciones de *backplane*.

Cuando una estación quiere transmitir una trama, la envía al *switch*. La tarjeta que recibe la trama comprueba si está destinada a uno de las estaciones conectadas en la misma tarjeta. En ese caso, la trama es copiada en dicha conexión. Si no, la trama se envía por el *backplane* de alta velocidad (1Gbps aproximadamente) a la tarjeta que tiene conectada la estación de destino.





El puerto de entrada tiene un buffer, de modo que las tramas que llegan se almacenan en la RAM de la tarjeta según llegan. Este diseño permite que todos los puertos reciban y transmitan tramas simultáneamente. Con este diseño, cada puerto es un dominio de colisiones separado, de modo que no hay colisiones. La capacidad del sistema puede aumentar un orden de magnitud con respecto al cableado 10-Base-5, que proporciona un único dominio de colisión para todo el sistema.

Como el *switch* sólo espera tramas 802.3 en cada puerto de conexión, es posible usar algunos como concentradores, de modo que la conexión no se efectúe con una única estación sino con otro *switch* o un *hub*. De esta forma, cuando las tramas llegan al *hub*,

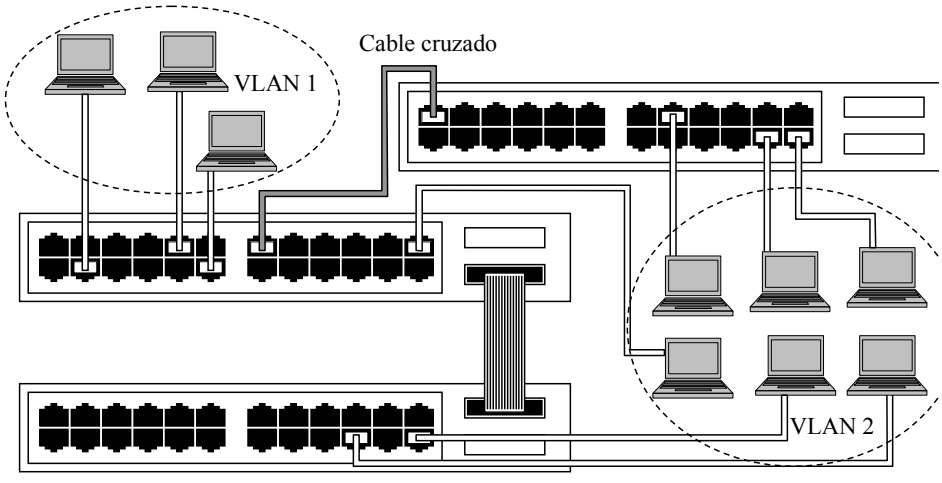
estas compiten por el canal según el mecanismo propio de la norma 802.3. La estación que se apodere del canal emitirá hasta el *switch*, y allí es tratada como cualquier otra. Si todas las conexiones en el *switch* son entre *hubs*, éste puede ser considerado como un puente entre distintas LAN 802.3.

Para conocer cuál o cuáles estaciones se encuentran conectadas a cada uno de los puertos, el conmutador mantiene una tabla de direcciones por cada puerto donde se registran de forma dinámica o estática las direcciones Ethernet de las estaciones conectadas a ese puerto o a los conmutadores o *hubs* que cuelgan de él. Estas tablas tienen capacidad generalmente para almacenar entre 256 y 1024 direcciones, según la calidad del equipo. El administrador del conmutador puede definir el carácter de cada puerto del conmutador, bloquearlo, activarlo, hacer que transmita todas las tramas recibidas en el conmutador o sólo las dirigidas a las direcciones de la tabla correspondiente, hacer que estas tablas sean dinámicas o estáticas, definir las direcciones de cada tabla, etc. Todas estas funciones y muchas más generalmente disponibles en un conmutador (de gama media o alta), hacen de estos equipos unos elementos muy flexibles, que proporcionan una gran seguridad a la red y que aumentan considerablemente el rendimiento de la misma. A continuación se describen algunas de estas características, que normalmente no están disponibles en un *hub*.

2.3.1 Redes virtuales: VLAN

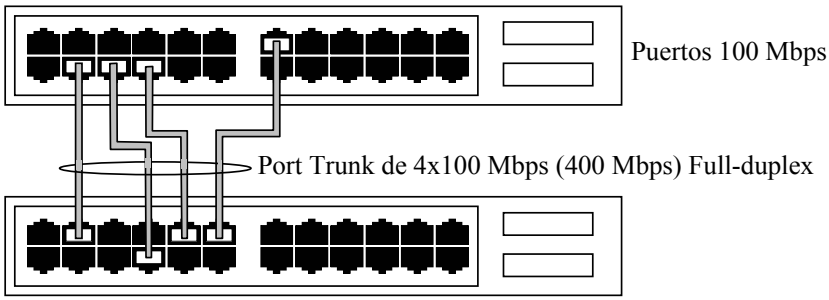
La norma IEEE 802.1Q recoge las funciones que permiten la configuración de redes locales virtuales en sistemas basados en conmutadores que soportan esta norma. Una VLAN es un conjunto de ordenadores conectados mediante un sistema de conmutadores Ethernet que funcionan como una red local independiente, aunque compartan estos conmutadores con otros ordenadores cuyo tráfico les es invisible al igual que para estos resulta invisible el tráfico de los ordenadores que constituyen la VLAN.

Una VLAN puede agrupar varios puertos de un solo conmutador, o integrar puertos distribuidos por varios conmutadores de la red, más o menos próximos. En configuraciones más complejas, se puede hacer que un mismo puerto de un conmutador pueda pertenecer a más de una VLAN.



2.3.2 Agregación de puertos: Port trunks

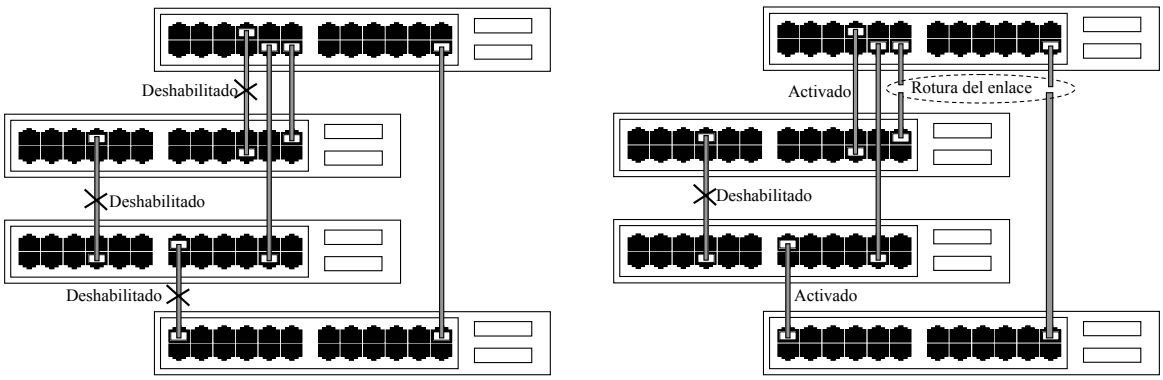
Para conectar conmutadores entre sí se utilizan puertos de conexión de alta velocidad que pueden ser estándar (puertos a 100 Mbps o 1 Gbps) o propietarios del fabricante mediante cableados especiales. Cuando se desea una conexión de alta velocidad y no se dispone de estos sistemas, algunos conmutadores proporcionan la posibilidad de agregar el tráfico de varios puertos para conseguir una unión de más alta velocidad.



2.3.3 Redundancia de conexiones: Spanning tree

La norma 802.1D define entre sus funciones la posibilidad de gestionar conexiones redundantes entre los conmutadores de una red. En principio estas conexiones redundantes no pueden existir en una red Ethernet, ya que se crearían bucles que propagarían de manera incontrolada las tramas Ethernet por la red.

Por lo tanto, el sistema Spanning tree debe reconocer de forma automática esta redundancia de conexiones y mantener deshabilitadas las necesarias para que no existan caminos duplicados en la red. Generalmente el sistema sigue unos criterios mediante los cuales ante dos conexiones redundantes deshabilita la menos óptima. Una vez configurada la red, si falla alguna de las conexiones seleccionadas, se habilitará o habilitarán aquellas conexiones desechadas en principio pero que ahora pueden permitir el mantenimiento de la conectividad de la red.



2.3.4 Gestión de la calidad de servicio

Originalmente el grupo de trabajo IEEE 802.1p desarrolló la definición del soporte de calidad de servicio (QoS, Quality of Service) en conmutadores para cualquier estándar 802.

Finalmente este trabajo quedo recogido en la norma IEEE 802.1D junto otras funcionalidades de los conmutadores. Este estándar busca dos objetivos:

1. Mejorar el soporte de tráfico crítico en la red.
2. Limitar la propagación del trafico multicast en una red de conmutadores.

Para hacerlo se define un método para establecer prioridades de tráfico. En estándares como 802.4 u 802.5 esto es relativamente sencillo porque el formato de trama ya dispone de campos para el establecimiento de prioridades. Pero en el formato de las tramas Ethernet no existen estos campos. Se utiliza el sistema de señalización del IEEE 802.1Q empleado para la clasificación del tráfico de diferentes VLANs (LAN virtuales) para permitir la etiquetación de las tramas con diferentes prioridades. Pero esto obliga a introducir dos nuevos bytes en la trama Ethernet que la mayoría de los dispositivos de red actuales no son capaces de soportar (hay que observar también que el tamaño máximo de la trama Ethernet se verá también incrementado en 2 bytes).

Sólo los conmutadores Ethernet con soporte 802.1D y 802.1Q serán capaces de gestionar correctamente este tipo de tramas y, por lo tanto, la prioridad de distintas tramas con distintas exigencias de calidad de servicio. Una red que de soporte QoS deberá estar integrada en su totalidad por conmutadores con estas capacidades.

2.3.5 Funciones de seguridad

2.3.5.1 Monitorización de puertos

Los conmutadores, por su forma de funcionamiento, hacer que la red sea más segura, al impedir la propagación de las tramas Ethernet por toda la red. Esto limita la capacidad de cualquier dispositivo que se conectase a la misma con el objeto de monitorizar el tráfico de toda la red a sólo aquellas tramas que el conmutador propague hacia el puerto en el que se encuentra conectado ese dispositivo.

En otras ocasiones esta monitorización del tráfico de la red es útil para el administrador para detectar y corregir problemas en la red. Para facilitar este trabajo al administrador, muchos conmutadores ofrecen la posibilidad de reflejar el tráfico que pasa por uno de sus puertos en otro donde el administrador tendrá conectado el dispositivo que le permita monitorizar y analizar el tráfico.

2.3.5.2 Estadísticas RMON

Mediante el protocolo RMON muchos conmutadores permiten la consulta de su estado y estadísticas de tráfico. Esto facilita tanto la detección de situaciones anómalas en la red como la previsión de situaciones de congestión. En base a esta información se puede mejorar la seguridad, la organización de los enlaces o prever nuevas inversiones necesarias para mantener el servicio.

2.3.5.3 Asignación fija de direcciones Ethernet a puertos del conmutador

Una mediada elemental que puede impedir la conexión de un ordenador intruso al puerto de un conmutador, es la asignación fija a este puerto de la dirección Ethernet del

dispositivo que tiene conectado. Una vez que el administrador configure esta situación ningún equipo que no tenga esa dirección Ethernet podrá transmitir o recibir tramas a través de ese puerto.

2.3.5.4 Protección contra tormentas broadcast

Las tramas dirigidas a la dirección broadcast de Ethernet, FF:FF:FF:FF:FF:FF (todos los bits de dirección a 1) se propagan en principio hacia todos los puertos de un conmutador. Si este tráfico es provocado artificialmente por una máquina conectada a la red con el propósito mal intencionado de degradar las prestaciones de la red, puede llegar a colapsarla. Por ello muchos conmutadores están capacitados para limitar el tráfico de tramas broadcast en el caso de que el número de estas sea excesivo, protegiendo así a la red del colapso. La agrupación de puertos en VLANs también limita el que tramas broadcast de una VLAN se propaguen a otra.

2.4 Fast Ethernet

Para aumentar la velocidad de la red Ethernet se creó un nuevo comité que desarrollo la especificación IEEE 802.3u, más conocida como Fast Ethernet. Hubiera sido posible mantener todos los procedimientos del estándar anterior y simplemente reducir la duración de un bit de 100 ns. a 10 ns. Pero en el caso de los cables coaxiales 10-BASE-5 y 10-BASE-2, sería necesario dividir por 10 la longitud máxima admisible, y teniendo en cuenta las ventajas del cable de par trenzado, el diseño de la red se basó en este sistema y la fibra óptica. Es decir, se emplean siempre *hubs* o conmutadores.

Sin embargo un único par trenzado sin pantalla de categoría 3 (UTP-3) no es capaz de transmitir señales en banda base a 200 Mbaudios (que serían necesarios para 100 Mbps en codificación Manchester) a una distancia de 100 metros, por lo que se ha optado por otros métodos de codificación. Se definen los siguientes sistemas:

Denominación	Tipo de Cable	Longitud Max.	Transmisión
100-BASE-T4	4 pares UTP-3 o sup.	100 m.	8B6T, NRZ Semi-duplex
100-BASE-TX	2 pares UTP-5 o STP	100 m.	4B5B, NRZI Full-duplex
100-BASE-FX	2 fibras ópticas	2000 m.	4B5B, NRZI Full-duplex

El 100-BASE-T4 se basa en cable telefónico de baja calidad para aprovechar instalaciones ya existentes. Necesita cuatro pares, uno siempre transmite hacia el hub (TX_D1), otro siempre en sentido contrario (RX_D2) y los dos restantes conmutan para transmitir en un sentido u otro (BI_D3 y BI_D4). La correspondencia entre los pines cableados en la tarjeta adaptadora de la computadora y el *hub* es directa (el 1 con el 1, el 2 con el 2, etc.). Como en el caso de la red Ethernet convencional a 10 Mbps, en algunas ocasiones se utilizan cables cruzados, donde los pines de recepción de un extremo se unen mediante un par a los de transmisión del otro. Las aplicaciones de este cable cruzado suelen ser la unión directa de dos ordenadores sin utilizar un *hub* para formar una red con sólo dos estaciones, o el entrelazado de *hubs* utilizando un puerto convencional de cada

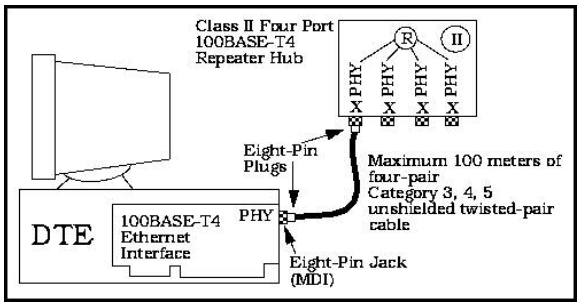
uno para ampliar la red. En este último caso, a veces no es necesario emplear un cable especial cruzado, ya que los *hubs* suelen disponer de algún puerto especial para estas funciones, que cruza internamente las líneas de transmisión y recepción.

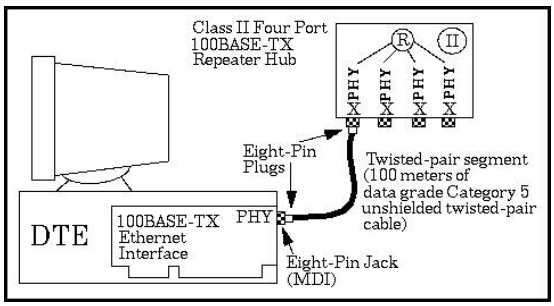
No se envía señal de reloj ni en la codificación ni por ninguna otra línea paralela. Esto se debe a que la precisión los relojes actuales y la longitud de las líneas permiten la sincronización de una trama completa sin errores. Por cada par uno de los tres pares que se emplean en la transmisión se envía un elemento de señalización que pueden estar en tres estados posibles: positivo, negativo o cero voltios. Se pueden codificar de esta manera 27 símbolos, lo que permite transmitir en cada instante 4 bits con alguna redundancia extra. A este método se le llama **8B6T** [STALLINGS 97] [HALSALL 95] porque para transmitir 8 símbolos binarios (8 bits) se emplean 6 símbolos ternarios (dos secuencias consecutivas de tres símbolos, uno en cada par trenzado, con tres estados posibles cada símbolo). Como la codificación empleada es NRZ, sólo se necesita transmitir a 25 Mbaudios para alcanzar una velocidad del 100 Mbps., funcionando los tres pares en paralelo. Esta velocidad es admisible ya que el UTP-3 permite una velocidad de hasta 30 Mbaudios para longitudes de 100 m. En el cuarto par se dispone además de un canal de retorno que se usa para detectar colisiones, cuando se recibe por el una señal mientras se está transmitiendo.

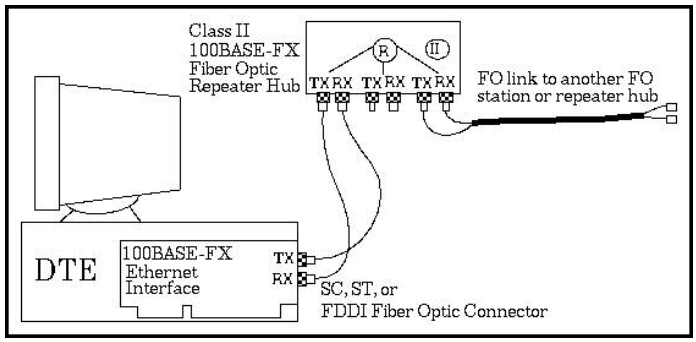
Computador		HUB
TX_D1+	1	1
TX_D1-	2	2
RX_D2+	3	3
BI_D3+	4	4
BI_D3-	5	5
RX_D2-	6	6
BI_D4+	7	7
BI_D4-	8	8

Cable cruzado

TX_D1+	1	1	TX_D1+
TX_D1-	2	2	TX_D1-
RX_D2+	3	3	RX_D2+
BI_D3+	4	4	BI_D3+
BI_D3-	5	5	BI_D3-
RX_D2-	6	6	RX_D2-
BI_D4+	7	7	BI_D4+
BI_D4-	8	8	BI_D4-





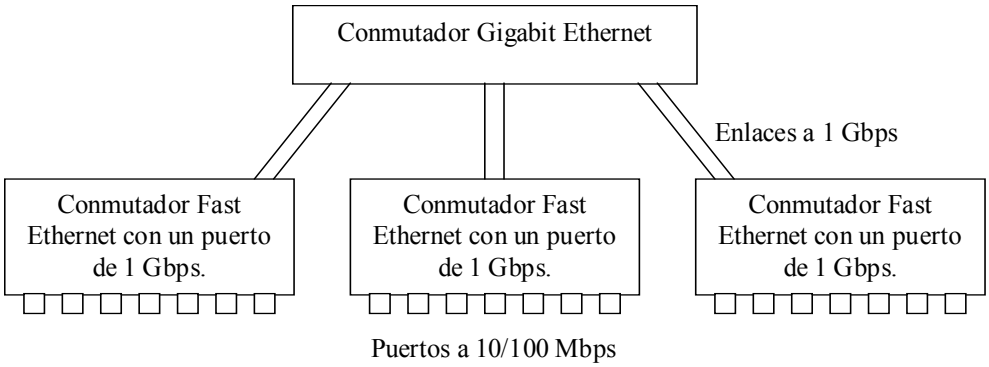


En la especificación 100-BASE-TX se usan un par de calidad UTP-5 o STP de ida y otro de vuelta (Full-duplex) con un reloj a 125 Mhz y que sólo tienen dos estados posibles. El cableado y la utilización de cables cruzados son idénticos a los descritos para 10-BASE-T en la red Ethernet convencional, por lo que si el cableado es de una calidad adecuada, se puede emplear el cableado antiguo para la nueva red a 100 Mbps. En este caso se utiliza el método de codificación **4B5B** que significa que cada secuencias cinco valores binarios transmitidos codifican sólo 4 bits de datos. El bit adicional asegura suficientes transiciones para la sincronización de los relojes y permite crear patrones exclusivos para delimitar tramas. Este mismo esquema es empleado por la especificación 100-BASE-FX y es compatible con el nivel físico de la red FDDI.

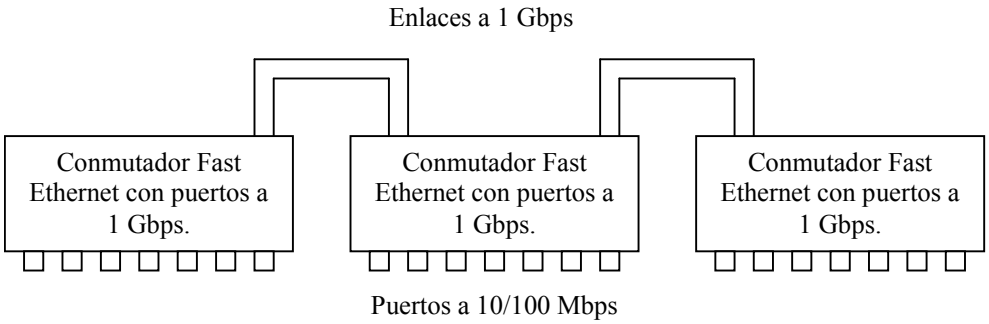
Todas las reglas del IEEE 802.3 son aplicables, incluso el que sólo una estación puede transmitir en cada instante, excepto si se emplean conmutadores (*switches*) en lugar de repetidores (*hubs)*. En este caso, usando conmutadores, una estación puede realmente recibir y transmitir a la vez y la comunicación es realmente Full-duplex aumentando el ancho de banda del sistema. Además, mediante un sistema con *switches* se pueden soportar estaciones que trabajan a 10 y a 100 Mbps. simultáneamente, haciendo más fácil la actualización del sistema si temporalmente han de convivir estaciones a ambas velocidades. El conmutador puede permitir además la coexistencia con otras redes Ethernet a distintas velocidades, como las inalámbricas que tienen velocidades a partir de 2 Mbps.

2.5 Gigabit Ethernet

Gigabit Ethernet es una nueva mejora tecnológica de la red Ethernet con el objeto de superar las prestaciones que las redes ATM pueden proporcionar a las redes locales. Sus bases se encuentran en las redes Ethernet conmutadas que trabajan con puertos a 100 Mbps. La mejora se encuentra en aumentar la velocidad de estos puertos a 1 Gbps. Actualmente existen muy pocos equipos que puedan conectarse a un puerto de 1 Gbps de un conmutador, por lo que las aplicaciones actuales consisten en utilizar estos conmutadores Gigabit Ethernet como elementos de unión de otros conmutadores que tienen puertos a 10 o 100 Mbps donde se conectan directamente las computadoras u otros elementos de la red.



En otros casos los puertos Gigabit se emplean directamente como un *backplane* para unir conmutadores entre sí.



3. REDES INALÁMBRICAS. IEEE 802.11

El estándar IEEE 802.11 especifica los parámetros de las capas Física y de Enlace incluido el control de acceso al medio (MAC) para redes locales inalámbricas. Habitualmente se denominan redes Ethernet inalámbricas, aunque poco tienen que ver con Ethernet salvo en que los dispositivos conectados a una red inalámbrica son fácilmente integrables con una red Ethernet cableada a través de un puente (punto de acceso) que permite la unión de ambas redes.

Las redes inalámbricas (Wireless Local Area Networks, WLAN) ofrecen las siguientes ventajas en productividad, conveniencia y costo sobre las redes cableadas convencionales:

- Movilidad: los sistemas WLAN ofrecen a sus usuarios acceso a la información en tiempo real en cualquier lugar de su organización.
- Velocidad y sencillez de instalación, evitando la necesidad de tender cables a través de paredes y techos.
- Flexibilidad de instalación, permitiendo llegar a lugares de difícil acceso par una red cableada.
- Reducción de gastos de instalación y durante el ciclo de vida de la red, aunque la inversión inicial puede ser mayor. Esto es primordial para entornos dinámicos que requieren mudanzas y cambios frecuentes
- Escalabilidad: los sistemas de WLAN se pueden configurar con diversos tipos de topología para satisfacer las necesidades de aplicaciones e instalaciones específicas. Las configuraciones se cambian con facilidad y varían desde redes igual a igual asta infraestructuras para redes de muchos usuarios.

También hay que tener en cuenta sus inconvenientes:

- Velocidad de transmisión: En términos generales la velocidad de transmisión siempre será inferior a la de una red cableada e incluso sus prestaciones se degradarán más rápidamente cuando se introduzcan nuevos nodos que en una red cableada.
- Interferencias: La red estará sometida a interferencias debidas al entorno radioeléctrico e incluso podría producir interferencias en otros dispositivos de su entorno.
- Privacidad: Las transmisiones se propagan por el espacio sin límites definidos por lo que podrían ser captadas por terceros y espiadas si no se habilitan los sistemas adecuados para mantener la privacidad de las transmisiones.

Este capítulo se centrará en las redes inalámbricas bajo el protocolo 802.11, conocidas también en algunas versiones bajo el nombre de Wi-Fi (Wíreless Fidelity). En realidad Wi-Fi es el nombre de una asociación de fabricantes que vela y certifica la compatibilidad de los productos para las redes inalámbricas de ordenadores 802.11.

3.1 Capa Física

Las redes inalámbricas se diferencian del resto principalmente en la capa Física y en la capa de Enlace de datos según el modelo de referencia OSI ya que sustituyen al cable típico por métodos de transmisión inalámbrica: la transmisión por **radiofrecuencia** y la **luz infrarroja**, siendo más práctico y versátil el uso de la primera.

La capa Física puede utilizar tanto enlaces por radiofrecuencia (FHSS y DSSS) en la banda de 2'4 GHz o enlaces por infrarrojos modulando la señal por *posición de pulso* en la banda 300-428 GHz.

Los sistemas por infrarrojos pueden clasificarse, a su vez, en sistemas de **corta apertura**, también llamados **de línea de vista** (LOS - Line Of Sight) o **de rayo dirigido** y en sistemas de **gran apertura** pudiendo estos últimos ser reflejados o difusos.

Los sistemas de radiofrecuencia son los más habituales y a los que dedicaremos mayor atención y se basan en sistemas de transmisión de **espectro disperso** o **extendido** (*spread spectrum*).

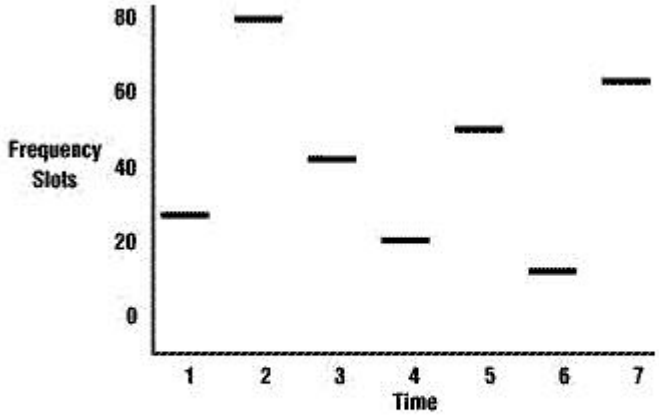
La FCC (Comisión Federal de Comunicaciones de los Estados Unidos de América) permitió la operación sin licencia de dispositivos que utilicen hasta 1 vatio de energía en tres bandas de frecuencias distintas: 902 a 928MHz, 2483.5MHz y 5725 a 5850MHz. Estas bandas de frecuencia son las denominadas bandas ICM (Industrial, Científico y Médico o ISM en inglés) limitadas, en principio, a su implantación en dispositivos para fines industriales, científicos y médicos. Hay que tener en cuenta que la normativa acerca de la potencia de transmisión y las frecuencias utilizables varía entre EEUU, Europa y Japón.

Sin embargo en la actualidad algunas de estas frecuencias se están abriendo y numerosos dispositivos: teléfonos inalámbricos, puertas de garaje automáticas, sensores remotos y microondas las utilizan. Por esto las redes inalámbricas que operan en estas frecuencias deben ser diseñadas para trabajar bajo interferencias considerables. Para ello utilizan, generalmente, una tecnología desarrollada en los años 40 para proteger las comunicaciones militares: *la técnica de espectro disperso*.

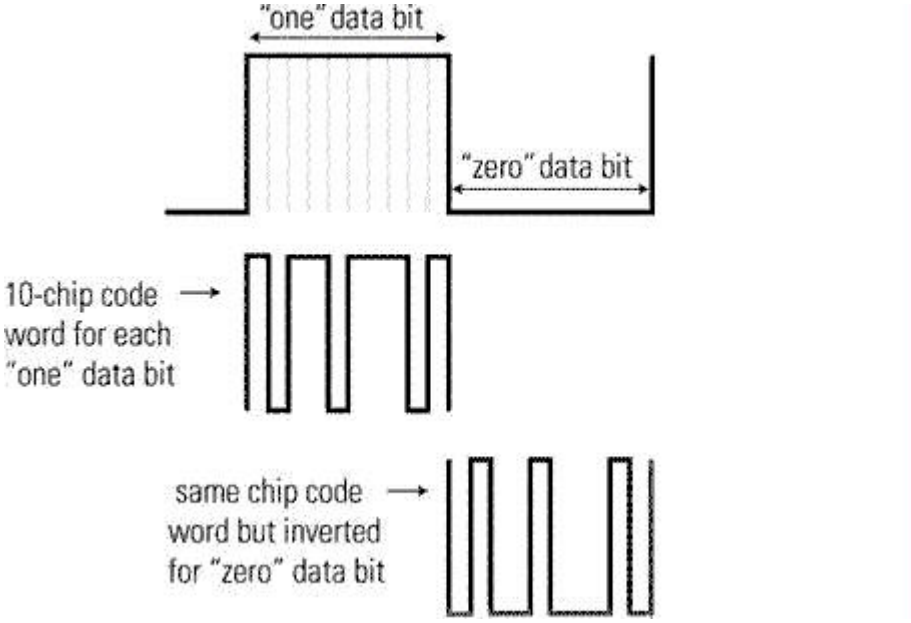
La idea es tomar una señal de banda convencional y distribuir su energía en un dominio más amplio de frecuencias. Así la densidad promedio de energía es menor en el espectro equivalente de la señal original. En aplicaciones militares el objetivo es reducir la densidad de energía por debajo del nivel de ruido ambiental de tal forma que la señal no fuese detectable; en cambio esta técnica aplicada las redes inalámbricas permite que la señal sea transmitida y recibida con un mínimo de interferencia.

Básicamente existen dos técnicas de modulación cuando se hace uso de la tecnología del espectro disperso:

- **Salto de frecuencia** (FHSS, *Frecuency-Hopping Spread Spectrum*). Los dispositivos saltan de una frecuencia a otra de manera síncrona según un patrón predeterminado. Sólo aquellos dispositivos sincronizados pueden acceder a la información.



- **Secuencia directa** (DSSS, *Direct-Sequence Spread Spectrum*). La información a transmitir se mezcla con un patrón pseudoaleatoro de bits para extender los datos antes de que se transmitan. Cada bit transmitido se modula por medio de la secuencia de bits del patrón de referencia, extendiendo su ancho de banda. Sólo el receptor que tenga el mismo código de extensión será capaz de regenerar la información original, mientras que para cualquier otro receptor es ruido de baja potencia que resulta ignorado. Esta técnica permite también corregir algunos de los errores que se puedan producir en la transmisión y requiere un procesador digital de señales (DSP) para correlacionar la señal de entrada.



Los estándar IEEE 802.11b y 802.11g hacen un exhaustivo uso de la banda de frecuencias de los 2'4GHz. El estándar el 802.11a, que utiliza la banda de los 5'2GHz es anterior al 802.11g pero no tuvo éxito por no ser compatible en una misma red con el 802.11b (no pueden compartir el mismo punto de acceso ni tarjetas adaptadoras). Sin

embargo 802.11g si permite una actualización gradual de los equipos 802.11b al ser compatible con esta, aunque la presencia de dispositivos 802.11b en la red hacen que las prestaciones sean algo menores (no se alcanzaran los 54 Mbps para ninguno de los dispositivos conectados).

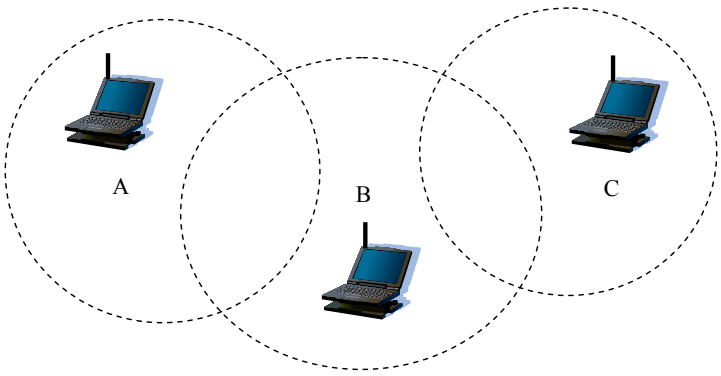
	Tasas de transmisión máximas	Rango	Modulación	Frecuencia
802.11a	Hasta 54 Mbps	50 m	OFDM (FHSS)	U-NII (5 GHz)
802.11b	Hasta 11 Mbps	100 m	CCK (DSSS)	ISM (2'4 GHz)
802.11g	Hasta 54 Mbps	100 m	OFDM (FHSS)	ISM (2'4 GHz)

El consorcio *Wireless Ethernet Compatibility Alliance (WECA)* formado por un grupo de empresas ha establecido un estándar llamado Wi-Fi que permite la certificación de productos acogidos a esta normativa para asegurar la compatibilidad, facilidad de configuración, unanimidad de protocolos, modo de funcionamiento, etc. (http://www.wirelessethernet.com/).

Estos estándares han de competir con otras tecnologías como Bluetooth o HomeRF que utilizan también el rango de frecuencias de 2'4GHz y están especializadas en ofrecer una conectividad inalámbrica enfocada a usos mucho más específicos.

3.2 Capa de Enlace

La capa enlace incluye el mecanismo CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*), donde un nodo se asegura de que el canal está libre antes de transmitir. El mecanismo de detección de colisiones usado en CSMA/CD no puede utilizarse en este caso debido a que un nodo no puede transmitir y escuchar el canal para detectar si otra estación lo hace al mismo tiempo. El mecanismo CSMA/CA no elimina las colisiones completamente, sólo minimiza su probabilidad.

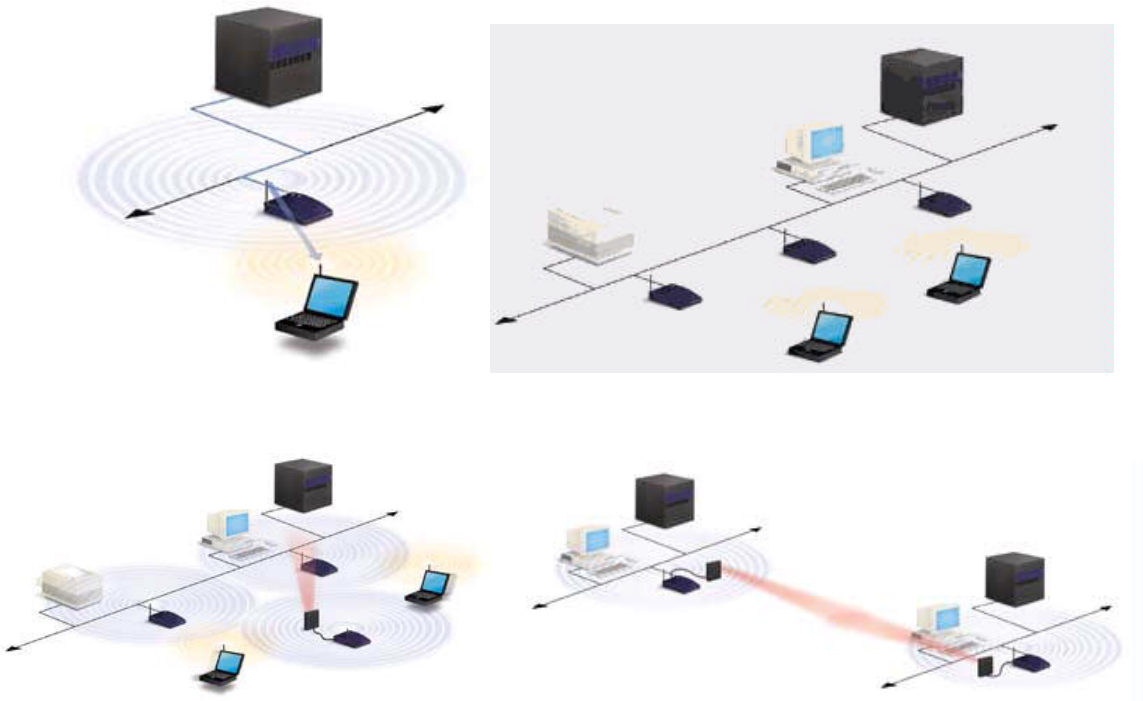


Cuando un paquete está listo para transmitir y el canal está vacío, en nodo emite un paquete RTS (*Ready To Send*) y espera a que el receptor le envíe un paquete CTS (*Clear To Send*). Tras este intercambio de paquetes el emisor envía su trama y si no hubo errores (utilizando un mecanismo basado en el uso de CRC), el receptor envía un paquete ACK.

El uso de este mecanismo se justifica debido al problema "del nodo oculto" ilustrado en la figura. La estación A puede comunicarse con B y B con C. Sin embargo A no puede comunicarse con C y, aunque detecte el canal vacío, C puede estarse comunicando con B. El mecanismo explicado anteriormente alertaría al nodo A de que B está efectivamente ocupado (no le envía el paquete CTS) y que debe esperar antes de transmitir el paquete de datos.

3.3 Dispositivos de la red.

Las redes inalámbricas 802.11 se configuran habitualmente entorno a un dispositivo denominado punto de acceso. Este dispone normalmente de una conexión para una red Ethernet cableada permitiendo integrar los ordenadores que hacen uso de la red inalámbrica con los que ya están conectados a la red Ethernet cableada.



El punto de acceso puede soportar entre 20 y 50 elementos inalámbricos que estén dentro de su radio de acción, unos 100 metros aproximadamente y dependiendo de las condiciones del edificio. Si hay que extender el alcance se pueden unir más puntos de acceso a la red cableada permitiendo además que los elementos inalámbricos móviles puedan conectar según su situación con el punto de acceso más próximo. También existen elementos para extender el alcance de la red que, sin tener conexión a la red cableada, pueden recibir la señal desde un punto de acceso base con una antena más o menos direccional y propagar la señal a zonas donde no llega el punto de acceso principal. Dispositivos similares pueden facilitar también la conexión de dos redes cableadas mediante un puente inalámbrico.

3.4 Seguridad de la red inalámbrica

Para mantener la privacidad en las trasmisiones se ha desarrollado un algoritmo de codificación denominado WEP (Wired Equivalent Privacy). Este algoritmo ha presentado deficiencias en su sistema de claves simétricas de 64 y 128 bits basado en el algoritmo RC4. Si se captura un número elevado y suficiente de paquetes, es posible descubrir la clave utilizada por el sistema. Para mantener la privacidad de la red y gracias a que el número de paquetes que es necesario capturar para romper la seguridad de WEP es enorme, es recomendable cambiar periódicamente las claves del punto de acceso y de los ordenadores de la red.

Otro método para aumentar la seguridad de la red es limitar el acceso a los equipos que tengan direcciones de red conocidas. Un sistema Radius (Remote Autentication Dial -In User Service) para la autentificación de los usuarios que acceden a la red inalámbrica o la alternativa WPA (Wi-Fi Protected Access), que están desarrollando los fabricantes de productos Wi-Fi, pueden ayudar a mejorar la seguridad de la red.

Otro problema es que las redes inalámbricas plantean un problema de seguridad para las redes cableadas. Si un usuario de la red instala por su cuenta y riesgo un punto de acceso conectado a la red cableada sin conocimiento del administrador de la red, está poniendo en peligro la privacidad de toda la red. Es conveniente que el administrador utilice un equipo con tarjeta de red inalámbrica para revisar la red periódicamente en busca de puntos de acceso no controlados.

4. EL PASO DE TESTIGO EN BUS. IEEE 802.4

El Paso de Testigo en Bus (Token Bus) esta definido por la norma IEEE 802.4 que fue desarrollado para ser la base de la arquitectura MAP (Manufacturing Automation Protocol) promovida por General Motors Corporation para resolver los problemas del aumento de la automatización industrial. MAP es una especificación para una red local industrial basada en el modelo de interconexión de sistemas abiertos ISO/OSI que cubre los siete niveles de este modelo y cuyos dos primeros niveles están definidos por la norma IEEE 802.4.

El nivel Físico de la norma IEEE 802.4, define como medio de transmisión el bus de cable coaxial de banda ancha (Broadband) a 10 Mbps. Este medio permite la coexistencia de señales digitales, voz y video. Su principal inconveniente es el alto coste de las interfaces de conexión al medio de transmisión. Se utilizan dos frecuencias, una para transmitir y otra para recibir, por lo que se precisa de un elemento retransmisor en la cabecera del bus de comunicación que realice la retransmisión de la señal que llegan por la frecuencia de transmisión a la de recepción. También admite la comunicación en banda portadora (Carrierband) sobre cable coaxial a 5 y 10 Mbps, con el fin de facilitar el desarrollo de interfaces de bajo coste.

Para el MAC la norma IEEE 802.4 define el paso de testigo como método de acceso. Su principal ventaja es ser determinista, es decir, el tiempo máximo de transmisión de un mensaje es calculable y además admite la priorización de las tramas. El mecanismo de acceso por paso de testigo utilizado por MAP tiene un comportamiento peor que el CSMA/CD de Ethernet cuando las cargas de la red son bajas, pero se comporta mucho mejor cuando el tráfico es elevado, alcanzando un rendimiento superior al del CSMA/CD.

Un testigo circula por el bus dando permiso de transmisión. La estación que se encuentra en posesión del testigo es la única que puede transmitir, y el tiempo que puede permanecer en posesión del testigo es limitado (un máximo de 10 ms). La estación puede administrar este tiempo entre las distintas clases de mensajes, permitiendo así la priorización de los mismos.

La característica de poseer un tiempo de acceso máximo limitado se debe a la imposición de los sistemas de prioridad, y al tiempo máximo de mantenimiento del anillo, que es una imposición de cada sistema particular.

El testigo viaja siempre siguiendo la misma secuencia de nodos. Esta secuencia se establece en orden descendente en función de la dirección física de las estaciones. Cada nodo conoce la dirección de la estación anterior y de la siguiente. La gestión del testigo incluye una serie de funciones complejas que permiten la inicialización automática del anillo lógico, la adición de nuevas estaciones al anillo, eliminación de una estación del anillo y el mantenimiento de un único testigo correcto en circulación.

Para el LLC se ha elegido la norma IEEE 802.2 con servicio de tipo 1. Este servicio permite la comunicación de datos entre unidades LLC homólogas sin establecimiento de conexión de enlace de datos, sin recuperación de errores ni reconocimiento de la secuencia de mensajes.

4.1 Formato de la trama IEEE 802.4

El formato de trama del protocolo IEEE 802.4 es el de la Figura.

El preámbulo varía de acuerdo con la velocidad de transmisión del bus. Su duración es de al menos 2 μs, y esta formado por un número entero de bytes. Su duración es de un byte para un bus a 1 Mbps y de 3 bytes para 10 Mbps.

Preámbulo	Delimitador de comienzo	Control trama	Dirección destino	Dirección fuente	Datos	CRC	Delimitador de final
1 a 3	1	1	2 ó 6	2 ó 6	0-1024	4	1

Los delimitadores de comienzo y final son una codificación analógica de símbolos diferentes al 0 y al 1, por lo que no pueden aparecer accidentalmente en la información, y no es necesario el campo de longitud.

El campo de control de trama en las tramas de datos, lleva la prioridad de la trama y un indicador que indica a la estación destinataria si ha de realizar acuse de recibo. Sin este indicador, el destinatario no podría enviar ninguna contestación al no disponer del testigo.

En las tramas de control, el campo de control indica el tipo de trama (véase la siguiente tabla).

Campo de control	Nombre	Significado
00000000	Reclamo-Testigo	Reclamo del testigo durante la iniciación del anillo
00000001	Solicito-Sucesor-1	Permiso para que las estaciones entren al anillo
00000010	Solicito-Sucesor-2	Permiso para que las estaciones entren al anillo
00000011	Quién-Sigue	Recuperación del testigo perdido
00000100	Resuelve-Contienda	Cuando múltiples estaciones quieran entrar al anillo
00001000	Testigo	Paso del testigo
00001100	Establece-Sucesor	Mensaje de las estaciones que salen o entran en el anillo

El tamaño del campo de direcciones depende de si está en uso la opción de direccionamiento de 16 o 48 bits al igual que en el IEEE 802.3.

El campo de datos puede contener una unidad de datos del LLC, una trama de datos de gestión del MAC o un parámetro relacionado con el campo de control. No hay longitud mínima del campo de datos y se recomienda que la longitud máxima no exceda los 1024 bytes, aunque el número máximo de bytes que pueden existir entre los delimitadores de comienzo y fin es de 8191.

El código de redundancia que se utiliza para detectar errores es el mismo algoritmo y polinomio empleado en el IEEE 802.3.

5. EL PASO DE TESTIGO EN ANILLO. IEEE 802.5

El subcomité de IEEE 802.5, desarrolló un conjunto de estándares que describen una red con paso de testigo en una topología lógica en anillo. El desarrollo de este estándar vino impuesto por IBM que había desarrollado su red Token Ring y también colocó idénticos estándares dentro de la estructura de la Asociación Europea de Fabricantes de Ordenadores.

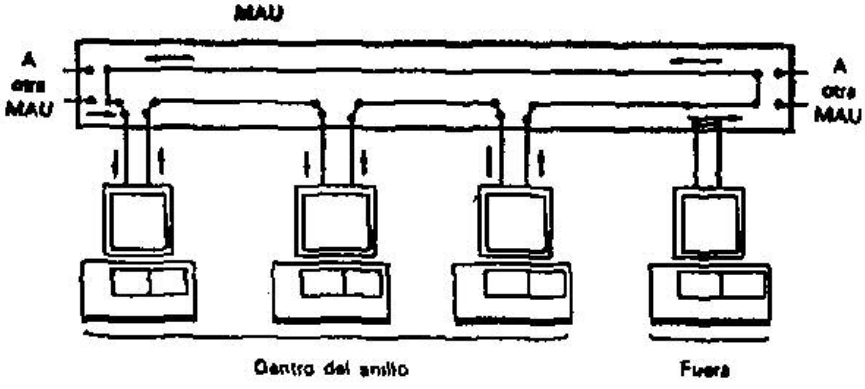
IBM no inventó el concepto de los testigos o la idea de la configuración en anillo. IBM realizó un pago (se dice que de 5 millones de dólares) por una patente sobre una red realizada por el holandés Olof Soderblom. Actualmente IBM ya ha abandonado la explotación comercial de Token Ring, que se ha visto desplazada del mercado por las soluciones Ethernet.

Cuando el tráfico es moderado, el testigo pasar la mayor parte de su tiempo en un estado inactivo, circulando alrededor del anillo. Ocasionalmente será capturada por una estación para transmitir una trama y, después, emitir un testigo nuevo. Sin embargo, cuando el tráfico sea muy elevado, de tal forma que hay una cola de espera en cada estación, tan pronto como una estación termine su transmisión y regenere el testigo, la siguiente estación en orden descendente lo retirará. De esta manera, la autorización para transmitir información gira paulatinamente alrededor del anillo, siguiendo un orden de transmisión en cadena. La eficiencia de la red puede llegar a acercarse al 100%, bajo condiciones de carga elevada.

5.1 Topología en anillo con apariencia de estrella

La apariencia física de una red Token-Ring no es la que cabría esperar. Aunque los testigos y mensajes viajan secuencialmente de nodo en nodo en una topología en anillo, los cables utilizados dan el aspecto externo de una topología en estrella.

Los sistemas Token-Ring utilizan un centro de cableado (nodo central) que incorpora dispositivos electromecánicos para convertir el cableado en un anillo físico. Hay que observar que el nombre dado por IBM al nodo central de cableado de la Token-Ring Unidad de Acceso a Multiestación (MAU), no debe confundirse con la unidad de conexión al medio MAU o transceptor, que se conecta al puerto AUI en el adaptador Ethernet.



La MAU como un concentrador

Cuando una estación intenta unirse al anillo, cierta tensión va de la tarjeta adaptadora, a través del cable, al nodo central donde se activa el relé para que ese cable se conecte al nodo central. La acción de este relé reconfigura el anillo en milisegundos e incorpora la nueva estación. Si el cable de la estación se rompe, se cortocircuitan los hilos del cable o la estación pierde alimentación, se abre el relé y la estación abandona el anillo. Esta disposición previene que un cable en mal estado provoque la caída de todo el sistema (un gran punto a favor a la hora de vender sistemas que utilizan un nodo central como Token-Ring, ARCnet y 10BaseT).

El típico nodo central de cableado de Token-Ring tiene conexiones para ocho nodos. Los nodos centrales se apilan uno encima de otro en un rack y se conectan por medio de cables de unión que van de un puerto de salida de un nodo central al puerto de entrada del siguiente nodo central. Estos cables extienden el anillo de un nodo central a otro, de forma que los nodos están en el mismo anillo incluso si están conectados a diferentes centros de cableado.

A pesar de que una topología con nodo central aumenta las posibilidades de supervivencia de la red ante un cable roto, el protocolo de acceso al medio mediante paso de testigo tienen su propio problema. Si un adaptador falla en un sistema Ethernet o ARCnet, únicamente ese nodo pierde su acceso a la red. Pero si un adaptador de una red Token-Ring falla, el testigo se detiene en ese punto. Aunque este tipo de fallo no es frecuente, resulta catastrófico. Por esta razón, debido a que una administración activa en el nodo central de la red tiene mucho sentido, varias compañías comercializan nodos centrales de Token-Ring con capacidad de gestión activa y con software de control para controlar desde un PC. Estos productos avisan inmediatamente a un administrador de distintos problemas, como el mal funcionamiento de adaptadores y proporcionan una forma de desconexión forzada de nodos del anillo. Los nodos centrales de administración cuestan más pero cada centro de administración puede también informar sobre actividades en unidades menos capaces. La MAU de IBM no tiene ninguna capacidad de administración o control, pero tampoco necesita alimentación primaria y de reserva de corriente alterna, como requieren los centros de administración de otras compañías.

El típico cable recomendado para instalaciones de Token-Ring es el cable de calidad para datos. Contiene dos pares trenzados de hilos cubiertos por una lámina de apantallamiento. La longitud máxima del cable entre el centro de Token-Ring y el punto de conexión para el nodo de la red puede ser de hasta 350 metros (se recomienda un máximo de 110 metros).

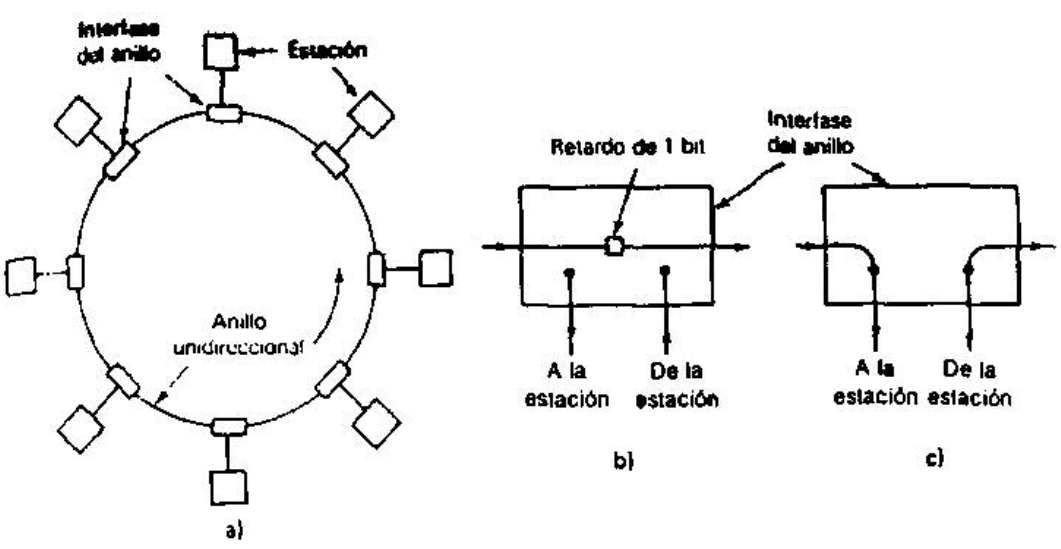
Es posible el uso de pares trenzados no apantallados hasta 110 metros (se recomienda un máximo de 50 metros), pero esta técnica no es recomendable, debido a problemas causados por las interferencias eléctricas que afectan a este tipo de cables. Debido a que el testigo debe circular a través de cada estación, un simple problema de ruido en un brazo de cable de la red podría paralizar toda la red.

En el uso de sistemas de control de acceso al medio por paso de testigo, los mensajes nunca interfieren con otros, garantizando que sólo una estación transmite en un momento dado. Este flujo de datos hace que las redes Token-Ring sean más adecuadas para medios basados en fibra óptica que en los de tipo difusión como son Ethernet o ARCnet. Los medios ópticos, por lo general, son de trasmisión en un sólo sentido, y el testigo viaja en

una única dirección alrededor del anillo, por lo que no hay ninguna necesidad de mezcladores ópticos que dividan la potencia, o de repetidores activos, que son caros.

El producto original Token-Ring de IBM utiliza una velocidad de 4 megabits por segundo en el cable de la red. En 1989, IBM lanzó una versión de Token-Ring que utilizaba una velocidad de 16 megabits por segundo. Los adaptadores a 16 megabits también trabajan a 4 en redes con adaptadores más lentos.

Un tema importante en el diseño y análisis de cualquier red en anillo es la "longitud física" de un bit. Si la velocidad de datos de un anillo es de R Mbps, se emite un bit cada l/R microsegundo. Con una velocidad típica de propagación de la señal de 200 m/microsegundo, cada bit ocupa 200/R metros en el anillo. Esto significa, por ejemplo, que un anillo de 1 Mbps, cuya circunferencia sea de 1000 metros, sólo podrá contener 5 bits a la vez dentro de él.



a) Una red en anillo. b) En modo para escuchar. c) En modo para transmitir.

Un anillo está constituido en realidad por una colección de interfaces de anillo conectadas por medio de líneas punto a punto. Cada uno de los bits que llega a una interfaz se copia en una memoria temporal de 1 bit, para después copiarse de nuevo sobre el anillo. Mientras el bit se encuentre en la memoria temporal, puede inspeccionarse, y quizá hasta modificarse, antes de ser escrito nuevamente sobre el anillo. Este proceso de copiado introduce un retardo de 1 bit en cada interfaz.

En un paso de testigo en anillo se tiene un patrón de bits especial, al cual se le conoce como testigo, que circula alrededor del anillo siempre que las estaciones se encuentren inactivas. Cuando una estación quiere transmitir una trama, es necesario capturar el testigo libre y marcarlo como ocupado, antes de efectuar la transmisión. Debido a que solamente hay un testigo, una sola estación puede transmitir en un instante dado, por lo tanto, se resuelve el problema del acceso al canal, del mismo modo que lo hace el paso de testigo en bus.

El anillo deber tener un retardo suficiente para contener un testigo completo que circule, cuando todas las estaciones se encuentren inactivas. Este retardo tiene dos componentes: el retardo de 1 bit introducido por cada una de las estaciones (o la MAU

cuando estas están inactivas) y el retardo de la señal de propagación. Los diseñadores deben suponer, en casi todos los anillos, que las estaciones deben ser apagadas en varias ocasiones, en especial durante la noche. Sobre un anillo corto, se tiene que insertar un retardo artificial en el anillo, para asegurarse de que el testigo pueda quedar contenido en el en cualquier circunstancia.

5.2 Tramas del IEEE 802.5

El testigo está formado por 3 bytes, según la figura siguiente.

SD	AC	ED

El formato de la trama es el de la figura que se muestra a continuación. Se indica el número de bytes de cada campo.

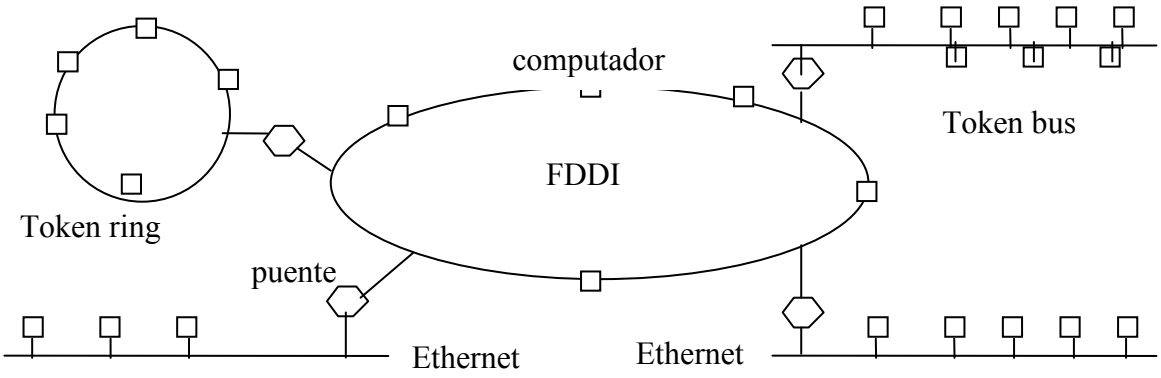
1	1	1	2 ó 6	2 ó 6	sin límite	4	1	1
SD	AC	FC	DEST.	FNTE.	DATOS	CRC	ED	FS

Los bytes SD (delimitador de comienzo de trama), AC (control de acceso) y ED (delimitador de final) son los mismos en la trama y en el testigo. Las direcciones fuente y destino (campos DEST. y FNTE.) son equivalentes a las direcciones de IEEE 802.3 e IEEE 802.4. La longitud del campo de datos no tiene límite, pero la trama completa tiene que caber en 10 milisegundos, para limitar el tiempo que la estación usa la red. El código de redundancia cíclico (campo CRC) es el mismo que en los otros dos estándares. El byte FC es el control de trama y distingue a las tramas de datos de las distintas tramas de control. El byte FS el registro de estado de la trama y contiene los bits A y C doblemente presentes para incrementar la fiabilidad.

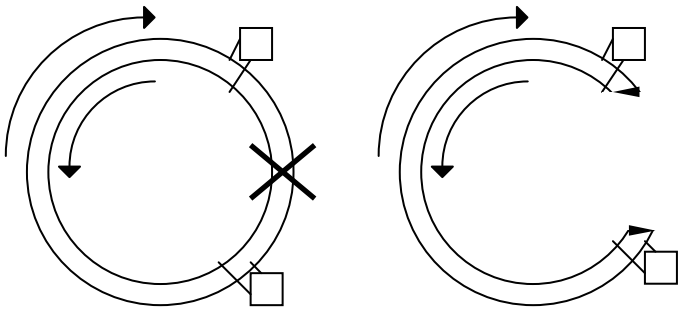
En el anillo, las señales se codifican mediante el código Manchester, con los estados bajo y alto identificados como señales positivas y negativas con magnitud absoluta de 3.0 y 4.5 voltios, respectivamente. Por lo general, la codificación diferencial Manchester utiliza una combinación de estados alto-bajo y bajo-alto para cada bit, pero la norma 802.5 también utiliza los estados alto-alto y bajo-bajo en algunos octetos de control (por ejemplo, para marcar el inicio SD y final ED de una trama). Estas señales, que violan el código Manchester (V), siempre se presentan en pares consecutivos, de tal manera que no introducen una componente de corriente continua en el voltaje del anillo.

5.3 FDDI

La red FDDI (Fiber Distributed Data Interfaz) es una red de fibra óptica de alto rendimiento basada en el paso de testigo en anillo. Los datos se transmiten a 100 Mbps sobre un anillo que puede tener hasta 200 km. de longitud y conectar hasta 1000 estaciones [TANENBAUM 96]. Dada su gran capacidad suele ser utilizada para unir otras redes locales basadas en cableado de cobre más que para unir computadoras directamente.



El anillo de fibra óptica es en realidad doble y el sentido de giro de la información es contrario en un anillo y otro. Esto permite por un lado que si falla uno de los anillos se pueda utilizar el otro y por otro lado que en caso de rotura de ambas fibras paralelas el anillo se pueda reconfigurar mediante unos relés que tienen las estaciones que estén a cada lado del punto de rotura, para formar un nuevo anillo con los dos anteriores que tendrá casi el doble de longitud. Se definen estaciones de clase A que están unidas a los dos anillos y de clase B que solo se unen a uno. La elección de una clase u otra está en la tolerancia a fallos que se desee. También es habitual el empleo de centros de cableado como las MAUs de Token Ring.



La fibra óptica utilizada es multimodo y se utilizan LEDs en lugar de luz láser, ya que con ello se cumplen sobradamente, sin incrementar costes, los requisitos de 100 Mbps y una tasa de error inferior a 1 bit erróneo cada $2{,}5 \cdot 10^{10}$ bits transmitidos.

Se abandona la codificación Manchester (que obligaría a transmitir a 200 Mhz) y se opta por el esquema **4B5B** a 125 Mhz utilizando 16 de las 32 combinaciones de 5 bits para datos, tres para delimitadores, 2 para control, 3 para señales del hardware y ocho no se utilizan. Al no tener señalización de reloj la estabilidad de estos ha de ser al menos del 0,005% para que tramas de hasta 4500 bytes puedan ser enviadas sin error.

Se mantiene el modelo del control de acceso al medio IEEE 802.5, pero con ciertas modificaciones:

a) En IEEE 802.5 no se genera el testigo libre hasta que la estación que lo tiene en uso no recibe la trama transmitida completa. En FDDI, donde puede haber hasta 1000 estaciones y 200 km., el tiempo que se pierde puede ser notable por lo que el testigo libre se genera de forma inmediata tras el envío del último bit de la última

trama que la estación transmite. Por ello, en un anillo grande pueden encontrase varias tramas transmitiéndose simultáneamente.

b) La estructura de la trama es prácticamente igual, salvo que delante del delimitador de comienzo se transmiten al menos 8 bytes de preámbulo para facilitar la sincronización del reloj de recepción.

c) El sistema de prioridades en FDDI esta basado en temporizadores que miden el tiempo de rotación del testigo en el anillo, y se establece un algoritmo semejante al utilizado en IEEE 802.4.

6. APENDCES

6.1 La opción CSMA/DCR en redes Ethernet

Con el fin de salvar el inconveniente de que el tiempo máximo de transmisión de una trama no está acotado, se han buscado alternativas al mecanismo de acceso al medio CSMA/CD. Una de estas alternativa es el mecanismo CSMA/DCR (Deterministic Collision Resolution). El circuito integrado para red Ethernet LAN i82596 de Intel Corporation incluye, junto con el mecanismo de acceso CSMA/CD, este mecanismo alternativo.

Se trata de un método idéntico al estándar de Ethernet, excepto en el mecanismo de resolución de las colisiones. El período de resolución de una colisión se divide en un número programable de "slots" (o ranuras), asignándosele un "slot" a cada estación. El primer "slot" comienza inmediatamente después de que el canal queda libre, tras la señal de "jamming" y el tiempo de espera obligado de canal en silencio entre paquetes. Cada estación sólo emitirá en el "slot" que le corresponda. Cuando se detecta una transmisión se abandona la cuenta de "slots" para reanudarla cuando finalice. Todas las estaciones han de detectar la colisión, incluso las que no participan en ella, de manera que también estas podrán transmitir en su "slot" correspondiente.

Si durante este período de resolución se produjese una nueva colisión, lo cual es imposible si el mecanismo DCR funciona correctamente en todas las estaciones, el proceso se repetiría de nuevo. Una vez alcanzado el último "slot" se vuelve al mecanismo CSMA. El tamaño del "slot" puede ser el mismo que el de la ventana de colisión definida para Ethernet, aunque el circuito integrado LAN i82596 permite programar los parámetros de la red (Slot-Time, Jam-Time, Overhead, etc) con valores distintos a los estándar con el fin de adaptarlos a la configuración de la red. En la figura se puede observar la multiplexación en el tiempo que se realiza mediante este mecanismo.

TEP: Tiempo de espera entre paquetes.

Cuando las condiciones de carga son suficientemente altas, los períodos de colisión se suceden sin períodos intermedios, dando lugar a una especie de multiplexación en el tiempo del canal de transmisión. Esto permite obtener unas expresiones sencillas que representan la utilización máxima del canal S_{max} y el retraso máximo en el acceso de una trama al canal de transmisión T_{max}. El valor de γ, representa el tiempo que transcurre en una colisión desde que la primera estación comienza a transmitir hasta que todas las estaciones detectan el canal libre, y que es aproximadamente igual para todas las estaciones. Los símbolos empleados en las expresiones indicadas son:

N Número de estaciones.

P	Longitud de la información de los paquetes (bits).
H	Longitud de la cabecera y cola de los paquetes (bits).
C	Velocidad de transmisión de la red (bits/s).
τ	Tiempo total de propagación de la señal a lo largo del bus.
$\tau/3$	Tiempo de propagación promedio entre las estaciones.
ε	Tiempo estimado que tarda la estación en detectar la colisión.
TEP	Tiempo de espera entre paquetes.
Jam	Tiempo de duración de la señal de "jamming".

$$S_{max} = \frac{N\frac{P}{C}}{N(\frac{P+H}{C}+\frac{\tau}{3}+TEP)+TEP+\gamma} \;;\; T_{max} = N(\frac{P+H}{C}+\frac{\tau}{3}+TEP)+\gamma \;;$$

$$\gamma = 2\tau + Jam + \varepsilon$$

En este mecanismo existe la necesidad de parametrización de las interfaces para que todas conozcan el número total de ellas conectadas a la red y para que cada una sepa en que "slot" le corresponde transmitir. Esto prioriza las estaciones en cuanto que tras una colisión, unas tendrán la oportunidad de transmitir antes que otras.

6.2 Gestión de la red en IEEE 802.4: Paso de testigo en bus

6.2.1 Mantenimiento del anillo lógico

Una vez que se ha establecido el anillo, cada interfaz de estación mantiene internamente las direcciones de las estaciones predecesoras y sucesoras. El poseedor del testigo en forma periódica genera invitaciones a entrar a estaciones que no se encuentran normalmente en el anillo y que desean ingresar, mediante el envío de una de las tramas *SOLICITO_SUCESOR_1*. La trama proporciona la dirección de la estación emisora, así como la dirección de la estación sucesora. Las estaciones que caen dentro de este rango pueden hacer una solicitud para ingresar (para mantener al anillo con una clasificación en orden descendente de direcciones de estaciones). El ingreso se realiza mediante el envío de una trama *ESTABLECER_SUCESOR* por parte de la estación que se incorpora.

Si ninguna estación solicita ingresar al anillo durante un tiempo de una ventana o ranura (de 2τ, como en el caso del 802.3), la "ventana de respuesta" se cierra y el poseedor del testigo continúa con su actividad normal. Por otra parte, si exactamente una estación solicita ingresar, se introduce al anillo y se convierte en el sucesor del poseedor del testigo.

Si dos o más estaciones solicitan ingresar, sus tramas sufrirán una colisión y quedarán en suspenso, como sucede con el 802.3. El poseedor del testigo pone entonces a funcionar un algoritmo de arbitraje, comenzando con la difusión de una trama *RESUELVE_CONTIENDA*. El algoritmo utilizado emplea dos bits aleatorios obtenidos de la dirección de la estación, los cuales se utilizan para retardar las solicitudes durante 0, 1, 2 y 3 ranuras de tiempo, para así reducir la contienda. Para evitar la situación en la que las estaciones tengan que esperar hasta 3 ranuras de tiempo, y por lo tanto tener una desventaja

permanente, los bits aleatorios se regeneran cada vez que se utilizan, o bien, en forma periódica, cada 50 ms.

La solicitud realizada por nuevas estaciones no debe impedir que se garantice el tiempo máximo de rotación del testigo entre las estaciones. Cada una de ellas tiene un temporizador que se reinicia cada vez que adquiere el testigo. Cuando obtiene el testigo, el antiguo valor del temporizador (es decir, el tiempo previo de la rotación del testigo) se inspecciona, justo antes de que se restablezca el temporizador. Si excede un cierto valor de umbral, significa que ha habido una gran cantidad de tráfico recientemente, por lo que no se podrán aceptar nuevas solicitudes en ese momento. Bajo cualquier condición, sólo una estación podrá entrar durante cada solicitud, con objeto de limitar el tiempo que puede consumirse para el mantenimiento del anillo. No se proporciona ninguna garantía que indique cuanto tiempo debe esperar una estación para unirse al anillo cuando existe un flujo fuerte de tráfico. En la práctica, no debería ser más que unos cuantos segundos.

Dejar el anillo resulta muy sencillo. Una estación X por ejemplo, siendo S y P, su sucesor y predecesor, respectivamente, deja en anillo al transmitir a P la trama *ESTABLECE_SUCESOR,* indicando que, desde ese momento en adelante, su sucesor es S en lugar de X. Entonces X deja de transmitir.

La iniciación del anillo resulta ser un caso especial del proceso de inclusión de nuevas estaciones. Considérese un sistema inactivo, en el cual están apagadas todas las estaciones. Cuando la primera estación se conecta a la línea, se percata de que no hay ningún tráfico durante cierto tiempo. Después de esto transmite una trama con la indicación *RECLAMO_TESTIGO*. Al no escuchar a ninguna estación competir por el testigo, genera un testigo y establece un anillo que la contiene sólo a ella. Periódicamente, este anillo solicita peticiones de nuevas estaciones para unirse al anillo, y a medida que las nuevas estaciones se activan, responderán a estas solicitudes y se unirán al anillo por medio de los algoritmos de contienda mencionados con anterioridad. Normalmente, todas las estaciones que deseen unirse al anillo, serán capaces de hacerlo. Si las dos primeras estaciones se encienden en forma simultánea, el protocolo se hace cargo de esto dejando que luchen por el testigo utilizando el algoritmo anterior.

Debido a los errores de transmisión, o a los fallos de hardware, pueden surgir problemas con el anillo lógico o con el testigo. ¿Que pasará, por ejemplo, si una estación trata de pasar el testigo a otra que ya se ha apagado? Después de pasar el testigo la estación escucha si su sucesora transmite una trama, o bien, transfiere el testigo. Si no toma ninguna de estas dos acciones, se le pasa el testigo por segunda ocasión.

Si también se tiene una respuesta negativa, la estación transmite una trama con la indicación de *QUIEN_SIGUE,* especificando la dirección de su sucesor. Cuando el sucesor de la estación que ha fracasado ve la trama con la indicación *QUIEN_SIGUE,* nombrando a su predecesor, responde mediante el envío de una trama con la indicación *ESTABLECE_SUCESOR,* a la estación cuyo sucesor fracasó, nombrándose a sí misma como el nuevo sucesor. De esta manera, la estación que fracasó queda desalojada del anillo.

Ahora supóngase que una estación falla al pasar el testigo a su sucesor y que también falla para encontrar al sucesor del sucesor, el cual puede estar también apagado. Entonces envía una trama *SOLICITO_SUCESOR_2,* para ver si alguien más está activo todavía. Una

vez más funciona la norma del protocolo de contienda, con todas las estaciones que desean estar en el anillo solicitando ahora un lugar.

Otro tipo de problema que puede ocurrir es que el poseedor del testigo se apaga y se lleva consigo el testigo. Este problema se resuelve mediante el algoritmo de iniciación del anillo. Cada estación tiene un temporizador que se reestablece cada vez que aparece una trama en la red. Cuando este temporizador llega a alcanzar un valor umbral, la estación emite una trama con la indicación *RECLAMO_TESTIGO*, el algoritmo de contienda se encarga de determinar quién gana el testigo.

Todavía existe otro problema que se refiere a los testigos múltiples. Si una estación, que actualmente posea el testigo, se da cuenta de que existe una transmisión de cualquier otra estación, de inmediato abandona su testigo. Si existen dos estaciones con testigo ahora sólo quedará una; si fueran más de dos, este mismo proceso se repetirá tarde o temprano hasta que todas, con la excepción de una de ellas, abandonen su testigo. Si, en forma accidental, todas las estaciones abandonaran su testigo, la falta de actividad, por lo tanto, ocasionará que una o más de ellas traten de reclamar el testigo.

6.2.2 Operación regular de la red

El modo de operación normal de un bus por paso de testigo comienza al finalizar la etapa de inicialización. Todas las estaciones que deseaban unirse al anillo lógico ya lo han hecho, de modo que las tramas se transmiten y reciben sin errores ni pérdidas.

El sistema de prioridades requiere que cada estación mida el tiempo total empleado por el testigo para pasar por todas las estaciones del anillo lógico. Se asigna a los mensajes una clase de acceso (6, 4, 2, 0 y mantenimiento del anillo) y se define un objetivo de tiempo de rotación del testigo para cada clase de acceso, excepto para la clase 6 (debido a que la clase 6 es la de prioridad más alta y ha de transmitirse con independencia del tiempo de rotación del testigo), y para la de mantenimiento del anillo. Los datos se transmiten solamente cuando el tiempo de rotación del testigo medido en la estación para la última iteración del testigo, es menor que el objetivo del tiempo de rotación de testigo para el nivel de prioridad asignado.

Para describir el modo de operación normal, usaremos los ejemplos dados en las figuras de la página siguiente [FREER 88]. Cada figura muestra la operación de una estación concreta desde que recibe el testigo hasta que lo pasa a la siguiente. Se explica a continuación la notación para dichas figuras:

a) El eje horizontal representa unidades arbitrarias de tiempo.

b) Las tramas sobre el bus se representan como bloques rectangulares:

T = Trama del testigo.

D= Trama de información o de datos con la clase de acceso indicada por el sufijo.

S = Solicitud de sucesor.

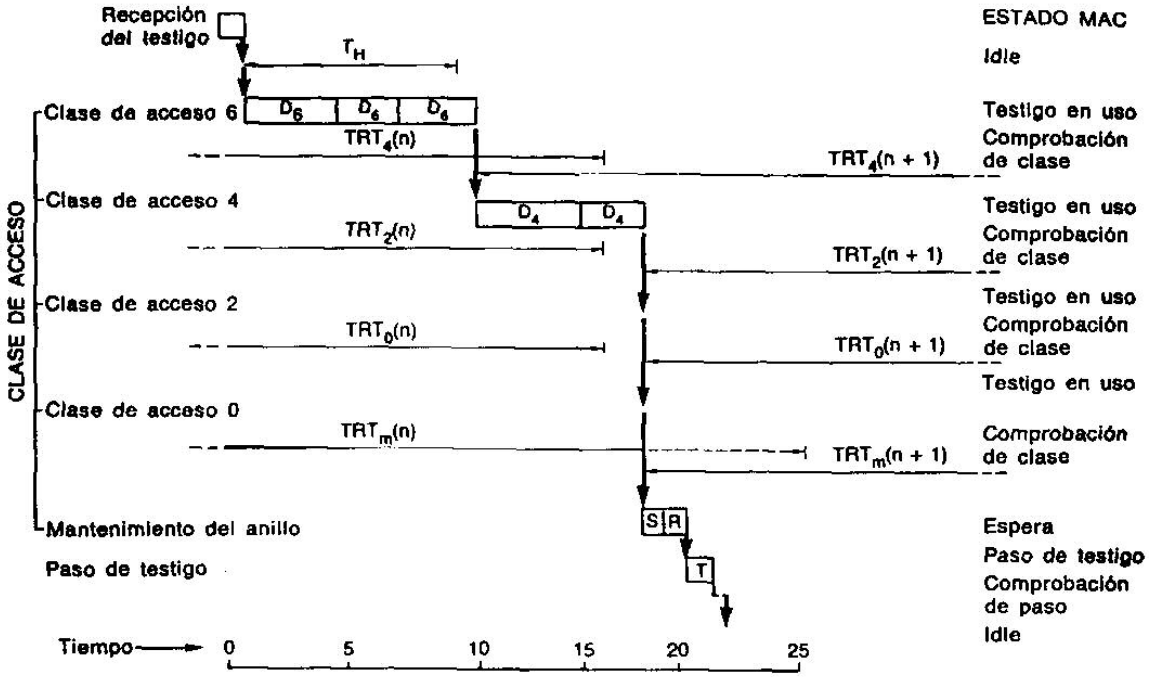
R = Ventana de respuesta.

c) Las duraciones de los temporizadores se muestran como líneas horizontales.

d) El etiquetado de los temporizadores es como sigue:

TH = Tiempo de mantenimiento del testigo para alta prioridad.

TRTa(n) =Tiempo de rotación del testigo para la clase de acceso de prioridad 'a' y para la rotación 'n'. La clase de acceso 'm' se emplea para mantenimiento del anillo.



En la primera figura, la estación está en estado DESOCUPADO mientras recibe el testigo. Cuando reconoce el testigo, la estación carga su temporizador de mantenimiento de testigo con el valor del tiempo de mantenimiento de alta prioridad, ajusta la clase de acceso a 6, y cambia el estado a testigo en uso. Esto ocurre en la unidad de tiempo 0 en la figura. La estación tiene datos de alta prioridad (clase de acceso 6) para enviar, y envía tres tramas de datos (D6). Las tramas de datos podrán ser de longitudes diferentes y podrán estar destinadas a direcciones diferentes. Cuando va a entrar en el estado de TESTIGO EN USO por cuarta vez, la estación encuentra que ha finalizado su período de mantenimiento de testigo, por lo que no puede enviar más tramas de datos D6. La estación cambia su clase de acceso a 4 y pasa al estado COMPROBACION DE CLASE DE ACCESO. Esto sucede en la unidad de tiempo 9 de la primera figura.

Cuando la estación entra en el estado COMPROBACION DE CLASE DE ACCESO, carga su temporizador de mantenimiento de testigo con el valor residual que tenga el temporizador de rotación de testigo para la clase de acceso 4 (TRT4), inicializa TRT4 con el objetivo de tiempo de rotación de testigo correspondiente, y vuelve al estado TESTIGO EN USO. En la figura, corresponde a una fracción de tiempo después de la unidad de tiempo 9.

La estación tiene datos con clase de acceso 4 para enviar y transmite dos tramas D4. Encuentra entonces que su temporizador de testigo ha finalizado (antes de TRT4), y debe interrumpir la transmisión de datos. Cambia ahora a la clase de acceso 2 y entra en el estado de COMPROBACION DE CLASE DE ACCESO. Esto sucede en la unidad de tiempo 17 de la figura.

La figura muestra que los temporizadores de rotación de testigo para las clases de acceso han finalizado ya al llegar a la unidad de tiempo 17, por lo que la estación pasa por encima de esas clases de acceso sin enviar tramas. Cuando la clase de acceso se ha reducido a la de mantenimiento del anillo, la estación entra en el estado de COMPROBACION DE CLASE DE ACCESO, y el temporizador de rotación del testigo para esta clase no ha expirado aún. La estación inicializa el temporizador de rotación del testigo para la clase de mantenimiento del anillo y entra en el subestado de "solicitud de sucesor" del estado PASO DE TESTIGO. En la figura corresponde a una fracción de tiempo después de la unidad 17.

En el subestado PASO DE TESTIGO (solicitud de sucesor), la acción usual es enviar una trama de control *SOLICITO_SUCESOR_1* e iniciar una ventana de espera de respuesta de duración simple. Esto permite identificarse a cualquier nueva estación con una dirección entre la actual y la siguiente. Un caso especial es cuando la dirección de la siguiente estación del anillo lógico es mayor que la de la estación actual (esto es, cuando el anillo de direcciones descendentes retorna a la dirección inicial). En este caso se envía una trama de control *SOLICITO_SUCESOR_2* y comienza una ventana de espera de respuesta de doble duración.

La estación espera el tiempo marcado por el temporizador de la ventana de respuesta en el estado denominado ESPERA DE RESPUESTA. En un caso normal, no hay estaciones nuevas y no habrá respuestas. La estación retorna entonces al subestado PASO DE TESTIGO (paso de testigo). Se envía la trama del testigo, y la estación se asegura (en estado COMPROBACION DE PASO DE TESTIGO) de que ha sido enviada una trama válida por la estación sucesora. En un caso normal, la estación puede entonces volver al estado DESOCUPADO habiendo manejado el testigo sin percances.

La figura inferior ilustra lo que podrá ocurrirle a la misma estación cuando recibe el testigo de nuevo. Las diferencias con la figura superior son las que siguen:

a) Sólo hay una trama de datos de alta prioridad para transmitir en TH.

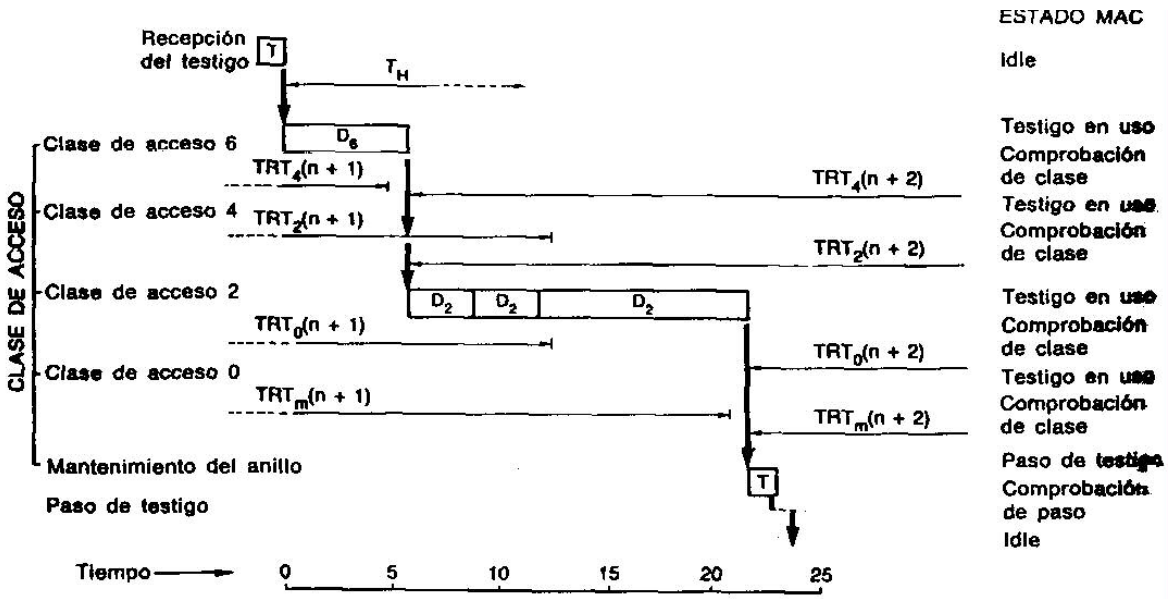
b) TRT4 expira antes de entrar en la clase de acceso 4, por lo que no pueden enviarse datos con dicha clase de acceso.

c) TRT2 permite que se envíen algunas tramas de acceso 2.

d) TRT0 evita que se envíen tramas con clase de acceso 0.

e) TRTm no permite mantenimiento del anillo, de modo que el estado de PASO DE TESTIGO comienza con el subestado de paso de testigo, omitiéndose el subestado de solicitud de sucesor.

Sin entrar en mucho detalle para conocer cómo se manejan los diferentes temporizadores, deber quedar claro que, con el ajuste apropiado de éstos, se puede asegurar que una fracción del tiempo total de posesión del testigo puede asignarse, con plena garantía, al tráfico con prioridad 6. Las prioridades más bajas tendrán que conformarse con lo que queda después de dicha asignación. Si las colas de mensajes con prioridad alta de las estaciones no necesitan usar todo el tiempo asignado, las subestaciones con menor prioridad pueden hacer uso de esta parte, de tal forma que no se desperdicie.



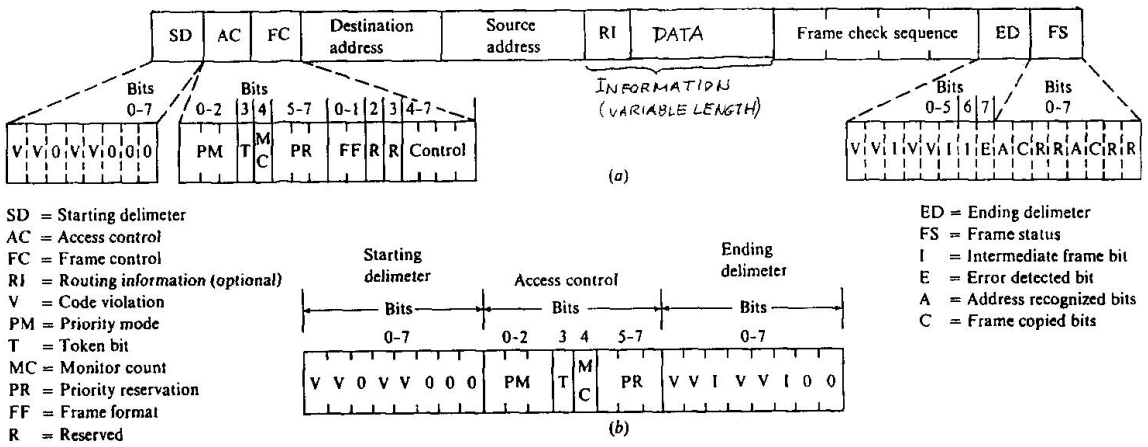
6.3 Gestión de la red en IEEE 802.5: Paso de testigo en anillo

6.3.1 Mecanismo del Paso de Testigo en Anillo

Hay dos modos de operación en las interfaces del anillo, uno para escuchar y el otro para transmitir. En el modo de escucha, los bits de entrada simplemente se copian con un retardo de tiempo de 1 bit. En el modo de transmisión, que sólo ocurre después de que un testigo libre haya sido capturado, la interfaz rompe la conexión existente entre la entrada y la salida, introduciendo sus propios datos al interior del anillo tras el testigo que acaba de marcar como ocupado (poniendo a 1 el bit T del control de acceso AC). La estación ha de tener la capacidad de conmutar entre los modos escucha y transmite en el tiempo de 1 bit.

Cuando la trama llega a la interfaz de una estación con la dirección del destinatario, la interfaz pone a uno el bit A, del octeto de estado de trama FS, durante su paso. Si, al mismo tiempo, la interfaz copia la trama en la estación, entonces también pone a uno el bit C del mismo octeto. Una estación puede llegar a fallar durante el proceso de copiado de una trama, como consecuencia de falta de espacio en la memoria temporal, o bien, debido a otras razones. Al revisar los bits A y C, el transmisor se puede encontrar tres combinaciones posibles:

1. A = 0 y C = 0: cuando el destinatario no está presente o no está encendido.
2. A = 1 y C = 0: cuando el destinatario está presente, pero la trama no es aceptada.
3. A = 1 y C = 1: cuando el destinatario está presente y la trama está copiada.



Con esto el acuse de recibo es automático para cada una de las tramas. Si se llega a rechazar una trama, estando presente la estación, el transmisor tiene la opción de intentar enviarla de nuevo más tarde. La trama continúa alrededor del anillo, cerrando un ciclo completamente cuando llega de nuevo a la estación transmisora. En condiciones normales, el primer bit de la trama regresará a la estación que transmite, antes de que se haya transmitido la trama completa. Sólo un anillo muy grande podría contener dentro una trama corta. Por ello, la estación transmisora deberá vaciar el contenido del anillo mientras continua transmitiendo.

A medida que regresan los bits que se han propagado alrededor del anillo, el transmisor los retira del anillo directamente. La estación transmisora puede optar por almacenarlos, con objeto de compararlos con los datos originales para controlar la fiabilidad del anillo, o bien, desecharlos. Esta arquitectura de anillo no impone ningún límite con respecto al tamaño de las tramas, dado que la trama completa nunca aparece en el anillo en un instante dado. Después de que la estación ha terminado de transmitir el último bit de su última trama, deberá regenerar el testigo libre. Cuando el último bit de la trama haya recorrido la trayectoria y haya regresado, se debe retirar, y la interfaz deberá conmutarse inmediatamente al modo de escucha, para evitar perder el testigo, en caso de que ninguna otra estación lo haya recogido.

Una estación puede mantener el testigo durante el "tiempo de retención de testigo", que es de 10 ms, a menos que en una determinada instalación se establezca un valor diferente. Si hay suficiente tiempo, para enviar más tramas, después de haberse transmitido la primera de ellas, éstas también podrán enviarse. Después de haberse transmitido todas las tramas que estaban pendientes, o bien, que la transmisión de otra trama llegara a exceder el tiempo de retención del testigo, la estación regenerará la trama del testigo y la colocará sobre el anillo.

El delimitador de fin ED contiene un bit E que se levanta siempre que cualquier interfaz detecte un error (por ejemplo, un patrón que no se encuentre en el código Manchester, en un lugar donde esto no sea permitido). También contiene un bit que puede utilizarse para marcar la última trama en una secuencia lógica, como si fuera un bit de fin de archivo.

El protocolo 802.5 tiene un planteamiento muy elaborado con respecto al manejo de tramas con distintas prioridades. El octeto de control de acceso, AC, establece la prioridad

del testigo, PM. Cuando una estación desee transmitir una trama con prioridad *n,* deber esperar hasta el momento en que logre capturar un testigo cuya prioridad sea menor que, o igual a *n.* Más aún, cuando una trama de datos pasa, una estación dada puede tratar de reservar el siguiente testigo al escribir la prioridad de la trama que desea transmitir en los bits de reserva, PR, de la trama. Sin embargo, si ya se hubiera reservado una prioridad más alta, la estación no podrá llegar a hacer una reserva. Cuando la trama actual se haya terminado, el siguiente testigo se generar con la prioridad que había quedado reservada.

Este mecanismo se comportaría aumentando siempre la prioridad de reserva a niveles cada vez más altos. Para eliminar este problema, el protocolo contiene algunas reglas complejas. La esencia de la idea es que, en el momento de elevar la prioridad de reserva, la estación también se haga responsable de disminuir de nuevo la prioridad de ese campo, cuando se haya fijado ésta en el campo PM.

Este planteamiento de prioridad es substancialmente diferente al correspondiente al paso de testigo en bus, en el cual cada estación siempre consigue un ancho de banda razonable, sin importar lo que las demás estaciones están haciendo. En el caso del paso de testigo en anillo, se puede observar que, una estación con tramas de baja prioridad, puede estar esperando de manera indefinida a que aparezca un testigo con baja prioridad.

6.3.2 Mantenimiento del anillo

El protocolo de paso de testigo en bus realiza el mantenimiento del anillo de una manera completamente descentralizada mientras que el protocolo de paso de testigo en anillo lo hace de una forma muy diferente. Cada anillo físico tiene una estación supervisora o monitor que se encarga de inspeccionar el anillo. Si el monitor se cae, un protocolo de contienda asegura que otra estación sea elegida como supervisora inmediatamente. Cada estación tiene la capacidad de llegar a convertirse en estación supervisora. Mientras que el supervisor funcione de manera adecuada, solamente él se hace responsable de ver que el anillo opere en forma satisfactoria.

Campo de control de la trama	Nombre	Significado
00000000	Prueba de duplicado de dirección	Prueba sobre si dos estaciones tienen la misma dirección
00000010	Baliza	Utilizado para localizar rupturas en el anillo
00000011	Reclamo de testigo	Intento para llegar a ser supervisor
00000100	Purga	Reiniciar el anillo
00000101	Supervisor activo presente	Emitido periódicamente por el supervisor
00000110	Supervisor alerta presente	Anuncia la presencia de supervisores potenciales

Cuando el anillo empieza a funcionar, una estación que se da cuenta de que no existe ninguna estación supervisora, transmite una trama de llamada *RECLAMO_DE_TESTIGO.* Si esta trama viaja a través del anillo, antes de que cualquier otra trama de *RECLAMO DE TESTIGO*se haya transmitido, el emisor se convierte en la nueva estación supervisora.

Entre las responsabilidades que adquiere el supervisor se encuentran: el vigilar que el testigo no se haya perdido, el tomar decisiones cuando se llegue a romper el anillo, la

limpieza del anillo cuando aparezcan tramas mutiladas y el observar la presencia de tramas huérfanas.

Para detectar los testigos perdidos, la estación supervisora cuenta con un temporizador cuyo valor se fija en el tiempo máximo que tarde el testigo en una rotación completa, por ejemplo, el caso en el que cada estación utilice todo el tiempo de retención del testigo. Si este temporizador se consume, la estación supervisora vacía la información del anillo y emite un nuevo testigo.

Cuando aparece una trama mutilada, la estación supervisora puede detectarla por medio de su formato o código de redundancia inválidos, para después abrir el anillo y vaciar su información, emitiendo un nuevo testigo en el momento en que se acabe de limpiar el anillo.

Una trama huérfana aparece cuando una estación transmite una trama corta íntegramente sobre un anillo muy largo, y después falla o se desactiva, antes de terminar de vaciar la trama. Si nada se hiciera, la trama circularía de forma indefinida. La estación supervisora detecta las tramas huérfanas poniendo a uno el bit de control de monitor MC en el octeto de control de acceso AC, que originalmente siempre se transmite con valor cero, cuando una trama pase a través de él. Si al regresar la trama continua este bit puesto a uno, algún fallo ha ocurrido ya que la misma trama ha pasado dos veces por el supervisor sin que haya sido retirada. Es entonces el supervisor quien lo hace y genera un testigo libre.

Otra función de la estación supervisora se refiere a la longitud del anillo. El testigo tiene 24 bits de longitud, lo cual significa que el anillo deber ser lo suficientemente largo para retener los 24 bits. Si el retardo de un bit que existe en las estaciones, más la longitud del cable, no llegan a sumar 24 bits, la estación supervisora inserta bits de retardo adicional, con objeto de que el testigo pueda continuar circulando.

Una función de mantenimiento que no puede ser hecha por la estación supervisora, es el hecho de localizar las rupturas en el anillo. Cuando una estación nota que alguno de sus vecinos no responde, transmite una trama de *BALIZA* indicando la dirección de la estación presumiblemente inactiva. Cuando esta señal se haya propagado tan lejos como pueda, entonces será posible ver cuantas estaciones están inactivas y así poder retirarlas del anillo, mediante el uso de relés, ubicados en la central de cableado, de forma completamente automática.

El comité del 802.4 diseño un sistema en el que la estación poseedora el testigo tuviera poderes especiales (por ejemplo, permiso para pedir solicitudes de unirse al anillo), sin que ninguna estación fuese diferente de las otras (por ejemplo tuviera una responsabilidad administrativa asignada para el mantenimiento).

El comité del 802.5, por otro lado, pensó que el hecho de tener una estación de supervisión centralizada para manejar los testigos perdidos, las tramas huérfanas y cosas por el estilo, hacían todo esto más fácil. Además, en un sistema normal, las estaciones difícilmente llegan a fallar, así que, el hecho de tener que soportar en ocasiones la contienda para una nueva estación supervisora, no llega a ser un gran problema. El precio que se paga es que si la estación supervisora no funciona correctamente, pero continua emitiendo periódicamente tramas de control indicando *SUPERVISION_ACTIVA_PRESENTE,* ninguna estación llegar jamás a sustituirla. Las estaciones supervisoras no pueden ser impugnadas.

La diferencia en el planteamiento tiene lugar a partir de las distintas áreas de aplicación que tenían en mente los dos comités. El del 802.4, por ejemplo, estaba pensando en términos de utilización para ordenadores que controlan máquinas dentro entornos industriales, donde los fallos de la red podrían provocar daños muy serios y tenían que impedirse a toda costa. Por otra parte, el comité del 802.5; estaba principalmente interesado en la automatización de oficinas, en donde la existencia de algún fallo, podrá tolerarse como precio por tener un sistema mucho más sencillo. Si el 802.4 es, en efecto, más fiable que el 802.5, es materia de discusión.

7. BIBLIOGRAFÍA

Bibliografía consultada para la realización de este capítulo:

[FREER 88]
Freer, J. (1988).
Introducción a la tecnología y diseño de Sistemas de Comunicaciones y Redes de Ordenadores.
Anaya Multimedia.

[HALSALL 95]
Halsall, F. (1995).
Data Communications, Computer Networks and Open Systems.
Addison-Wesley.

[STALLINGS 97]
Stallings, W. (1997).
Comunicaciones y redes de computadores, 5ª ed.
Prentice Hall Iberia.

[SLOMAN 87]
Sloman, M.; Kramer, J. (1987)
Distributed Systems and Computer Networks.
Prentice-Hall.

[TANENBAUM 96]
Tanenbaum, A.S. (1996).
Computer Networks. (Third Edition).
Prentice-Hall.