

## Capítulo 6: Redes de difusión: LANs, Satelitales e Inalámbricas. Subcapa de acceso al medio(MAC).

**Objetivos:** Describir las características principales de las redes de difusión. Explicar los orígenes y principales protocolos de redes LAN. Establecer las características de las redes satelitales e inalámbricas. Describir la implementación de LANs: las diversas maneras de clasificarlas (topología, método de acceso al medio, velocidad y tipo de transmisión) y los principales componentes de software y de hardware. Enumerar y describir los distintos estándares en LANs: 802.3,802.4, 802.5,FDDI y Fibre Channel. Explicar la necesidad de mayores velocidades y los estándares que responden a ella: 100 Base-T,100VG-AnyLAN,100 Base-FX, Gigabit Ethernet y 10Gigabit Ethernet..

### 6.1.-Introducción.

En la **Sección 5.2** se describió brevemente la clasificación de la redes en base a su arquitectura y a la técnica de transferencia de información, en base a ello mencionamos las **redes conmutadas** y las **redes de difusión**, en esta Sección nos ocuparemos de estas últimas, que allí solo enumeramos, y de sus protocolos, trataremos entonces de:

1. **Redes de área local(LANs).**
2. **Redes por satélite.**
3. **Redes inalámbricas.**

La característica básica de la redes de difusión es: **el medio es compartido**, lo que significa que todos los integrantes de la red utilizan el mismo medio y todos ellos reciben la información emitida, por lo que el problema básico de este tipo de redes es establecer quién tiene derecho a utilizar el canal en un momento dado, puesto que varios usuarios pueden querer hacerlo simultáneamente, ó con muy pequeños intervalos de tiempo, y por lo tanto **competirán** por el medio. Un símil típico es una reunión ó asamblea donde es necesario establecer reglas para el uso de la palabra, en una red la situación es más complicada pues no se puede alzar la mano ó dar una señal convenida para hablar, sin embargo existen diversos **protocolos** que permiten enfrentar este problema de **contienda por el acceso al medio**, y estos protocolos tienen características distintas según de cual de los tres tipos enumerados se trate y además dentro de cada uno de ellos hay muchos **dialectos** ó protocolos específicos.

### 6.2.-Las redes LAN.

Al comienzo del Capítulo 4 se dieron las características de las redes LAN:

- **Su campo de acción es no mayor de unos pocos kilómetros, típicamente un edificio ó un sector de edificios.**
- **Pertenecen a una sola organización.**

Esto conduce a estas consecuencias importantes:

- **La organización puede tender su propio cable de gran ancho de banda.**
- **La velocidad total de transmisión es de muchos Mbps y aún varios Gbps.**
- **Los protocolos son mucho más simples**, al disponerse de gran ancho de banda los diseñadores no deben esforzarse por obtener grandes rendimientos.
- **El cable de la LAN es un elemento muy confiable**, y la tasa de errores será mil veces inferior a una WAN, lo que simplifica aún más a los protocolos pues el manejo de errores no debe ser hecho en todas las capas sino solo en las superiores, haciendo que los de las inferiores sean más sencillos.
- **Los dispositivos de la red son "peers"**,cualquier dispositivo puede iniciar un intercambio de datos con cualquier otro dispositivo(no se confunda con uno de los dos modelos de redes:"peer" to"peer" y "cliente-servidor").

Cuando asignamos un solo canal a varios usuarios estos compiten por él, una solución para evitarlo sería subdividirlo en frecuencia (FDM) ó en el tiempo (TDM) y asignar estáticamente una de esas partes, pero ocurre que esto es altamente ineficiente ya que el número de usuarios varía y aún cuando tuviesemos un número fijo  $N$  y asignásemos un trozo a cada uno, estos no siempre están transmitiendo y su ancho de banda simplemente se perdería. Además en las redes de computadoras el tráfico se presenta en ráfagas (a veces con relaciones 1000:1) lo que indica que la mayoría de los canales está inactivo la mayor parte del tiempo. Al estudiar la Teoría de Colas se concluyó que FDM ó TDM están en franca desventaja frente a un medio compartido y ello es lo que produjo el auge de las LANs cuya evolución describiremos en lo que sigue, estas técnicas son usadas también en las MAN.

### 6.3.-Asignación dinámica de canal.

Vamos a establecer con cuidado el modelo de trabajo de esta área:

1. **Modelo de estación:** El modelo consiste de  $N$  **estaciones**, cada una generando **tramas**<sup>1</sup> para ser transmitidas. La probabilidad de que una trama sea generada en un intervalo de tiempo  $\Delta t$  es  $\lambda \Delta t$ , donde  $\lambda$  es una constante que representa la velocidad de llegada de nuevas tramas. Una vez que se genera una trama, la estación se bloquea hasta que la trama ha sido transmitido exitosamente.
2. **Suposición de un solo canal:** existe un solo canal para todas las comunicaciones. Todas las estaciones transmiten y reciben a través de este canal y son equivalentes por lo menos en lo que se refiere al hardware, aunque puedan asignarse algunas prioridades mediante el software de los protocolos.
3. **Suposición de colisiones:** si dos o más tramas son transmitidas simultáneamente, se superpondrán en el tiempo y se convierten en ininteligibles. A este evento se le llama colisión. Todas las estaciones pueden detectar colisiones y una trama colisionada debe ser retransmitida. No hay más errores que los generados por colisiones.
4. **Tiempo :**
  - **continuo:** La transmisión de tramas puede darse en cualquier momento. No hay un reloj maestro que divide el tiempo en intervalos.
  - **discreto:** El tiempo se divide en intervalos discretos llamados ranuras ó slots. Las transmisiones de tramas siempre comienzan al principio de una ranura. Un ranura puede tener 0, 1 o más tramas representando un canal vacío, una transmisión exitosa o una colisión respectivamente.
5. **Portadora:**
  - **Con detección de portadora (carrier sense):** las estaciones pueden saber si el canal está siendo usado antes de transmitir. Si detectan que está en uso, ninguna estación transmite hasta que esté libre.
  - **Sin detección de portadora (no carrier sense):** las estaciones no pueden saber si el canal está en uso antes de transmitir. Sólo pueden saber después de transmitir si la transmisión fue exitosa o no.

Estas premisas merecen algunos comentarios, la primera implica que las estaciones son independientes, generan trabajo a velocidad constante y son monoproseso (cuando está bloqueada no puede generar nuevo trabajo). En lo que hace al tiempo este tiene dos alternativas : continuo ó ranurado, cada uno de ellos dará lugar a sistemas diferentes. Lo mismo ocurre con la detección de portadora, cada alternativa da lugar a un sistema diferente.

---

<sup>1</sup> La información para su transmisión es dividida en grupos ó paquetes de bits, a ellos se agregan al comienzo y al final bits ó grupos de bits con diversos fines. Este conjunto se denomina **trama** (frame)..

#### 6.4.-Protocolos de Acceso Múltiple.

En la década del 70 las necesidades de comunicación en una geografía tan especial como la de Hawai hizo que en su Universidad el Profesor Norman Abramson y algunos colegas diseñaran un protocolo para resolver el problema de asignación de canal en un sistema de radio terrestre, sin embargo la idea básica es aplicable a cualquier sistema que tenga usuarios compitiendo por un solo canal, este sistema se denominó ALOHA, lo que no es extraño dado su origen.

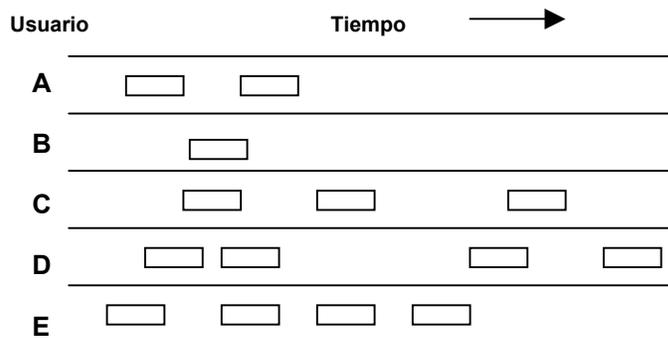
##### 6.4.1.- ALOHA.

Hay dos tipos de ALOHA, puro y ranurado.

##### 6.4.1.1.- ALOHA puro.

La idea es simple: dejemos que las estaciones transmitan cuando quieran. Van a haber colisiones, pero cada estación puede saber si la trama que envió colisionó ó no pues escucha la salida del canal (en una LAN la realimentación es inmediata, en un sistema satelital tarda cerca de 270ms). Si hubo colisión, los emisores esperan cada uno un tiempo aleatorio (de otro modo tendríamos colisiones una y otra vez) y tratan nuevamente. Se da una colisión aunque solamente se haya solapado el último bit de una trama con el primero de otra.

ALOHA tiene rendimiento máximo cuando las tramas son de tamaño fijo, por ello en la **Figura 6.1** se muestran tramas de igual longitud emitidas en forma arbitraria.



**Figura 6.1.-Emisión de tramas en ALOHA puro.**

¿Cuál es la eficiencia de este ALOHA? Eficiencia es el porcentaje de tramas que se escapan de colisionar, o sea que llegan exitosamente.

Asumimos un número infinito de estaciones que cumplen con el modelo de estación dado más arriba. Llamamos "tiempo de trama" al tiempo que toma transmitir una trama, será el largo de la trama dividido por la velocidad en bps.

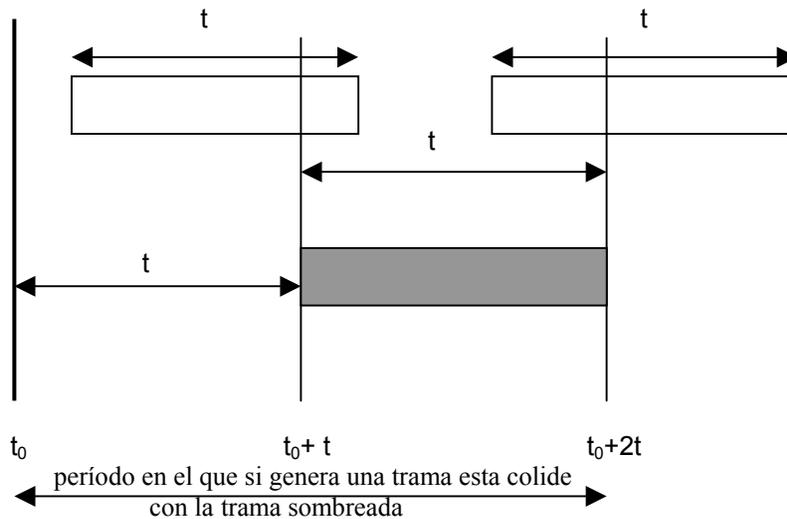
Suponemos que una población infinita de estaciones genera tramas de acuerdo a una distribución de Poisson con media en  $S$  tramas por tiempo de trama,  $S$  se denomina **caudal**. (Si la población no fuera infinita,  $S$  decrecería con cada estación que se bloquea).

Si  $S > 1$ , las estaciones generan más tramas de las que el canal puede manejar, y casi todas las tramas producirían colisiones, así que suponemos que  $0 < S < 1$ .

Además de las tramas nuevas, deben ser retransmitidas también las tramas viejas que sufrieron colisiones. Suponemos que la probabilidad de  $k$  intentos de transmisión por tiempo de trama, incluyendo tramas nuevas y viejas, es una distribución de Poisson con media  $G$  por tiempo de trama.

Obviamente  $G \geq S$ . Si no hay mucha carga ( $S \approx 0$ ), no vamos a tener muchas colisiones, por lo tanto habrán pocas retransmisiones, y será que  $G \sim S$ . Si hay mucha carga vamos a tener muchas colisiones, así que  $G > S$ . Bajo cualquier carga, el caudal ( $S$ ) no es más que la carga real ( $G$ ) multiplicada por la probabilidad de que una transmisión tenga éxito, por lo tanto  $S = G P_0$ , donde  $P_0$  es la probabilidad de que una trama sufra cero colisiones.

¿Bajo qué condiciones llega bien una trama?. Sea  $t$  el tiempo requerido para enviar una trama, establezcamos un origen de tiempos  $t_0$  de manera que **una** estación comience a transmitir en un tiempo  $t_0+t$ . Si alguna **otra** estación comienza a generar una trama entre  $t_0$  y  $t_0+t$ , el final de esta trama va a colisionar con el principio de la anterior. De igual forma, si una estación comienza a generar una trama entre  $t_0+t$  y  $t_0+2t$  pasa lo mismo. El tiempo vulnerable de la trama es de dos tiempos de trama. Esta situación se muestra en la **Figura 6.2**.



**Figura 6.2. Período en la trama sombreada es vulnerable a colisiones**

La probabilidad de que  $k$  tramas sean transmitidos durante un tiempo de trama, tal como ya se dijo, está dada por la distribución de Poisson:

$$P(k) = G^k e^{-G}/k! \tag{6.1}$$

así que la probabilidad de tener 0 tramas en un tiempo de trama es  $e^{-G}$ . En un intervalo de dos tiempos de trama, el promedio de tramas generadas es  $2G$ . La probabilidad de que no haya ninguna transmisión durante el período de vulnerabilidad es:

$$P_0 = e^{-2G} \tag{6.2}$$

Usando  $S = GP_0$  tenemos ,

$$S = G e^{-2G} \tag{6.3}$$

En resumen: se generan  $G$  tramas por tiempo de trama, tienen éxito  $S$  tramas por tiempo de trama (caudal ó rendimiento). La proporción de éxitos es  $S/G$ . Las que tienen éxito son las que no son colisionadas, si se envía un trama de prueba la probabilidad de que los demás usuarios estén en silencio durante dos periodos consecutivos es  $e^{-2G}$ , ó sea  $P_0$ , probabilidad de que no se genere ninguna trama (cero tramas) en dos tiempos de trama.

### PROCOLOS ALOHA

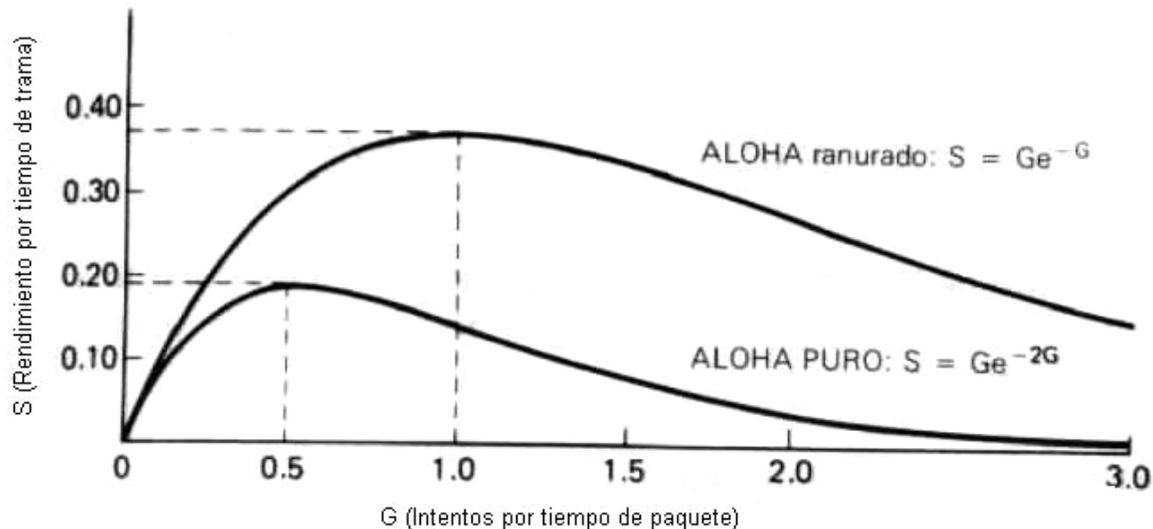


Figura 6.3 Rendimiento(caudal) versus el tráfico(G) para ALOHA .

La relación entre el tráfico y el caudal (rendimiento) se ve en la Fig. 6.3. El rendimiento máximo ocurre en  $G = 0.5$  intentos por tiempo de trama, con  $S = 1/(2e)$ , que es 0.184. En otras palabras, en el mejor de los casos la utilización del canal es del 18%.

#### 6.4.1.2.-ALOHA ranurado.

Una mejora a ALOHA es hacer que el tiempo sea discreto, a idea corresponde a Roberts(1972). Se coloca una estación que emite una señal cada ciclo y sirve como reloj maestro, a cada estación solo se le permite transmitir cuando comienza la ranura siguiente al momento en que en la estación se pulsa el "retorno de carro" para ordenar la transmisión. Debido a que ahora las estaciones tienen que esperar el principio de una ranura (slot) para transmitir, el período de vulnerabilidad se reduce a la mitad. La probabilidad de que no haya tráfico en una ranura es  $e^{-G}$ , de modo que es:

$$S = G e^{-G}$$

6.4

El ALOHA ranurado tiene su máximo rendimiento para  $G = 1$ , con un rendimiento de  $S = 1/e$  que es 0.368 o sea el doble del ALOHA puro. Sin embargo, lo mejor que podemos esperar del ALOHA ranurado es: 37% de ranuras vacías, 37% de transmisiones exitosas y 26% de colisiones. Si operamos en un valor más alto de  $G$ , reducimos el número de ranuras vacías, pero aumentan exponencialmente el número de colisiones. Para ver esto calculemos el número promedio de retransmisiones por trama:

La probabilidad de que una trama evite una colisión es la probabilidad de que ningún otro usuario transmita en un slot, que es  $e^{-G}$ . La probabilidad de una colisión será entonces  $1 - e^{-G}$ .

La probabilidad de que una transmisión requiera exactamente  $k$  retransmisiones es la probabilidad de que  $k-1$  transmisiones fallen (colisionen) por la probabilidad de que la  $k$ -ésima transmisión tenga éxito, y resulta:

$$P_k = e^{-G} (1 - e^{-G})^{k-1} \quad 6.5$$

El número esperado de transmisiones ( $E$ ) por trama enviada es:

$$E = \sum k P_k = \sum k e^{-G} (1 - e^{-G})^{k-1} = e^{-2G} \quad 6.6$$

Como resultado de la dependencia exponencial que tiene  $E$  de  $G$ , pequeños aumentos en la carga pueden reducir drásticamente el rendimiento.

## 6.5.-Protocolos actuales de LAN.

El problema con ALOHA es que no toma en cuenta si alguien está transmitiendo para comenzar a hacerlo. Estos protocolos que veremos a continuación primero verifican el canal (escuchan a ver si hay una portadora ó sea una transmisión) y luego toman acciones dependiendo del estado del canal, intuitivamente percibimos que esto será una mejora respecto de ALOHA.

### 6.5.1.-Protocolos Carrier Sense Multiple Access (CSMA).

#### 6.5.1.1.- CSMA 1-persistente.

Cuando una estación va a enviar una trama, primero verifica el canal. Si el canal está ocupado, espera hasta que se desocupe. Cuando detecta que el canal está vacío, transmite la trama. Si ocurre una colisión, espera un tiempo aleatorio y empieza otra vez.

Es llamado 1-persistente, debido a que cada estación transmite con probabilidad 1 al detectar un canal vacío.

Una consideración importante es el tiempo de propagación. Hay una pequeña probabilidad, de que justamente después que una estación empieza a transmitir, otra estación esté lista para mandar una trama y verifique el canal. Si la señal de la primera estación no ha llegado todavía a la segunda, la segunda va a detectar un canal vacío y va a transmitir, causando una colisión. Mientras

más largo es el tiempo de propagación, más importante es este efecto y resulta peor el rendimiento del protocolo.

Aun si el tiempo de propagación es cero, pueden haber colisiones. Si dos máquinas verifican la ocupación del canal al mismo tiempo y lo encuentran ocupado por una tercera, ambas van a esperar a que termine esa transmisión y van a empezar a transmitir al mismo tiempo, causando una colisión.

#### 6.5.1.2.- CSMA no persistente.

En este protocolo se verifica el canal, si está vacío enviamos la trama, pero si está ocupado, esperamos un tiempo aleatorio y repetimos el proceso. Se observa que este protocolo es menos codicioso que el precedente pues no está verificando el canal continuamente para usarlo apenas termine la transmisión presente, se presupone que esto conduce a mejor utilización del canal pero a mayores retardos que el CSMA 1-persistente.

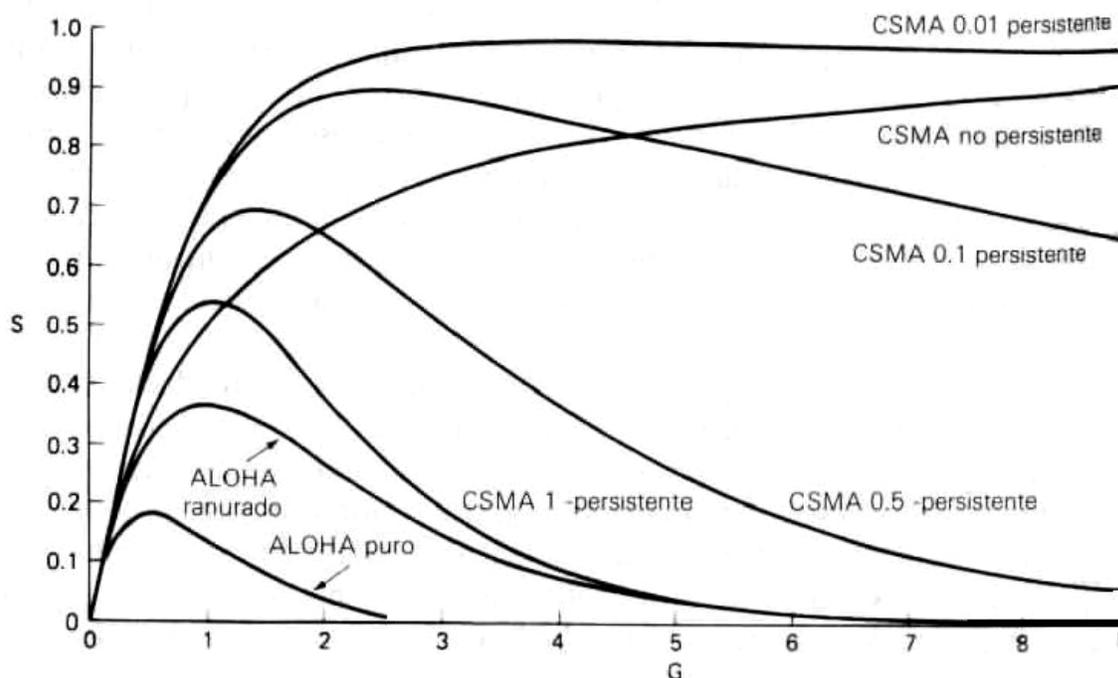
#### 6.5.1.3 CSMA p-persistente.

Este protocolo se aplica a canales ranurados (tiempo discreto), cuando una estación está lista para transmitir, verifica el canal, si está vacío transmite con probabilidad  $p$  y retarda la transmisión, hasta la siguiente ranura con probabilidad  $q = 1 - p$ . Si la siguiente ranura está vacía transmitimos o esperamos con probabilidades  $p$  y  $q$  respectivamente. El proceso se repite hasta que la trama sea enviada ó se detecte que el canal está ocupado (otra estación empezó a

transmitir). Si el canal está ocupado, actúa como si hubiera ocurrido una colisión: se espera un tiempo aleatorio y se repite el proceso.

Si inicialmente el canal estaba ocupado, esperamos una ranura de tiempo y aplicamos el mismo procedimiento.

La **Figura 6.4** es muy útil para comparar el rendimiento (caudal  $S$ ) versus el tráfico (carga  $G$ ) para los 3 protocolos CSMA (el  $p$ -persistente con varios grados de persistencia), ALOHA puro y ALOHA ranurado.



**Figura 6.4.** Rendimiento (caudal  $S$ ) versus el tráfico (carga  $G$ ) para los 3 protocolos CSMA (el  $p$ -persistente con varios grados de persistencia), ALOHA puro y ALOHA ranurado.

### 6.5.2.-CSMA con detección de colisiones (CSMA/CD).

La mejora introducida por CSMA respecto de ALOHA consiste en “escuchar” el canal antes de transmitir y esto se hace bajo las modalidades descritas, sin embargo aún podemos perfeccionar el CSMA, esto se puede lograr observando que una vez que se ha producido una colisión las estaciones involucradas no tienen por qué seguir transmitiendo.

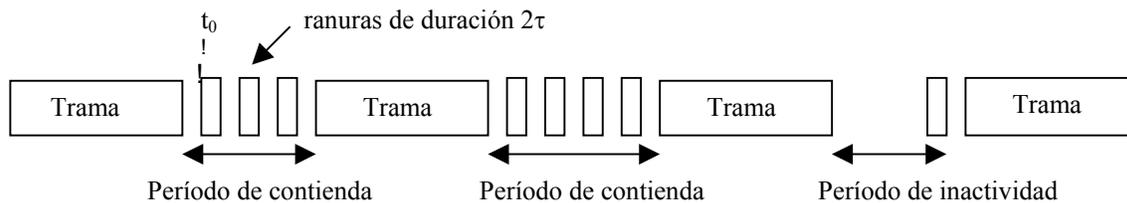
Debido a ello si el protocolo una vez detectada la colisión detiene el proceso (“aborta” la transmisión) se produce un ahorro de tiempo y ancho de banda, este protocolo se conoce como **CSMA/CD** (Carrier Sensing Multiple Access/Colisión Detection), acceso múltiple por detección de portadora con detección de colisión.

Debido a la naturaleza común del canal, podemos saber cuando ocurre una colisión y abortar una transmisión que ya sabemos que colisionó.

CSMA/CD va a consistir de tres períodos importantes:

1. **Período de contienda**(algunos lo llaman **de contención**) : es cuando dos ó más estaciones accesan el canal simultáneamente. Van a detectar que hubo colisión y abortarán la transmisión produciéndose dos ó más tramas incompletas en el canal. Las estaciones esperarán un tiempo aleatorio, escucharán el canal y si este está libre comenzarán a transmitir.
2. **Período de transmisión**: eventualmente alguna estación va a obtener el control del canal. Durante el tiempo que la estación transmite nadie más usa el canal.
3. **Período vacío**: es cuando ninguna estación tiene nada que transmitir. El canal va a estar vacío.

Estos tres períodos están ilustrados en la **Figura 6.5**.



**Figura 6.5. Los tres períodos del CSMA/CD: contienda, transmisión e inactividad(vacío)**

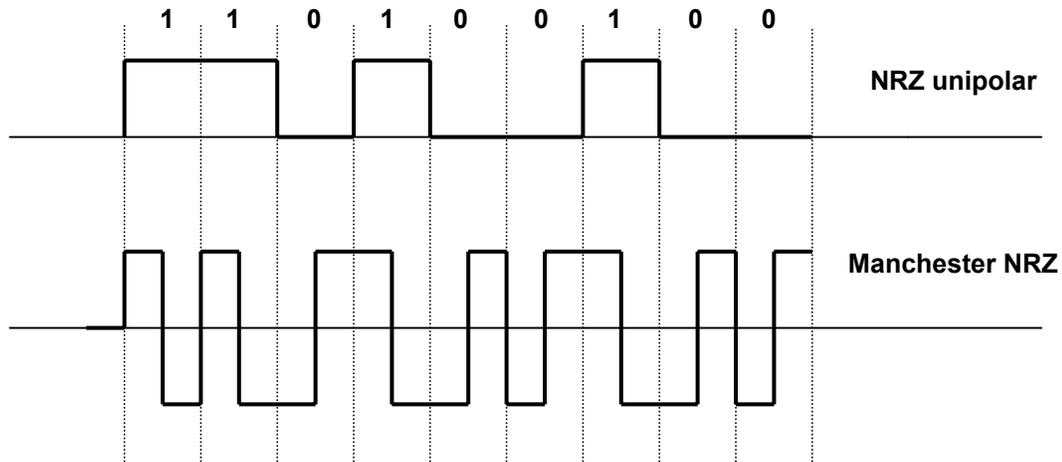
Nos interesa el **período de contienda**(donde se muestran ranuras  $2\tau$ )que es el tiempo que una estación tardará en darse cuenta de que su trama colisionó, para ello: supongamos que la estación A, ubicada en uno de los extremos, para considerar el caso más desfavorable, empieza a transmitir en el instante  $t_0$ , la señal se va propagando y a su paso alertando a las estaciones intermedias que el canal está ocupado. La señal tardará un tiempo  $\tau$  en llegar a la estación más alejada, B ubicada en el otro extremo.

Esta estación B, podrá comenzar a transmitir hasta un instante antes de que la señal de A llegue, si lo hace inmediatamente se da cuenta que hubo una colisión y aborta su transmisión. Pero ese pequeño ruido causado por la colisión **no llega hasta la estación A** hasta un tiempo igual al doble del tiempo de propagación entre A y B o sea  $2\tau$ . Por lo tanto una estación no puede estar segura de que obtuvo el canal sino hasta que ha transmitido durante  $2\tau$  sin tener una colisión. Por esta razón modelamos el período de contienda como un ALOHA ranurado con tamaño de ranura  $2\tau$ , con lo que se calculará el tiempo de retardo y el caudal, para un cable coaxial de 1 km de largo,  $\tau = 5\mu\text{seg}$ . Por simplicidad suponemos que cada ranura  $2\tau$  contiene sólo un bit. Una vez que una estación ha transmitido  $2\tau$  sin detectar una colisión obtiene el canal, y decimos que **se posee de él**, por lo que puede transmitir a cualquier velocidad.

Se verá luego que en la norma 802.3, una de las implementaciones más populares de CSMA/CD, se ha establecido un tiempo de ranura de 512 bits ó  $51.2\mu\text{seg}$  a 10 Mbps, cuando ocurre una primera colisión cada estación espera, en forma aleatoria 0 ó un tiempo de ranura, antes de intentarlo nuevamente. Si dos estaciones sufren una colisión y escogen el mismo número aleatorio volverán a colisionar, luego de esta segunda colisión cada una seleccionará un número entero en el intervalo  $0 - 3$ , y esperará ese número de tiempos de ranura antes de transmitir nuevamente, si ocurre una tercera colisión(cuya probabilidad es 0.25), el número de ranuras que debe esperar para la próxima transmisión se elige en forma aleatoria en el intervalo  $0 - (2^3 - 1)$ , si vuelve a producirse otra colisión el proceso sigue en forma parecida hasta 10 colisiones donde el intervalo se congela a un máximo de 1023 ranuras y luego de 16 colisiones se toman otras medidas.

La detección de colisiones es un proceso **analógico**, el hardware debe poder escuchar lo que hay en el cable a la vez que está transmitiendo, si lo que lee es diferente de lo que está escribiendo hay colisión.

Para poder detectar correctamente esta colisión debemos ser cuidadosos con el tipo de codificación que se emplea, dado que si utilizamos codificación unipolar, como el del caso a) de la **Figura 2.18** cuando colisionan dos ceros no podemos detectar la colisión, por ello es que es común utilizar una codificación llamada Manchester, que tiene dos niveles +V y -V y un 1 viene dado por una transición +V a -V en el centro del período del bit y un 0 por una transición -V a +V, ver **Figura 6.6**.



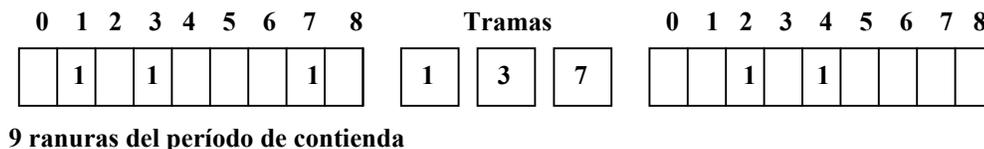
**Figura 6.6 Codificaciones NRZ y Manchester NRZ.**

### 6.5.2.-Protocolos sin colisión.

Con CSMA/CD durante el período de transmisión no pueden haber colisiones, pero sí durante el de contienda, sobre todo si la longitud del cable es grande (y por ende lo es  $\tau$ ) y las tramas son pequeñas, tal es el caso de redes de fibra óptica de gran longitud y ancho de banda, existen una serie de protocolos [1] que resuelven el problema de modo que no haya colisiones ni siquiera en el período de contienda.

No dedicaremos mucho tiempo a estos protocolos pues, como se verá en Secciones posteriores, otros se han ganado la aceptación de la industria y de los usuarios, por ello solo describiremos brevemente uno llamado **método del mapa de bits**.

Supongamos tener N estaciones, en el tiempo se establecen **períodos de contienda** compuestos de N ranuras de un bit cada una y correspondientes a cada estación. Si la estación tiene algo que transmitir coloca un uno en su ranura, si no tiene nada que transmitir coloca un cero.



**Figura 6.7. Método de mapa de bits.**

Esto se puede observar en la **Figura 6.7**. Finalizado el período de contienda todas las estaciones saben quien tiene algo que transmitir y comienza el **período de transmisión** en que las estaciones que se "anotaron" para transmitir lo hacen en el mismo orden de la ranura de contienda, cuando han terminado comienza otro período de contienda y así sucesivamente.

### 6.6.-Redes por satélite.

Los enlaces por satélite poseen una serie de propiedades que los hacen muy diferentes de los de cable(incluyendo los de fibra)y de los de radio terrenales, las más importantes son:

- ▶ Un satélite geoestacionario puede ser accedido desde prácticamente la cuarta parte de la superficie terrestre.
- ▶ Los costos de transmisión son casi independientes de la distancia.
- ▶ Pueden realizarse tanto enlaces punto a punto como de difusión.
- ▶ Es posible disponer de considerable ancho de banda.
- ▶ La calidad del enlace es superior a los terrenales.
- ▶ Existe un retardo de propagación tierra-satélite-tierra de unos 250 ms.
- ▶ La estación emisora puede recibir su propia emisión.

En esta Sección solo daremos algunas ideas generales sobre los sistemas satelitales, el tema es muy extenso y debe recurrirse a literatura especializada[2].

Los satélites operan en las bandas C,K,Ku y Ka,ocupando sectores entre 4 GHz y 44 GHz y utilizan un par de frecuencias de portadora en cada enlace, una frecuencia(la menor) para el **enlace de bajada(downlink)**,satélite-tierra, y otra (la mayor) para el **enlace de subida(uplink)**,tierra-satélite.

Un satélite de comunicaciones típico posee un ancho de banda considerable que se divide en partes(cada parte corresponde a un equipo llamado **transpondedor**, castellanización de **transponder**),asi tenemos satélites con 12 ó 24 transpondedores cada uno de ellos de 36 MHz lo que nos dá cerca de 500 MHz en el primer caso y alrededor del doble en el segundo, a fin de incrementar la capacidad los diseñadores de satélites recurren al “reuso” de frecuencia y/o a diferentes polarizaciones.

Las **estaciones terrenas** se clasifican según la capacidad de servicio que prestan en:

- a) **Estaciones terrenas maestras**, que son utilizadas para servicios de comunicación públicos, especialmente para comunicaciones internacionales. Usan antenas de más de 9 metros de diámetro y amplificadores de más de 400 watios de potencia.
- b) **Estaciones terrenas de mediana capacidad**, son utilizadas por corporaciones y redes privadas, el tamaño de la antena varía según las necesidades típicas de cada aplicación, y en general están entre los 4 y 9 metros.
- c) **Estaciones terrenas de diámetro muy pequeño ó VSAT(Very Small Aperture Terminal)**que se caracterizan por su pequeño diámetro(0.7 a 2.8 m)y por lo general prestan servicios de voz y datos a un solo usuario. Poseen uno ó dos canales de voz comprimida y hasta cuatro canales de datos de baja capacidad.[3].

En los satélites son de gran importancia los **métodos de acceso**, que se refieren a los métodos empleados para utilizar las facilidades de comunicación del satélite con **varias** estaciones terrenas,y casi siempre empleamos los términos **métodos de acceso** para significar **acceso múltiple**,en el sentido que varias estaciones terrenas **comparten** los transponders del satélite y su característica de radiodifusión(broadcast).

Los métodos de acceso son fundamentalmente tres:

- ◆ **FDMA** por **F**requency **D**ivision **M**ultiple **A**ccess, se aplica tanto a los sistemas analógicos como a los digitales.
- ◆ **TDMA** por **T**ime **D**ivision **M**ultiple **A**ccess.
- ◆ **CDMA** por **C**ode **D**ivision **M**ultiple **A**ccess denominado espectro extendido (spread spectrum).

El **FDMA** emplea portadoras multidestino que comparten el punto de origen, o dicho de otro modo en cada estación terrena se transmite una(o varias) portadora preasignada modulada en FM con todo el tráfico que genera esa estación. En el transpondedor del satélite son amplificadas y cambiadas de frecuencia y retransmitidas a la tierra con la modalidad de difusión, de manera que cada estación receptora terrena recoge **todas** las portadoras y **selecciona** en el equipo multiplex el tráfico que le corresponde.

Una variedad importante de **FDMA** es **SCPC(Single Carrier Per Channel)**, del cual a su vez hay dos tipos: canales preasignados y canales asignados por demanda(**DAMA**).

El **SCPC preasignado** es un servicio punto a punto en el que los dos usuarios tienen asignada una portadora y un ancho de banda en forma permanente, se requiere de dos portadoras por cada estación(una para transmitir, TX y otra para recibir, RX),el costo de arrendamiento mensual es fijo.

El **SCPC/DAMA** utiliza más eficientemente el espectro y reduce costos pues solo se paga por el tiempo de ocupación del canal, ya que permite la asignación dinámica de canales entre parejas de estaciones(lo que permite la creación de redes malladas).Para ello existe una estación de control que permite a las estaciones solicitar(aquí hay tres métodos de control: polling, control central aleatorio y control central distribuido, ver [2]) la asignación de un par de frecuencias para comunicarse con cualquier estación de la red, una vez concluida la comunicación se libera el canal para su reuso por cualquier otra pareja de estaciones.

También existe otro sistema llamado **SPADE(Single Channel Per Carrier PCM multiple Demand Assignment Equipment)**que no ha tenido mucha aceptación por su complicación.

Uno de los problemas de FDMA es la intermodulación entre portadoras en el transponder, este problema desaparece con **TDMA**, ya que sólo se permite que **una** portadora pase por el transponder en cualquier instante, de manera tal que el transponder es dedicado exclusivamente a cada estación terrena durante un pequeño intervalo. La **Figura 6.8** muestra como funciona el sistema: un periodo de trama(establecido por la estación de referencia)es dividido entre las diversas estaciones terrenas, así durante su intervalo esa estación envía sus datos y estos son procesados por el transponder, que envía a la tierra de regreso una señal compuesta con todas las contribuciones de las estaciones, la estación receptora seleccionará el tráfico a ella destinada.

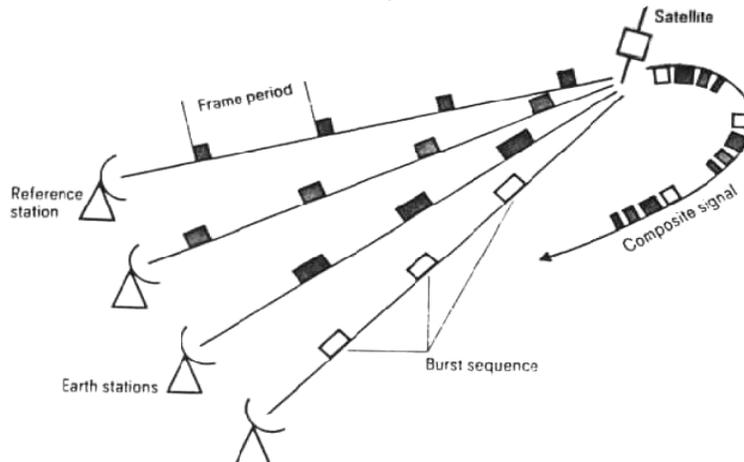


Figura 6.8 Principio del TDMA

Con **CDMA** todas las estaciones transmiten dentro de la misma banda de frecuencia sin limitaciones en cuanto a la frecuencia de portadora ó de cuando pueden transmitir(transmite cuando lo desea)ó de que ancho de banda puede utilizar, por esta última característica CDMA se identifica como **acceso múltiple de espectro disperso(ó Spread Spectrum)**.Las transmisiones son separadas por técnicas de **encriptación/desencriptación de cubiertas**, lo que significa que cada estación codifica su transmisión con una palabra única binaria denominada **código de chip** conocido también por la estación receptora, el receptor recibe del satélite **varias** señales PSK codificadas y el **correlacionador** debe separa solo el código destinado al receptor respectivo, una desventaja es que el la velocidad del código de chip es varias veces la velocidad original y con ello el ancho de banda y otra es la necesidad de sincronización de tiempos[12], y aunque pudiera verse como una desperdicio del ancho de banda el sistema de recuperación es tan eficiente que puede decodificar señales muy débiles, permitiendo entonces el uso simultáneo del mismo espectro por varias estaciones. En realidad esta es una de las dos modalidades de **Spread Spectrum** que se denominada **DSSS(Direct Sequence Spread Spectrum)**, la otra es **FHSS(Frequency Hopping Spread Spectrum)** en ella el transmisor está constantemente cambiando la frecuencia de portadora, dentro de la banda permitida, de acuerdo a un código específico, el receptor debe conocer este código para poder seguir la frecuencia de la portadora. En realidad ambas modalidades intercambian potencia de transmisión por ancho de banda, permitiendo que varias estaciones compartan una cierta parte del espectro.

Mencionamos anteriormente los sistemas **VSAT[3]** estos sistemas se componen de antenas y equipos de pequeño tamaño y bajo costo, que frecuentemente (no siempre) operan en conjunción con una **estación central ó maestra** llamada **Hub** y proveen de servicios de información y datos, son el resultado de desarrollos tecnológicos en el área de antenas y microondas, en el de protocolos de conmutación de paquetes, protocolos de acceso múltiple, etc.

Existen tres modalidades de VSAT:

- a) **Difusión(punto a multipunto)**: donde una estación central ó hub transmite a todas las estaciones pequeñas VSAT video, música de alta calidad ó datos.
- b) **Punto a punto**, donde voz, datos ó imágenes (VDI)(o cualquier combinación de ellos)se transmiten uni o bidireccionalmente entre dos estaciones remotas sin la intervención de un hub.
- c) **Sistemas interactivos bidireccionales**, provee de VDI interactivos bidireccionales a un gran número de VSAT inteligentes que se comunican entre ellos mediante un hub.

En VSAT se utilizan topologías tipo estrella y tipo malla, las **Figuras 6.9 y 6.10** muestran estas topologías.

En la tipo **estrella** se utiliza **TDMA**, mientras que en la tipo **malla** se usa **SCPC**.

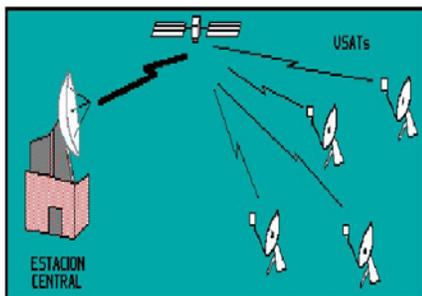


Figura 6.9. Red VSAT tipo estrella

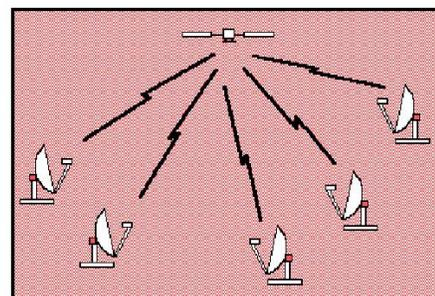


Figura 6.10.Red VSAT tipo malla

Dado que un mensaje tarda cerca de 250 ms en hacer el recorrido tierra-satélite-tierra las técnicas de acceso tipo polling(pregunta y respuesta)deben descartarse inmediatamente, algo similar puede decirse de CSMA, por ello en estas redes se utiliza ampliamente ALOHA ranurado, sobre todo en las redes de control industrial

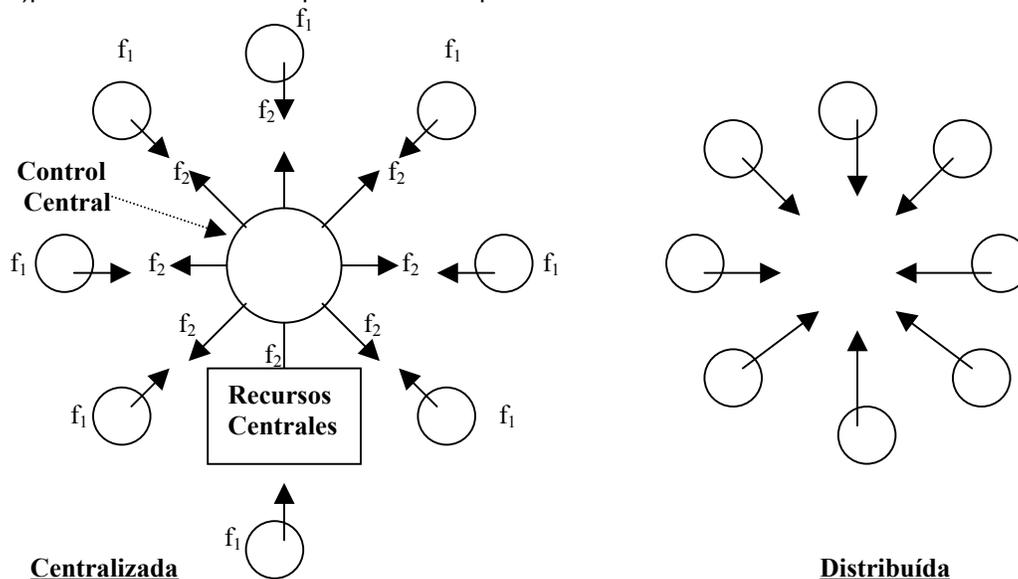
### 6.7.-Redes inalámbricas(WirelessNetworks).

Esta arquitectura de redes une las ventajas de transmisión ofrecidas por las redes de conmutación con las debidas a la ausencia de instalación de líneas físicas de conexión entre los equipos. Las **redes inalámbricas** comenzaron por **packet radio**[4] tecnología impulsada por radioaficionados e introducida en diversas universidades norteamericanas y en los países en desarrollo por su bajo costo y gran flexibilidad, luego fueron seguidas por las llamadas **WLANS (Wireless LAN)** de las que actualmente hay tres tipos fundamentales: **wireless Lans** estándar 802.11 que utiliza las tecnologías **Spread Spectrum :DSSS(Direct Sequence Spread Spectrum)** y la otra es **FHSS(Frequency Hopping Spread Spectrum)**, **wireless PAN(Personal Area Network)** estándar 802.15 y **wireless MAN** estándar 802.16, aunque volveremos sobre esto en el Capítulo 8 es oportuno mencionar que las **redes inalámbricas** constituyen el tópico de redes de mayor atención en la actualidad .

Existen dos configuraciones básicas: centralizada y distribuida, ambas se muestran en la **Figura 6.11**.

- ♦ **Configuración centralizada**, requiere de disponer de dos canales de radio para la transmisión y de un nodo central para transferir la información de un canal a otro. Los nodos individuales envían paquetes al nodo central a través de uno de los canales, y el nodo central radia dichos paquetes por el otro canal. Los paquetes radiados por el nodo central son recibidos por todos los nodos individuales, siendo por lo tanto esta configuración un sistema multipunto con una estación primaria y varias secundarias.
- ♦ **Configuración distribuida**, solamente requiere de un único canal de radio. Este canal es utilizado para las transmisiones y es recibido por todos los nodos, equivale por tanto a una red de área local.

Dado que este tipo de redes está basado en **compartir** el medio de transmisión (canales de radio)por todos los nodos, es necesario establecer un procedimiento (denominado protocolo de acceso)para arbitrar cual es el próximo nodo que transmitirá.



**Figura 6.11** Arquitectura centralizada y distribuida en una red de paquetes por radio.

Los tres protocolos de acceso más utilizados en este tipo de redes son:ALOHA,ALOHA ranurado, CSMA(Carrier Sensing Multiple Access) y CSMA/CA donde el **CA** significa **Colission Avoidance** que es un mecanismo para **evitar** colisiones que implica informar a los demás usuarios que cantidad de bits se van a transmitir de modo que ellos esperen el final de la transmisión antes de comenzar otra.

## 6.8.- Implementación de las Redes de Área Local(LANs).

### 6.8.1.-Conceptos.

Los primeros computadores no fueron diseñados para propósitos de comunicación. Con el fin de compartir recursos y disminuir costos se crearon las **redes de área local**, estas para cumplir con su función necesitan de flujo de datos entre computadores. Entonces podemos definir:

- **RED**: es una colección de computadores autónomos interconectados.
- **LAN**: Red de Area Local, conjunto de equipos conectados entre sí con capacidad de procesamiento local en cada uno de ellos, logrando **compartir** los recursos en áreas limitadas geográficamente.

En la **Sección 6.2** se dieron las características principales de las LANs, solo agreguemos ahora que su instalación es fácil y flexible como se verá dentro de poco, veamos ahora como se implementan en la práctica las Redes Locales.

### 6.8.2.-Clasificación de las LAN.

Las redes de área local(LANs) pueden ser clasificadas desde distintos puntos de vista, existen cuatro maneras típicas de ordenarlas:

- en base a su **topología**.
- en base al tipo de **protocolo de acceso al medio**.
- en base a la **velocidad de transmisión**.
- en base al **tipo de transmisión**(banda base o broadband).

Veamos:

#### 6.8.3.1.-Topología.

Cuando hablamos de **topología de una red** nos referimos al modo en que están interconectadas las computadoras y básicamente pueden darse tres puntos de vista:

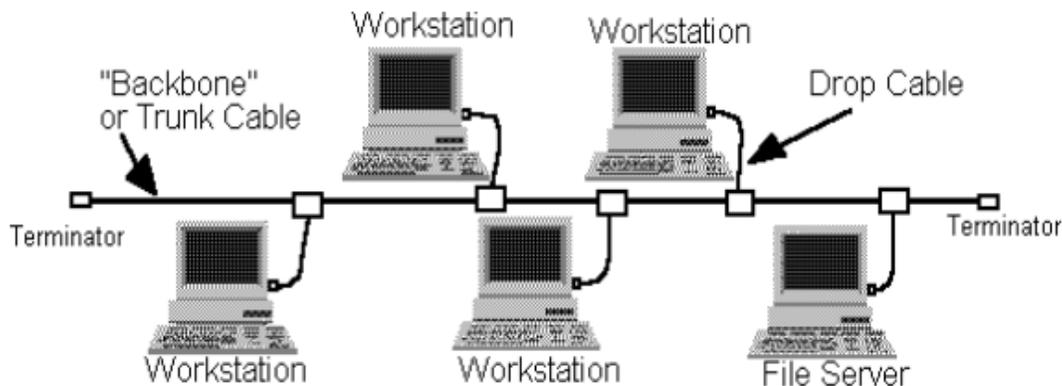
- **topología física**, es la que se observa en el cableado.
- **topología eléctrica**, es la que tiene que ver con el recorrido de la señal eléctrica.
- **topología lógica**, describe como el usuario ve la red.

Generalmente solo nos referimos a las topologías física y lógica, en lo que hace a la **topología física** básicamente podemos hablar de 3 topologías:

- bus ó lineal**,
- estrella**.
- anillo**.

□ **Topología bus ó lineal.**

Consta de un único cable al que están conectadas las computadoras en paralelo en distintos puntos, al final de cada cable hay una resistencia ó terminación, la señal se propaga a lo largo del cable siendo recibida por todas las estaciones, cada una verifica si es la destinataria del paquete procediendo en consecuencia a procesarlo ó a descartarlo, y la señal es finalmente absorbida por las terminaciones, tal como muestra la **Figura 6.12.**



**Figura 6.12. Topología tipo bus ó lineal**

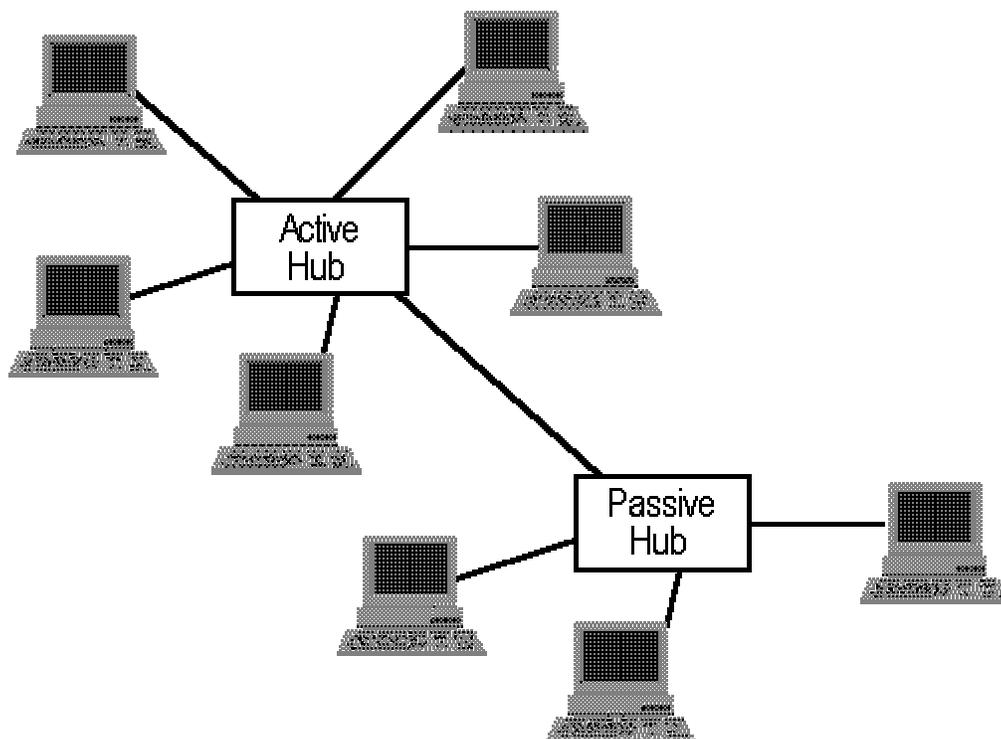
Esta topología configura una red **pasiva** en el sentido que las computadoras ó estaciones de trabajo solo escuchan los datos que han sido puestos en la red y no son responsables de mover los datos de una máquina a otra, si una de estas falla no produce inconvenientes al resto de la red, sin embargo si la conexión a una máquina se daña ó el cable principal se interrumpe todo el tramo entre las dos terminaciones sale de servicio.

Enumeremos las ventajas y desventajas de esta topología:

Ventajas	Desventajas
La falla de una estación de trabajo no afecta a toda la red	La rotura del cable afecta a gran número de usuarios
Sencilla de conectar, flexible	La longitud del cable y el número de estaciones está limitado
Cable y conectores baratos	No es fácil encontrar fallas de cableado
	La degradación de comportamiento es brusca cuando aumenta el número de usuarios

□ **Topología estrella**

En esta topología cada estación de trabajo está conectada a una unidad central que generalmente se denomina **hub ó concentradores**, estos dispositivos inicialmente eran solo medios de interconexión entre todas las estaciones, dando lugar a una **topología lógica** tipo bus ó lineal, sin embargo han ido evolucionando, los hay pasivos y activos y pueden conectarse entre sí para extender la red, dentro de poco nos referiremos a ello extensamente.



**Figura 6.13. Topología estrella**

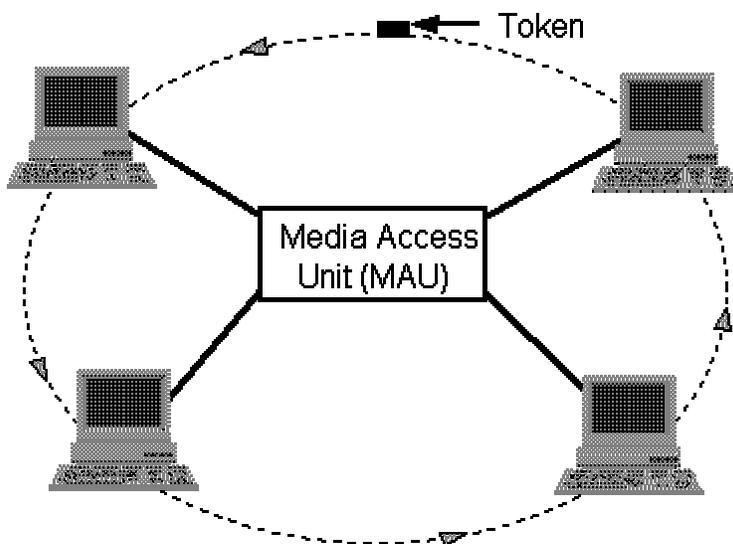
Enumeremos las ventajas y desventajas de esta topología:

Ventajas	Desventajas
Es fácil agregar estaciones de trabajo	Una falla en el hub afecta a todas las estaciones conectadas a él.
Tenemos un punto central de monitoreo y administración de la red	

□ **Topología en anillo.**

En esta topología el cable se conecta circularmente, a veces se dice en forma de bucle cerrado. Las señales viajan en un anillo, esto significa que cada estación recibe el mensaje, lo regenera(luego seremos más precisos) y lo envía a la estación siguiente. Esto indica que los mensajes viajan en un solo sentido.

Las topologías en anillo físicas son raras, generalmente se configuran **físicamente** como estrella a un hub denominado MSAU(Multi Station Access Unit) y **lógicamente** como anillo, esto tiene la ventaja de que una interrupción en un cable afecta solo al usuario(s) respectivo pues el anillo lógico "puentea" esa máquina. Las estaciones utilizan un **token** para transmitir y deben esperar por un **token libre** para poder hacerlo, cuando lo obtienen colocan sus datos y este, que ahora es **token mensaje ó lleno**, irradia a lo largo del anillo. La **Figura 6.14** ilustra esta topología.



**Figura 6.14. Topología anillo lógico**

Veamos las ventajas y desventajas:

Ventajas	Desventajas
Las fallas en el cable afectan a un número reducido de usuarios.	Cableado y conexiones costosas
Acceso igualitario de todas las estaciones	
Degradación suave en el desempeño a medida que la red crece	

### 6.8.3.2.-Usos típicos de las distintas topologías.

Cada topología, como ya se describió, tiene sus ventajas y desventajas, cuando se desea examinar cual topología usar ó la significación de ellas deben considerarse las siguientes propiedades:

**Impacto de la rotura de un cable en la red.** La rotura de un cable en un red mal diseñada causa serios problemas. En el caso de la red tipo bus ó lineal la red sale inmediatamente de servicio hasta que se encuentre y repare la rotura. La topología estrella por el contrario ofrece mayor protección contra roturas y facilita la ubicación de las mismas

**Impacto del agregado o retirada de nodos.** El agregado o retiro de nodos depende de su ubicación, si se trata del extremo de una red lineal es muy fácil, pero si se agregan y quitan nodos constantemente lo mejor es una red estrella.

**Flujo de mensajes y que nodos los ven.** En una red lineal(o en una estrella física pero lineal lógica) todos los mensajes van a todos los nodos, si se necesita más privacidad una red en anillo es una mejora y una red switchada (topología estrella con switches que se verá luego) es la solución.

**Habilidad de usar los nodos como repetidores.** Normalmente un hub es un repetidor y pueden extenderse poniendo hubs en cascada. Con cualquier topología las redes pueden extenderse con puentes, enrutadores, switches, etc.

**Máxima dimensión física de la red.** En redes medianas ó grandes no se utilizan redes lineales porque la administración se hace casi imposible.

**Cantidad de cable utilizado.** Se trata de una solución de compromiso pues las redes lineales usan más cable, en la mayoría de los casos, pero no requieren del hub.

**Cada caso debe analizarse en función de necesidades, costo, velocidad y confiabilidad, sin embargo la topología estrella por las razones expuestas es la preferida.**

### 6.8.4.- Acceso al medio.

Se dijo anteriormente que la clasificación de las redes LAN podía hacerse en base al método de acceso al medio, recordemos que los protocolos ó métodos de acceso al medio establecen:

- \* La forma en que una estación se conecta o desconecta de la red.
- \* Cual es la próxima estación a transmitir.
- \* Los formatos para la transmisión de datos y control de errores.
- \* Lo que debe hacerse cuando falla una estación.

#### Metodos de acceso al medio

Los métodos aplicables en el control de acceso a las redes locales son múltiples y variados, no obstante los organismos de normalización(ISO, IEEE) se han inclinado por la adopción de un número reducido de estos entre los cuales figuran:

- \* Método de contienda(CSMA/CD)
- \* Método por paso de testigo(token passing)

**Método de contienda(CSMA/CD)**, es el descrito en la **Sección 6.5.2**, que sería oportuno que el lector revise ahora para comparar con la de token-passing.

### **Métodos sin contienda ó métodos de selección.**

Esta técnica de acceso consiste en que el usuario debe esperar hasta ser “seleccionado” para poder depositar los mensajes en la red. Debido a ello las redes que la usan son determinísticas y se garantiza que no habrá colisión.

Existen diversas maneras de efectuar esa “selección”.

Una de ellas es el **método de acceso por sondeo**(polling), que consiste en que la estación de control efectúa las dos siguientes funciones sondeando(accesando) la población de usuarios uno tras otro:

- a.-pregunta al usuario si tiene algo que transmitir.
- b.-si la respuesta es sí, da el control del canal de transmisión a ese usuario bajo ciertas condiciones y este transmite los mensajes acumulados en un buffer(ó memoria temporal), si la respuesta es no, pasa al siguiente usuario.

Otra es el llamado, quizás impropio pues el anterior también lo es, **método por paso de testigo(token passing)**, en él existe una **trama clave** ó **testigo** que permite al dispositivo que lo posee hacer uso del canal. Este conjunto de bits perfectamente definido llamado **testigo(token)**, es en realidad una señal de control, y hay dos tipos de testigos:

- \* **testigo libre**(free token), indica a la computadora a que llega que si lo desea puede transmitir.
- \* **testigo mensaje**, le indica a la computadora que sigue un mensaje.

El usuario recibe el testigo y hay solo dos posibilidades: que sea testigo libre ó testigo mensaje:

- Si es libre y desea enviar un mensaje lo cambia a testigo mensaje, agrega el mensaje y envía todo al usuario siguiente.
- Si es libre y no desea enviar mensaje, simplemente lo reenvía al usuario siguiente.
- Si es mensaje lee la dirección del destinatario,
  - ❖ de no ser la propia, lo reenvía al usuario siguiente.
  - ❖ de ser es la propia ,copia el mensaje le agrega un “conforme”(ACK),y lo envía al usuario siguiente.
  - ❖ cuando el usuario originario del mensaje recibe el mensaje modificado lo reconoce, o borra y reemplaza el testigo mensaje por un testigo libre.

Obsérvese que el testigo no es devuelto a una unidad central sino que es trasladado de un usuario a otro en un orden predeterminado, por lo que el método puede ser considerado como de sondeo distribuido.

Cuando se dijo que un usuario envía el mensaje al siguiente no quedo claro como es que se hace, en realidad hay dos maneras de hacerlo llamadas: **paso de testigo en bus** y **paso de testigo en anillo**.

Como su nombre lo indican la primera es físicamente un cable lineal ó en árbol mientras que la segunda es física ó lógicamente un anillo, más adelante al considerar las normas para LANs se dan más detalles.

### 6.8.5.-Velocidad de transmisión.

También pueden clasificarse las LANs en función de la velocidad de transmisión de datos en ellas, así tenemos:

- 1 Mbps: Usan cables telefónicos(Starlan de AT & T).
- 2.5 Mbps: Usan cables telefónicos ó cables coaxiales finos(Arcnet de Data Point)
- 4 Mbps : Cables coaxiales finos y cables telefónicos(Token Ring).
- 10 Mbps, aquí hay varias implementaciones:
  - Cables coaxiales gruesos en el troncal(backbone) y finos para conectarse a este ó para redes pequeñas(Ethernet)(10 Base 2 y 10 Base 5).
  - Par trenzado(UTP 3,4 ó 5) (10 Base T).
- 16 Mbps: Cables coaxiales ó par trenzado(Token Ring).
- 100 Mbps: UTP5 y Fibra Óptica(FDDI).
- Gbps: Gigabit Ethernet con :Fibra Óptica y UTP 5.
- 10 Gbps: Ethernet de 10 Gbps con Fibra Óptica

### 6.8.6.-Tipo de transmisión.

- **Banda Base:** señal digital directa(son todos las implementaciones vistas con excepción de las vía ondas electromagnéticas no guiadas y fibra óptica).
- **Banda Ancha:** utilizan por ejemplo cable coaxial de CATV(75 ohms) ó fibra óptica, con topología bus(lineal) ó bus/tree(lineal/árbol),con una longitud máxima de 1800m,vía modem utilizando modulación DPSK

### 6.9.- Componentes de una Red de Área Local.

Los componentes de una LAN, al igual que en otros sistemas de computadoras, pueden ser divididos en dos categorías básicas: **software y hardware**.

Los componentes del **software** entregan a todas las estaciones de trabajo la habilidad de utilizar las conexiones suministradas por el hardware, deben permitir la identificación del usuario y su acceso a recursos remotos tales como directorios, programas, impresoras, etc.

Los componentes del **software** incluyen:

- Sistema operativo de la red(NOS).
- Programas de aplicación
- Sistemas operativos de las estaciones de trabajo.

Los componentes de **hardware** incluyen:

- Hubs.
- Tarjetas de interfaz(NIC).
- Servidor/es.
- Periféricos de LAN.
- Estaciones de trabajo.
- Medio físico de transmisión.

Comencemos por los primeros:

□ **Componentes de software..**

**Sistema operativo de la red(NOS):** las redes locales(LAN's) generalmente funcionan bajo dos esquemas: **peer to peer** (igual a igual) y **cliente-servidor**.

**Modelo peer to peer.**

Una red **peer to peer** como Windows para trabajo en grupo, Windows 95,98,Me,2000 ó XP, Network OS, TOPS(Sun Microsystem) ó DLINK, permiten que cada usuario pueda compartir recursos con las demás, así por ejemplo un usuario puede estar imprimiendo un documento en nuestra impresora y aún así nosotros estamos actualizando una base de datos ó intercambiando datos con un tercer usuario.

Esta característica es muy atractiva, pero cuando aumenta el número de usuarios su implementación se complica ya que es difícil mantener orden en el uso de los archivos y se incurre en la redundancia de la información, para evitarlo se distribuyen los sistemas entre las estaciones, pero decae sensiblemente el rendimiento por nodo, además el usuario exigente no está dispuesto a sacrificar ciclos de su máquina para atender los requerimientos de otro usuario.

Por otra parte los usuarios que disponen de sistemas de uso común no pueden abandonar la red ya que de hacerlo dejarían a los demás sin ese servicio ó peor aún al abandonar pudieran interrumpir a algún otro usuario trabajando con su sistema. Otro detalle es la seguridad ya que cualquier usuario, **si no se toman medidas adecuadas**, podría acceder archivos de cualquier estación o crear directorios en estaciones de trabajo remotas.

Por las razones precedentes la mayoría de las organizaciones rechazan este esquema.

**Modelo cliente-servidor.**

Bajo este modelo hay dos tipos de máquinas(individuos)en la red:

- el ó los **servidores**: que proveen uno ó varios servicios a otras máquinas.
- las estaciones de trabajo, son los "**clientes**" que hacen uso del servicio.

Los servicios más comunes son: impresión, bases de datos y comunicaciones.

Los problemas mencionados en el esquema anterior quedan resueltos permitiendo que puedan concentrarse más usuarios en la red, esto puede conducir a "cuellos de botella" que deben ser solucionados estudiando la topología y el manejo de colas de impresión, acceso a información, comunicaciones, etc.

Bajo este esquema el sistema operativo conocido como **NOS**, Network Operating System, permite que las computadoras hablen entre sí e incluye dos partes: la del servidor y el shell.

El software del servidor corre en un computador llamado de igual modo, servidor, y permite compartir recursos tales como almacenamiento en disco impresión, comunicaciones, etc, actúa como un semáforo inteligente (ó policía de tránsito) determinando que usuario acceda que recursos y en que momento.

El software shell corre en las demás computadoras de la red, o nodos, permitiendo la comunicación con el servidor y con otros computadores en un sistema igual a igual(peer to peer)

### Sistemas Operativos usuales

Existen en el mercado diversos sistemas operativos de redes LAN, nos referiremos solamente a los más difundidos sin pretender agotar el tema.

Dos estilos han sido tomados por los creadores de sistemas operativos de redes(NOS): **usar un sistema operativo existente ó crear un ambiente operativo propietario.**

Al primer grupo pertenecen: el VINES de BANYAN, que utiliza Unix System V como plataforma; los equipos de SUN Microsystem, que son prácticamente un estándar en este segmento del mercado y también utilizan Unix y el LAN MANAGER que utiliza OS-2 como plataforma.

Unix es un sistema operativo propietario que ofrece a la comunidad científica, educativa y comercial una herramienta muy poderosa para procesar datos bajo los esquemas multiusuarios y multitareas, la versión pública se conoce como LINUX y está compitiendo con Windows.

Bajo el esquema de atención a estaciones no inteligentes a través de puertos sincrónicos(vía interfaces seriales RS-232), Unix paga un alto precio en rendimiento debido a dos factores primordiales, primero la velocidad máxima de transmisión de estos interfaces solo llega a 19.600 baudios, y segundo que debe proveer memoria a cada tarea generada por el usuario. Esto último hace que sea raro encontrar una implementación de sistema operativo Unix con menos de 16 Mega Bytes en RAM y que se requieran unidades de almacenamiento de datos de muy rápido acceso, todo lo que encarece notablemente estas instalaciones.

Sin embargo Unix(y Linux) ofrece una alternativa para descentralizar esta modalidad de operación, utilizando los beneficios de la topología bus y las ventajas tecnológicas de las interfaces Ethernet (802.3), a tal fin utiliza el protocolo de transmisión y transferencia de paquetes conocido como TCP/IP (ver Capítulo7), que se ha convertido en un estándar "de facto", no solo en LAN sino también en interconexión de redes.

Adicionalmente podemos mencionar que parte fundamental del NOS de Vines es un servicio de nombre y directorio llamado StreetTalk que permite a los usuarios ver los recursos de la red como extensiones virtuales de sus estaciones locales, otro servicio de gran importancia en este NOS es el de comunicaciones que permite: emulación de terminales asincrónicos, comunicaciones con mainframes IBM(SNA,BISYNCH), soporte de :TCP/IP, aplicaciones OSI, X.25/X.29 y a puentes (bridges) token ring.

El LAN MANAGER como se dijo utiliza OS/2 como plataforma y el HPFS(High Performance File System) de Microsoft en su sistema de archivo.

El segundo grupo, que crea un **ambiente operativo propietario**, lo integra principalmente NETWARE de Novell, que es el NOS más instalado en todos los medios.

Novell ha diseñado un sistema propietario que no se ha alejado mucho de los esquemas de trabajo impuestos por el Sistema Operativo DOS. El **servidor** ó servidores de la red son normalmente **dedicados** a la tarea del despacho de servicios, en algunas versiones que manejan pocos usuarios trabajan en modo no dedicado.

Un servidor NETWARE, puede concentrar los servicios de Archivos, Bases de Datos, Impresión ó Comunicaciones en una sola unidad pero estos servicios pueden distribuirse a otros servidores que pueden actuar independientemente y ofrecerlos por separado, disminuyendo el congestionamiento.

Las estaciones de trabajo funcionan con DOS por lo que pueden ser cualquier equipo compatible IBM con bus ISA, EISA, Microcanal ó PCI, y puede ser usado en cualquier topología: Token Ring, Ethernet, ó Arcnet.

Hay tres tipos básicos de redes: el nivel Entry(ELS) Netware 286 Avanzado(con ó sin SFT, System Fault Tolerance) y Netware 386.

El primero es para redes muy pequeñas, el segundo que corre en microprocesadores basados 80286 y 80386,es para redes medianas, y el Netware 386,es la versión más robusta y contiene grandes ventajas, se usa en redes grandes.

La red Novell ha pasado por diversas versiones desde las primeras 2.1 para 4 usuarios, hasta las actuales: 2.2,2.11 y 2.15 con servidores dedicados y no dedicados; 3.11 con servidor dedicado y hasta 100 estaciones,3.12 con servidor dedicado y recomendada como actualización de la 3.11,y la 4.0 con servidor dedicado, usada en redes grandes, con trabajo de multiservidor.

Recuérdese que NOS incluye dos partes una la que corre en el servidor, que actúa como un semáforo"inteligente", determinando que estación de trabajo accesa que recursos y en que momento; y la otra, el "shell",que corre en cada estación de trabajo, esta parte del NOS intercepta todos los pedidos de impresión, manejo de disco, etc y determina si serán ejecutados localmente ó enviados a un equipo de la LAN.

El software operativo del servidor incluye funciones para establecer comunicación con el hardware de la red, con otros PC y otros servidores.

El software de las estaciones de trabajo, además del DOS ó OS/2,contiene, tal como se dijo, el Shell Netware, que comprende dos partes:

- El IPX.COM, que se comunica directamente con la tarjeta de interfase NIC en el PC e implementa los protocolos de bajo nivel que permiten la comunicación básica entre las diferentes estaciones y dispositivos de la red.
- El NET?.COM(NET2,NET3 para DOS 3.X, NET4 para DOS 4.X, NET5 para DOS 5.X y 6.X, ó NETX que sirve para cualquier versión de DOS, pero consume mucha memoria)y es quien al recibir una requisición de servicio determina si será satisfecha localmente ó por la red, en el primer caso pasa la solicitud al DOS, en el segundo lo pasa al IPX.COM quien a su vez requiere a la NIC la organización del transporte, este organiza los paquetes de datos y los envía al sistema de cable.

En realidad el IPX.COM es un emulador(para no depender del diseño original) del protocolo de sesión NETBIOS (que es un programa de interfase de aplicaciones(API) creado para IBM),y que recibe solicitudes para la red y las maneja.

**Los programas de aplicación**, son programas como los típicos de una PC: Word, Lotus, Excel, etc, disponibles en versión para redes, que incluyen características como tipos de acceso a archivos y datos, necesarios por seguridad en ambientes multiusuarios.

**Los sistemas operativos de las estaciones de trabajo**, son simplemente eso: DOS, Windows en sus diversas versiones, LINUX y muchos otros.

□ **Componentes de hardware**

**Hubs[5] ó concentradores**, inicialmente con Thin Ethernet se usaron repetidores de dos puertos, para regenerar la señal, al aparecer 10Base-T el esquema varió para acomodarse al nuevo estándar, para ello el repetidor se uso multipuerto y fueron llamados **concentradores**. Existen muchos tipos de concentradores, tantos que el tema pudiera ocupar un libro completo, en su forma más simple un concentrador es un dispositivo que centraliza la conexión de los cables provenientes de las estaciones de trabajo bajo una topología tipo estrella. Existen concentradores pasivos y activos.

- **Concentradores pasivos.** Son dispositivos que toman la señal que entra por un puerto y la distribuyen a todos los demás, en realidad se trata de paneles de distribución que no amplifican, ni regeneran la señal, utilizados en ARCNET pasiva y en 10 Base F.
- **Concentradores activos.** Disponen normalmente de más puertos que los concentradores pasivos y regeneran las señales que viajen entre los dispositivos conectados, obviamente requieren de conexión eléctrica y se utilizan como repetidores que proporcionan una extensión del cable conectado a una estación de trabajo, son utilizados ampliamente en ARCNET activa y en 10 Base T.

En la **Sección 2.10.4** ya se mencionó que los concentradores típicamente se conectan a otros concentradores (o se “apilan”) formando una jerarquía, tal como muestra la **Figura 6.15**.

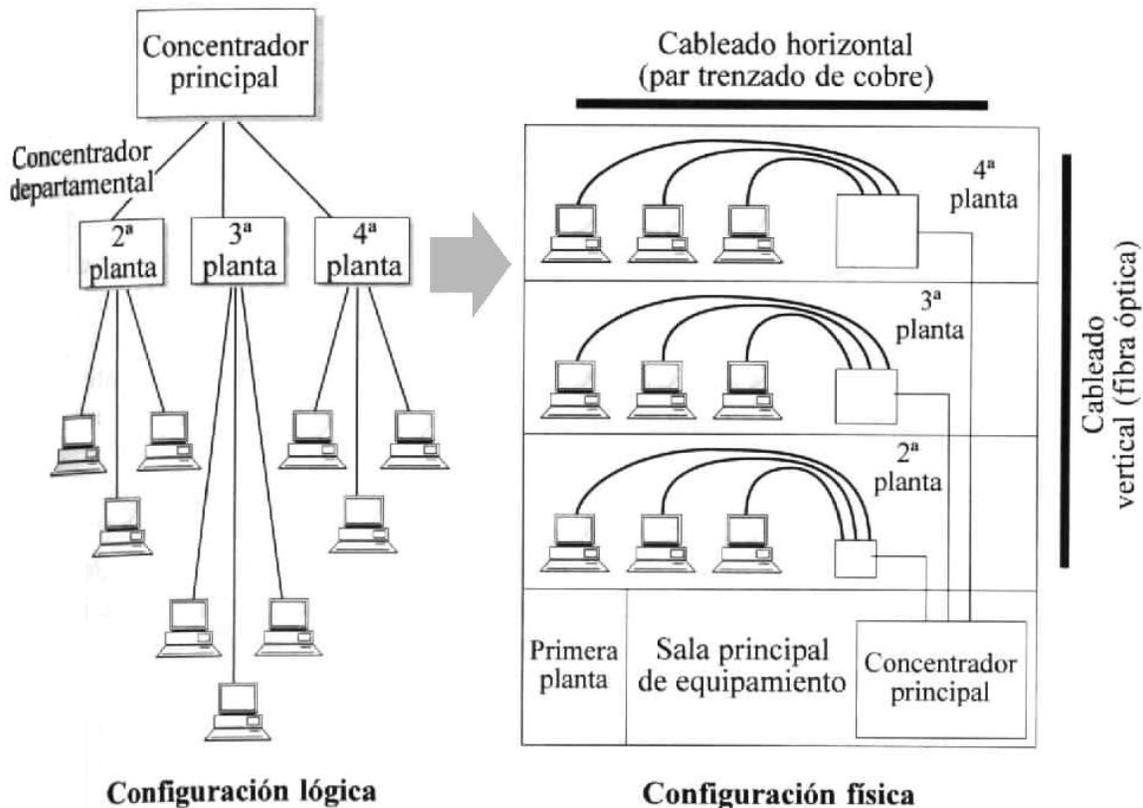


Figura 6.15. Cableado estructurado

Allí en la parte izquierda está la configuración lógica y en la derecha la física, está última corresponde a un **Sistema de Cableado Estructurado** tal como se discute en la sección “**Normativa de cableado para edificios comerciales EIA/TIA\* 568**”, que es la referencia obligada cuando se desea cablear un edificio ya que el cableado estructurado es sencillo de instalar, gestionar y expandir, en él se habla del cableado horizontal en cada piso con par trenzado, tal como se ve en las **Figura 2.30** y **6.15**, y luego la conexión vertical (con fibra óptica) entre los concentradores de cada piso ubicados en el armario de telecomunicaciones y el concentrador principal, que está en la planta bajo ó en el sótano. Los concentradores hacen posible el cableado estructurado (y los anillos lógicos, como ya se explicó), y proporcionan varios beneficios:

- Los cambios en la red necesarios por modificaciones en la organización de la empresa son fáciles de realizar cuando el cableado estructurado se ha hecho en torno a concentradores.
- Las redes pueden crecer armónicamente mediante cableado estructurado y concentradores.
- Los concentradores se acomodan a diversas opciones de red: Ethernet, Token Ring, FDDI, y a las de redes WAN: Frame Relay, SMDS, ATM y otras.
- Los concentradores permiten una gestión centralizada y recolección automática de información sobre la red.
- Los concentradores proporcionan utilidades tolerantes a fallas, que mantienen el cableado funcionando.

Los concentradores han ido evolucionando en tres generaciones, en una primera eran **repetidores simples** de ocho ó más puertos usando UTP y adecuados a LAN pequeñas, en la segunda se denominaron **concentradores inteligentes (smart hubs)** pues incorporaban utilidades de gestión de redes como SNMP (Simple Network Management Protocol), además contaban con “back planes” (plano posterior), esta es una placa que tiene varios “buses”, que pueden dar soporte a diversos medios (ethernet, token ring, FDDI, etc), cada bus es análogo a los buses ISA ó EISA y allí se conectan módulos que son repetidores multipunto en forma de tarjetas enchufables, los buses a su vez se conectados entre sí a muy alta velocidad (a veces Gbps) por la electrónica del plano posterior, la tercera generación son **concentradores corporativos** que soportan todas las necesidades de cableado de una organización, tienen utilidades inteligentes para segmentar las LANs, planos posteriores de muy alta velocidad, son altamente modulares incluyendo conexiones para WAN y utilidades de gestión avanzada, para más detalle ver [5] páginas 189 a 208.

La nomenclatura actual llama **hubs ó concentradores** a los repetidores multipuerto, **concentradores apilables (stackable hubs)** a los repetidores multipuerto apilables y **armario de telecomunicaciones** al “distribution rack” de la **Figura 2.30**, y todos ellos forman parte de una serie de equipos que se denominan **Componentes de Grupo de Trabajo (Workgroup Components)**, a esa serie solo falta agregar uno, que es de gran importancia pues se utiliza cada día más, se trata de los **switches (switching hubs)**.

**Switches**, no hay unanimidad en el uso de la palabra switch pero su uso más común es el que le dió la empresa Kalpana, un **switch** es un componente de la red que recibe los paquetes de un puerto, los **almacena temporalmente** y los **envía a otro puerto**.

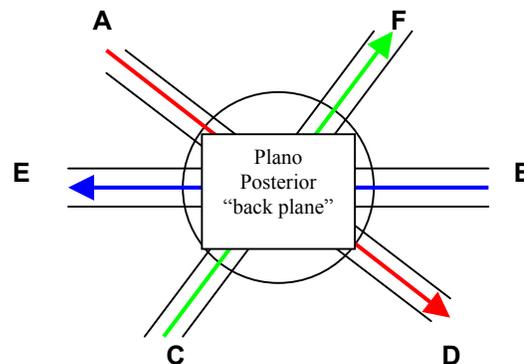
---

\* EIA corresponde a Electronic Industries Association y TIA a Telecommunications Industry Association y son dos organizaciones de estándares de la industria norteamericana ver **Sección 2.2.1**.

Por lo tanto el switch **reemplaza el medio compartido** por **un enlace dedicado**, uno por usuario, **no hay por lo tanto colisiones**, en consecuencia no es necesario detectar portadora ni colisiones como en CSMA/CD, sin embargo puede haber **contienda** cuando dos ó más puertos de entrada desean enviar datos al **mismo** puerto de salida.

El **ancho de banda total** es la suma de los de cada uno de los puertos. Así por ejemplo si cada puerto es Fast Ethernet de 100 Mbps y hay 16 puertos tendremos 1.6 Gbps(considerando el tráfico de entrada y el de salida),pero efectivos(global del switch)son 0.8 Gbps.

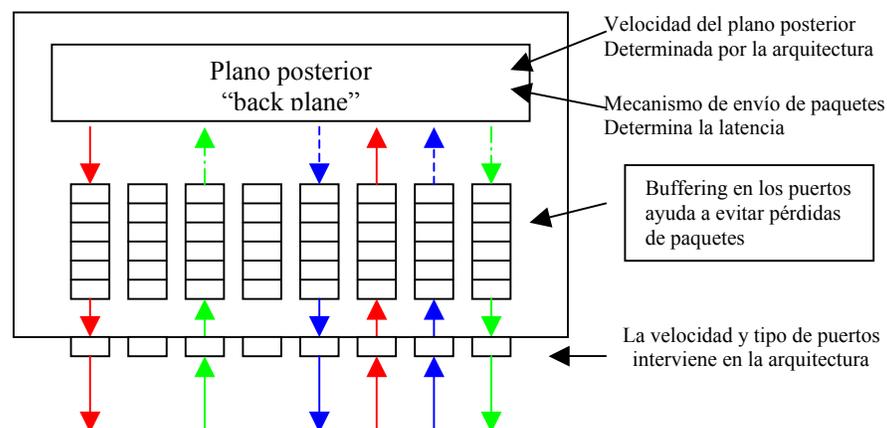
Un switch puede recibir tramas de cualquier numero de puertos y enviarlos al mismo tiempo a otros puertos,tal como muestra la **Figura 6.16**,donde entran tramas ó paquetes desde **A, B y C** que son enrutados **simultáneamente** hacia **D, E y F** respectivamente. Múltiples “canales”de datos pasan por el switch sin afectarse entre si.



**Figura 6.16** En un switch los datos van de un puerto a otro sin interferirse.

Adicionalmente los switches 10Base-T y 100Base-TX pueden incorporar puertos full duplex. que pueden ser utilizados en enlaces de alta velocidad.

Hay cuatro componentes básicos de un switch estos son: **puertos, dimensión del buffer, mecanismo de envío de paquetes y arquitectura del plano posterior(back plane)**,tal como ilustra la **Figura 6.17**.



**Figura 6.17.** Arquitectura básica del switch.

**Puertos**, inicialmente utilizados en 10Base-T y 100 Base-T además de esos tipos de puertos pueden traer puertos para 100 Base-TX, 100 Base-T4 o 100Base-FX (estos estándares serán descritos más adelante).

**Dimensión del buffer**, buffers grandes mejoran el desempeño pero son caros, por ello se utilizan mecanismos para evitar el llenado de los buffers y la pérdida de paquetes [6].

**Mecanismo de envío de paquetes**, es definido por dos factores, el primer factor es si el switch está configurado para puentear o para enrutar, esto quiere decir que algunos switches se configuran como enrutadores pues almacenan totalmente la trama recibida, la analizan y la envían al puerto correspondiente en base a la información de protocolo del encabezamiento, esto permite al enrutador dividir una LAN en subredes, enrutar entre LAN disímiles y enrutar a la WAN, otros switches están configurados como puentes, lo que significa que lee la dirección de destino y lo reenvía ó no según su "memoria" del destino de tramas anteriores. El segundo factor tiene que ver como en un switch configurado **como puente** se manejan los paquetes, hay tres modos de hacerlo:

**Almacenamiento y envío**: el switch almacena completamente la trama antes de mandarla, esto toma un tiempo, denominado **latencia**, proporcional a la longitud del paquete, que puede ser importante especialmente si se usan en **cascada**.

Ventajas: uso de CRC (detección y corrección de errores), filtros de paquetes y filtro de paquetes incompletos ó colisionados.

**Cut-through**: el switch solo examina el destino del paquete y lo envía de inmediato (como un puente o bridge común). Tiene menor latencia, no se puede usar CRC, ni filtros. Por ello se usan en grupos de usuarios pero no en backbones.

**Cut-through modificado**: combina ambos esquemas. almacena el paquete hasta que llegan 64 bytes ya que si ocurre una colisión ó un paquete está incompleto lo más probable es que ocurra al principio. Funciona como almacenamiento y envío para tramas cortas (las de control lo son) y como cut-through para las largas (las de datos).

**Arquitectura del plano posterior (backplane)**: define como los paquetes son enviados de un puerto a otro mediante la electrónica interna del switch [5].

**La gerencia y monitoreo** es más difícil que en los concentradores, se usan dos métodos uno analiza el backplane, el otro hace un "mirror" (espejo) de un puerto hacia un PC dedicado a gerencia y monitoreo. En lo que hace a **precio**: los switches aún son caros, pero eso está cambiando y cambiará rápidamente.

Existen también **switches ópticos** que conmutan paquetes entre puertos alimentados por fibra óptica, los hay de dos tipos:

- **Switches Electrónico-Ópticos**: la conmutación es electrónica, por lo que la señal luminosa debe ser convertida en eléctrica y luego nuevamente en óptica.
- **Switches Ópticos**: la conmutación es puramente óptica lo que aumenta su ancho de banda notablemente, algunos están basados en MEMS (Miniature Electro-Mechanical Systems) u otras tecnologías de conmutación.

Los switches son utilizados de muchas maneras, veamos las más importantes:

**Switches de segmentación**, los switches pueden ser diseñados para enlazar diversas LANs, Figura 6.18.

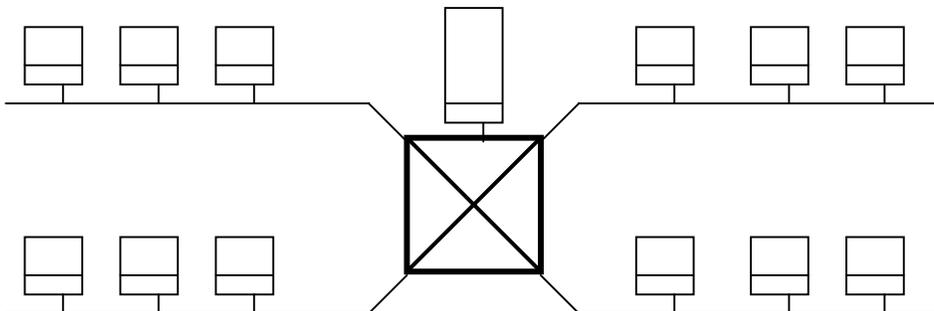


Figura 6.18. Switch de segmentación

**Switches de LAN privada**, diseñadas para conmutar tráfico entre usuarios individuales, ver Figura 6.19.

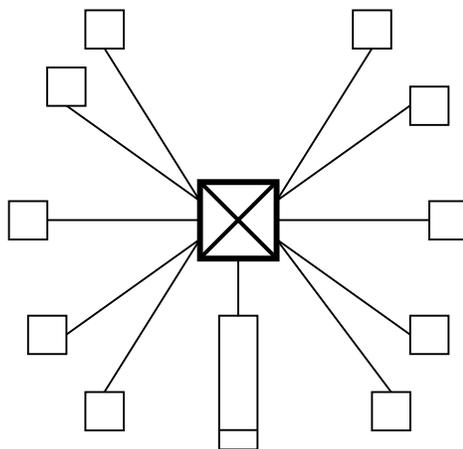
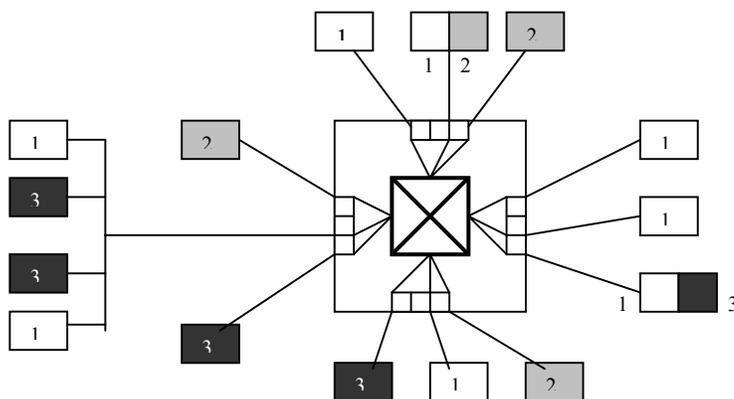


Figura 6.19. LAN privada.

**Redes LAN Virtuales**, los switches evitan que el tráfico sea difundido (broadcast) a todos los puertos, eso puede ser una dificultad cuando se desea difundir (broadcast) algo, por ello están apareciendo switches que soportan VLAN (Virtual Lans), Figura 6.20.



Cada sombreado representa una red LAN Virtual diferente(1,2 y 3)

**Figura 6.20.LANs Virtuales.**

#### **Tarjetas de interfaz de la red ó NIC(Network Interface Card) ó Network Adapter.**

Para la comunicación de las estaciones de trabajo en la LAN, la tarjeta de interfaz de red(NIC) debe estar conectada a la estación de trabajo como una opción. Esta tarjeta es conectada insertándola en uno de los slots libres que se encuentran en el slot de expansión de la estación de trabajo y utiliza el protocolo adecuado a la red: Ethernet, Token-ring, FDDI, ATM, etc.

Las **tarjetas de red** se definen como el **nodo** ó como la unidad **cliente/servidor**, cada **estación de trabajo** y cada **servidor** tiene su NIC, según que la NIC sea para un **cliente** ó para un **servidor** hay requerimientos diferentes.

Las funciones que un tarjeta de red debe manejar son:

- **Comunicación estación de trabajo-NIC**, debe mover los datos entre la tarjeta de interfaz y la memoria principal de la PC.
- **Buffering**, almacena temporalmente los datos ya sea en su paso por el cable ó hacia la memoria de la estación de trabajo, el “buffer” es necesario para compensar los retardos inherentes en el procesamiento de la información transmitida. Los servidores de red generalmente necesitan tarjetas con buffers más grandes porque manejan más tráfico.
- **Paquetes**, la tarjeta debe armar y desarmar los paquetes que utiliza la red.
- **Paralelo-serial-paralelo**, los datos vienen desde el computador en forma paralela, pero deben viajar por la red en forma serial, y viceversa,esta conversión la efectúa la NIC.
- **Codificación/Decodificación**, cuando un paquete esta listo sus unos y ceros se deben convertir al formato de transmisión por ejemplo Manchester, al llegar una señal debe efectuarse el proceso inverso.
- **Acceso al cable**, antes que un dato sea enviado la tarjeta de interfaz debe ganar acceso al cable, según sea el método de acceso al medio.
- **“Handshaking”**,antes de que sea transmitido un paquete una segunda estación debe estar lista para recibirlo, para hacerlo hay un breve período de comunicación llamado **“handshake”**.
- **Transmisión**, finalmente cuando el paquete esté listo debe ser enviado hacia la línea por un **transceiver** (descrito en la Sección 2.10.4).

En la selección de una NIC deben tenerse en cuenta[6]:

- ◆ Velocidad:10,100,10/100 Mbps,1Gbps, full duplex, ó multiple ports.
- ◆ Tipo de bus:ISA, EISA, PCI, MCA, S-Bus, NuBus.
- ◆ LAN en tarjeta madre(motherboard) pues algunas traen ya la NIC.
- ◆ Driver support, Driver Certification, Technical Support.
- ◆ Administración de red(Network Managment)(SNMP ó DMI).

**Servidores de red**, los servidores de red son computadoras que arrancan el sistema operativo de la red y lo administran, tramitan todas las comunicaciones, acceso de usuario y discos I/O, aunque pueden haber diferentes servidores para distintos hardware todas las LAN bajo el esquema cliente-servidor deben tener al menos un servidor, en una sección de este mismo Capítulo volveremos sobre el tema.

**Periféricos**, los periféricos son equipos tales como modems, fax, sistema de respaldo en cinta magnética o tipo ZIP, impresoras, etc y pueden estar ubicados en una estación de trabajo (requiere de un software especial), en un servidor(lo controla el sistema operativo) ó a través de una conexión directa(requieren adaptador de red, memoria, sistema operativo de red y su propio software). El compartirlos es una de las principales virtudes de las LANs.

**Estaciones de trabajo**, las estaciones de trabajo son computadoras personales que además de formar parte de la red pueden ser utilizadas como estación de trabajo individual en cualquier momento.

**Medio de transmisión**, a él nos referimos extensamente en la **Sección 2.2**.

### 6.10.-Normalización de las redes de área local(LANs).

Mucho del trabajo en el desarrollo de los estándares para las LANs ha sido realizado a través de IEEE. Fué organizado inicialmente un comité conocido como IEEE 802 y desarrolló estándares para LANs con velocidades de datos que van de 1 Mbps hasta 20 Mbps. Las necesidades de más y mejores estándares obligó a dividir ese comité en varios subcomités que atienden a tecnologías específicas(fibra, UTP, inalámbricos, etc) y que se titulan en base al número de la norma(por ejemplo 802.3 ó alguna de sus variantes). Para más detalles de cómo IEEE maneja esta labor de estandarización es conveniente visitar la página web del Comité de Estándares en la dirección: <http://standards.ieee.org/catalog/it.html#gen90>.

Inicialmente el Comité IEEE 802 publicó cuatro estándares, los cuales fueron adoptados en 1985 por ANSI como estándares nacionales de los Estados Unidos de América. Más tarde estos estándares fueron revisados y reemitidos por ISO en 1987 como estándares internacionales designados como ISO 8802.

El estándar 802.2 trata de una parte de la Capa 2 del modelo OSI (Enlace de Datos), denominada Control de Enlace Lógico(LLC, Logic Link Control), la otra parte de esta Capa y la Capa 1 ó Capa Física no tienen una normalización única sino que se ha optado por generar diversas recomendaciones dependiendo del tipo de configuración y el método de acceso al medio.

Como ya se ha dicho, ver el **Capítulo 4**, la Capa 2 se ha dividido en dos subniveles el Control de Enlace lógico(LLC) y el Control de Acceso al Medio(MAC), el primero es común para todas las redes locales, mientras que el MAC es específico para cada una de las configuraciones, tal como ilustra la **Figura 6.20**.

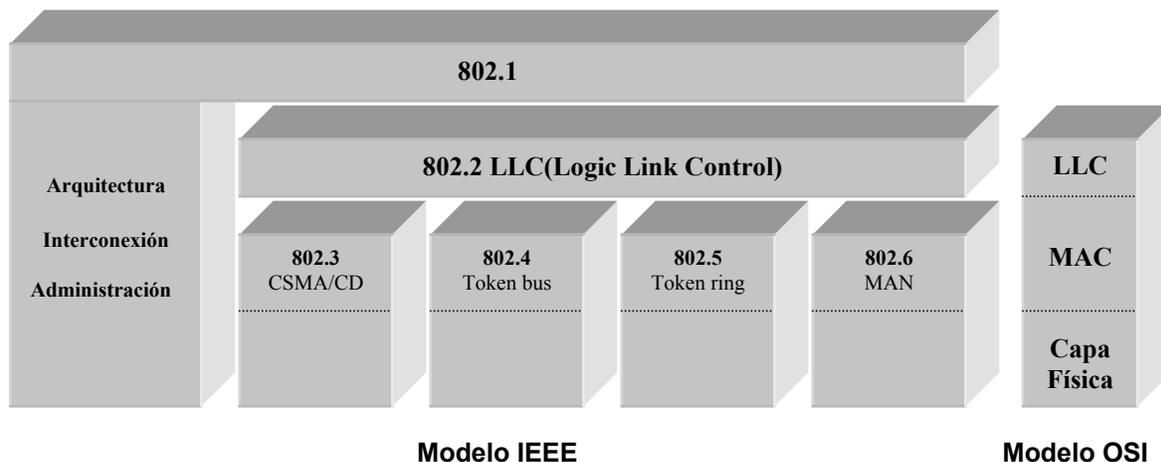


Figura 6.20 Modelos IEEE y OSI para LANs.

El trabajo del Comité 802 es organizado como se dijo en subcomités( nuevos se crean con frecuencia) y ellos a su vez se subdividen para detalles ver <http://www.ieee.org/standards> :

- ❖ **802.1** : interfaz de capa superior.
- ❖ **802.2** : Control de Enlace Lógico(LLC).
- ❖ **802.3** : Redes CSMA/CD.
- ❖ **802.4** : Redes Token Bus.
- ❖ **802.5** : Redes Token Ring.
- ❖ **802.6** : Redes de Área Metropolitana(MAN).
- ❖ **802.7** : Grupo Consejero Técnico de Banda Ancha.
- ❖ **802.8** : Grupo Consejero Técnico de Fibra Óptica.
- ❖ **802.10** : Norma para seguridad de LAN interoperable.
- ❖ **802.11** : Redes inalámbricas LAN.
- ❖ **802.12** : 100 Base VG.
- ❖ **802.15** : Redes inalámbricas **PAN (Personal Area Networks)**.
- ❖ **802.16** : Redes inalámbricas MAN.

#### 6.10.1.-Norma 802.2(Subnivel LLC).

Esta recomendación describe las funciones propias de este subnivel más los interfaces con el nivel superior(Capa de Red)y con el subnivel inferior(MAC).

La interfaz con la Capa de Red(Capa 3 del modelo OSI),describe los servicios que este subnivel, más los restantes inferiores, ofrecen a los niveles superiores, independientemente de la topología y del medio físico sobre el que se apoyen. Ofrece la transferencia de una unidad de datos a una dirección concreta(SAP) pudiendo garantizar el control de flujo y errores.

El interfaz con el subnivel de control de acceso al medio(MAC),describe los servicios que esta capa suministra al subnivel LLC, según se ha dicho existe una especificación MAC distinta para cada una de las configuraciones, pero el servicio que proporciona este nivel debe ser el mismo en todos los casos independientemente del nivel físico.

### 6.10.2.-IEEE 802.3/Ethernet.

La norma 802.3 tiene una historia interesante[6], sus bases están en el sistema ALOHA, ya descrito, luego a esta primera versión se le agregó detección de portadora. A mediados de los años 70 Xerox PARC implementó un sistema CSMA/CD de 2.94 Mbps para conectar hasta 100 estaciones personales de trabajo en un cable de 1Km de longitud.

Dado el éxito de esta red, DEC(Digital Equipment Corporation), Intel y Xerox unieron sus esfuerzos y crearon una norma llamada DIX(por las empresas) Ethernet (por *éter lumínifero*) ó simplemente Ethernet(ahora versión 1,v1)que opera en banda base( la empresa Mitre lo desarrolló para banda ancha), se utilizan en la transmisión tramas(ó frames) y el mecanismo de acceso al medio más popular(CSMA/CD).

La necesidad de un estándar que no fuese propietario de una ó varias empresas hizo que IEEE estudiase la situación y produjese la norma IEEE 802.3 que define una red similar, pero en realidad una familia completa de sistemas CSMA/CD 1-persistente operando a velocidades que van de 1 a 10 Mbps en varios medios físicos y con un formato de trama ligeramente diferente

Frecuentemente, e incorrectamente, se usa Ethernet para referirse a todos los protocolos CSMA/CD, aún cuando Ethernet sólo se refiere a un producto específico muy similar a uno que desarrolla el 802.3.

También debe aclararse que luego de emitido el 802.3 las empresas que crearon Ethernet produjeron en 1982 el Ethernet versión 2(ó Ethernet v2)que es casi igual a 802.3 excepto en el contenido de un campo de las tramas, que por lo demás son iguales, esto hace que uno deba estar atento a que protocolo se está implementando para asegurar compatibilidad, más adelante daremos alguna información sobre la tramas de estos protocolos(Ethernet,802.3 y Ethernet v2).

En lo que hace a la señal eléctrica se utiliza la Codificación Manchester, esto significa que para 10 Mbps estamos operando con un ancho de banda de 20 MHz, de acuerdo a la **eficiencia espectral** de este código,ver [13] pags. 88-91 y 175.

Hay diferentes categorías ó topologías LAN incluidas en las especificaciones 802.3,veamos las más importantes:

#### **10 Base 5(Thicknet).**

Este Ethernet "grosso" o Thicknet está basado en un coaxial grueso de 50 ohms específicamente diseñado para Ethernet,que a veces se denomina cable N-Ethernet(es similar al RG-8 y al RG-213) frecuentemente es de color amarillo con marcas negras cada 2.5 metros para indicar donde pueden colocarse las estaciones de trabajo.

La topología utilizada es lineal(bus) y el coaxial grueso es terminado en resistencias (cargas) de 50 ohms,las estaciones de trabajo son conectadas en paralelo mediante un dispositivo llamado "vampiro" que permite efectuar la conexión sin cortar el cable,que por ser grueso es difícil de conectorizar,ó bien por una T tipo "N",en la **Figura 6.21** esta conexión se denomina "tap".

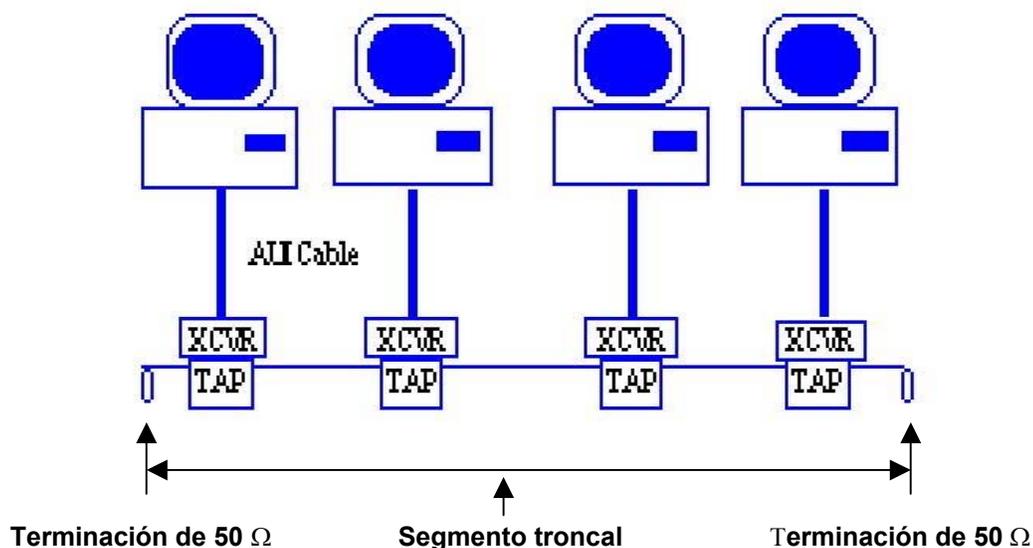


Figura 6.21. Norma 802.3 implementada con coaxial grueso (Thicknet)

El "tap" está unido (ó forma parte) de un equipo llamado "transreceptor" ó más comunmente transceiver, que en la 802.3 es denominado MAU (Media Attachment Unit, unidad de enlace al medio), que realiza funciones de la Capa 1 incluyendo detección de colisiones e inyección de los bits en la red, el transreceptor está unido a la estación de trabajo a través de un cable con conectores llamados DIX ó AUI (Attachment Unit Interface), estos son conectores de 15 pines de formato D (que es el formato de RS-232 pero con 15 pines) [7].

La Figura 6.21 nos dice que se entiende por **segmento troncal**, que a su vez está compuesto por varios **segmentos**, y muestra también que deben colocarse terminaciones (cargas) de  $50 \Omega$  en cada extremo, una de estas debe ser terminación N aterrada.

Las características de la norma 10 Base 5 son:

- ♦ La longitud máxima de un segmento troncal es de 500 metros (1.640 pies)
- ♦ Los transreceptores se conectan al segmento troncal.
- ♦ La distancia máxima entre una estación de trabajo y el transreceptor es de 50 metros (164 pies).
- ♦ La distancia mínima entre transreceptores es de 2.5 metros (8 pies).
- ♦ Pueden unirse hasta cinco segmentos troncales mediante cuatro repetidores. Las estaciones de trabajo pueden conectarse únicamente a tres de esos segmentos.
- ♦ La longitud máxima principal resultante de la unión de los segmentos es de 2460 metros (8.200 pies).
- ♦ En un segmento troncal pueden existir un máximo de 100 estaciones de trabajo, los repetidores se consideran estaciones de trabajo, o sea habrá como máximo 300 estaciones de las cuales 8 serán repetidores.

Finalmente mencionaremos que 10 Base 5 está en desuso debido a lo poco manejable del cable grueso, sin embargo debe conocerse pues hay muchas redes instaladas que requieren mantenimiento ó "upgrading".

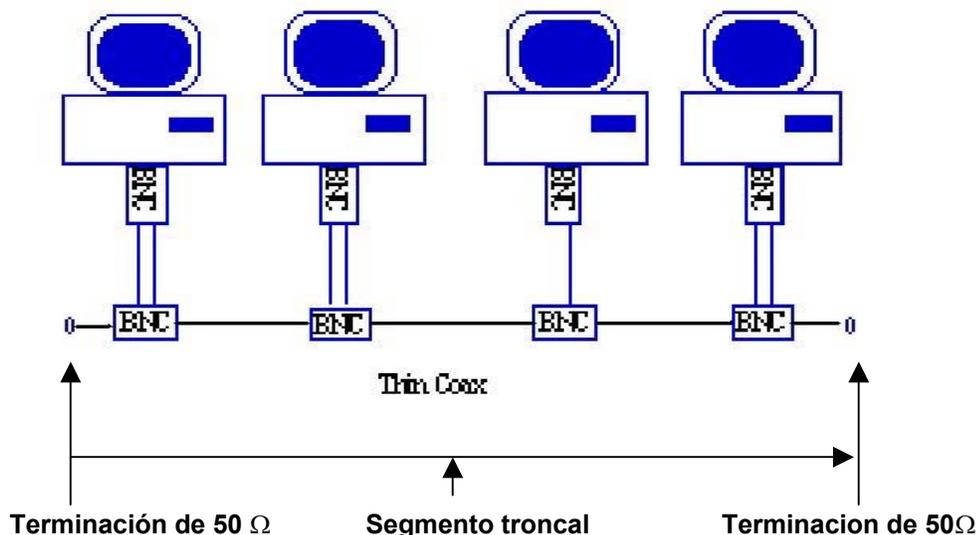
\* lamentablemente la nomenclatura a veces es confusa, MAU también es usado como dispositivo de Token Ring

**10 Base 2(Thinnet).**

El 10 Base 2 ,ó Thinnet,utiliza cable coaxil delgado,RG-58 A/U ó RG-58 C/U,que también se suministra plenum(para interiores a prueba de incendios),para interior non-plenum,subterráneo y aéreo.Cada segmento debe estar conectorizado con conectores tipo BNC.

Como se observa en la **Figura 6.22** cada segmento del coaxil fino está conectado a un T BNC que proporciona dos conexiones en sus extremos para el cable y una central conectada a la tarjeta NIC(ó tarjeta de interfaz de red)que se coloca en cualquierde los slots de expansión de la estación de trabajo.

Cada troncal estará terminado en un carga de  $50\Omega$ ,una de ellas debe estar aterrada.



**Figura 6.22.** Norma 802.3 implementada con coaxil fino(Thinnet).

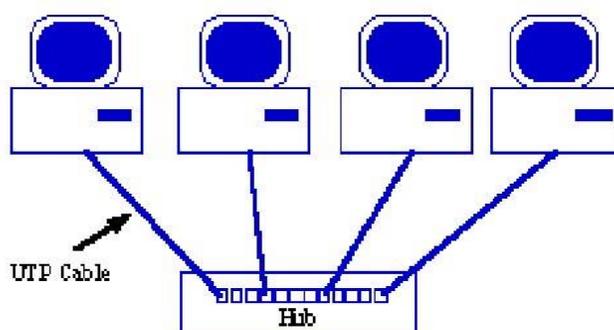
Las características de la norma 10 Base 5 son:

- ♦ La longitud máxima del segmento troncal es de 185 metros(607 pies).
- ♦ Los conectores T-BNC deben conectarse a la NIC.
- ♦ Pueden unirse hasta cinco segmentos troncales mediante cuatro repetidores. Las estaciones de trabajo solo pueden conectarse en tres de los segmentos, los otros se utilizan para extender la red.
- ♦ La longitud máxima de la línea troncal es de 925 metros(3.035 pies).
- ♦ En un segmento troncal puede haber hasta un máximo de 30 nodos, los repetidores, puentes, enrutadores y servidores se consideran nodos, o sea que tendremos un máximo de 90 nodos de los cuales 8 serán repetidores
- ♦ La línea troncal debe estar terminada con cargas BNC de  $50\Omega$  ,una de las cuales debe ser del tipo aterable.

### 10 Base-T(Par trenzado).

El 10 Base-T ofrece la mayoría de las ventajas de Ethernet sin las restricciones y el costo que impone el coaxial, utiliza cable UTP Categoría 3, ó Categoría 5 que permite crecimiento futuro a sistemas de 100 Mbps (ver **Capítulo 2**), y topología estrella con un hub ó concentrador central que sirve de repetidor para toda la red, lo que quiere decir que la señal de entrada es difundida a todas las líneas de salida. Los concentradores pueden apilarse de manera de configurar una red jerárquica

La especificación 10 Base-T incluye una utilidad de verificación de cableado denominada *verificación de integridad del enlace*, gracias a ella el sistema puede realizar controles constantes del par trenzado en busca de fallas en el cable, para ello tanto el hub como la NIC emite un "latido" pulsante cada 16 ms y tanto el hub como la NIC lo buscan, si lo reciben significa que la conexión física está en buenas condiciones, la mayoría de los equipos tienen un LED indicando la condición del enlace, la supervisión se hace desde un punto central.



**Figura 6.23. Norma 802.3 implementada con Par Trenzado(UTP)**

Esta variedad de la 802.3 fue adoptada como estándar 802.3i en 1990 y requiere de:

- Una NIC con su respectiva MAU(ó transreceptor)para la interacción el nodo con la red.(generalmente todo está en la misma tarjeta)
- Una MAU exterior para interacción entre la red y nodos coaxiales ó de fibra óptica.
- El cable UPT(3,4 ó 5) con dos pares de cable trenzado, un par para transmitir y otro para recibir, utilizando el conector de ocho pines RJ-45. Esto facilita el **full duplex**, que si bien no es parte del estándar los switches lo permiten.
- 10 Base-T utiliza codificación de Manchester pero con predistorsión de la señal a fin de permitir su transmisión sobre UTP, la frecuencia de señalización es 20 MHz.
- El concentrador ó hub, normalmente dispone de hasta 12 puertos y uno de conexión a redes coaxiales ó de fibra óptica. El concentrador puede ser externo con conectores RJ-45 ó una tarjeta llamada "peer hub" que está instalada en una de las máquinas de la red.
- Los conectores RJ-45 se usan para conectar NICs, placas de pared, concentradores,etc ,las "patas" 1 y 2 son transmisoras y las 3 y 6 receptoras, cada par está cruzado de modo que el transmisor en un extremo se conecta con el receptor del otro.

El *cableado estructurado(EIA/TIA 568)* requiere de cuatro pares trenzados.

Las características de la norma 10 Base-T son:

- ◆ La distancia desde el transreceptor hasta el concentrador no debe exceder los 100 metros(328 pies).
- ◆ Un concentrador normalmente conecta 12 estaciones de trabajo.
- ◆ Pueden conectarse hasta 12 concentradores a un concentrador central para aumentar el numero de estaciones de la red.
- ◆ Los concentradores ó hubs pueden ponerse en cascada,pero la distancia repetidor-repetidor está limitada a 100m y su número no debe hacer que se exceda el “dominio de colisión”(que se definirá un poco más adelante),esto resulta en una red con profundidad de tres a cinco repetidores(cuatro es la norma).
- ◆ 10 Base-T conserva la regla de 4 repetidores-cinco segmentos de 10 Base 5.
- ◆ Los switches descritos en la **Sección 6.9** al tomar el lugar de los hubs ó concentradores,que eran meros repetidores multipuerto,hacen que sean válidos todos los conceptos de: Segmentación,LAN privada,LAN virtuales,etc que fueron analizados en esa misma Sección con referencia a las **Figuras 6.18,6.19 y 6.20.**

### 6.10.3.-Formatos de trama para Ethernet v2, IEEE 802.3 y IEEE 802.2 ó protocolos de subcapa MAC.

Las tramas de Ethernet v2,de IEEE 802.3 y de IEEE 802.2 son muy similares,nos referiremos a ellas pués son las más utilizadas,la **Figura 6.24** muestra las correspondientes a Ethernet v2 y IEEE 802.3.

#### Ethernet v2

Preámbulo	SDF	DA	SA	Tipo	Datos LLC	Relleno	FCS
7 bytes	1	2 ó 6	2 ó 6	2 bytes	46-1518 bytes	variable	4 bytes

#### IEEE 802.3

Preámbulo	SDF	DA	SA	Longitud	Datos LLC	Relleno	FCS
7 bytes	1	2 ó 6	2 ó 6	2 bytes	46-1518 bytes	variable	4 bytes

**Figura 6.24. Trama MAC (64 bytes mínimo,todos los valores en bytes)**

Cada trama comienza con un **preámbulo** de 7 octetos cada uno con el siguiente patrón de bits:10101010,la codificación Manchester de este patrón genera una onda cuadrada de 10 MHz,durante 5.6  $\mu$ s,con el objeto que el reloj del receptor se sincronice con el del transmisor.A él sigue el **SDF**(Start Frame Delimiter),que indica el inicio de la trama y contiene la secuencia 10101011.

A continuación el campo **DA**(Destination Address)donde se dá la dirección de destino tiene 2 ó 6 bytes dependiendo de la implementación, generalmente son 6 bytes, y esa direccion puede ser una única dirección un grupo de direcciones ó una dirección global[1].El campo **SA**(Sender Address)informa sobre la dirección de origen del mensaje y generalmente es de 6 bytes.

Cada NIC tiene una dirección de 6 bytes de longitud, de los cuales tres corresponden a identificación del fabricante y los otros tres son arbitrarios.

El campo siguiente, de 2 bytes, es la diferencia entre Ethernet v2 e IEEE 802.3, en la primera informa sobre el **Tipo** de protocolo utilizado, por ejemplo IP es 0800 (ver otros en [7] pag.353), en IEEE 802.3 este campo nos da la **Longitud** del siguiente campo, que es el de datos.

Sigue el campo **Datos LLC** que contiene los paquetes pasados por el protocolo superior, de manera diferente en ambas versiones, este campo no debe ser inferior a 46 bytes, en caso que los datos no cubran los 46 bytes mínimo se usan bytes en el campo **Relleno** para completar.

Finalmente el campo **FCS** (Frame Check Sequence) contiene un CRC de 32 bits que comprueba la trama exceptuando el preámbulo, SDF y FCS.

Existe un tercer tipo de trama la IEEE 802.2 que es muy similar a la 802.3 pero incluye en el campo de datos información proveniente de la subcapa LLC, para más detalles ver [7].

Estos son los formatos de trama que se usan:

**Ethernet v2** en AppleTalk Phase I, redes conectadas a sistemas DEC ó estaciones de Trabajo que operan bajo TCP/IP.

**IEEE 802.3** en NetWare de Novell.

**IEEE 802.2** en Netware 4.x de Novell.

Aquí no finaliza la variedad existe Ethernet\_SNAP utilizada en redes AppleTalk Phase II.

Nos resta decir que la razón por la que el campo de datos debe tener al menos 46 bytes tiene dos orígenes, una debida a que cuando un transreceptor detecta una colisión trunca la trama que está transmitiendo, lo que significa que en el cable aparecerán pedazos de trama y bits parásitos, para simplificar la distinción entre tramas válidas y basura 802.3 establece que las tramas válidas deberán tener 64 bytes (512 bits) desde la dirección destinataria hasta el fin del FCS, eso da los 46 bytes mínimos para el campo de datos.

La otra razón es que la trama debe tener una longitud mínima a fin de evitar que una estación complete la transmisión de una trama corta antes que el primer bit haya alcanzado el extremo final del cable, donde pudiera sufrir una colisión con alguna otra trama, en la **Sección 6.5.2** nos referimos a esto y determinamos que: "una estación no puede estar segura de que obtuvo el canal sino hasta que ha transmitido durante  $2\tau$  sin tener una colisión", debemos ahora afinar un poco esto. En el caso de la trayectoria más larga que permite 802.3, que es de 2,5 Km considerando cuatro repetidores, tendremos que sumar la "demora" (delay) introducido por los 4 repetidores (es el tiempo de latencia dado por el fabricante, 2  $\mu$ seg típico), la demora de las NICs (que es similar) y el del cable (teniendo en cuenta que el dieléctrico es polietileno cuyo  $\epsilon_r$  es 2.3 por lo que  $v_f$  en el coaxial es de 197.814 Km/seg), se ha establecido un tiempo de ranura equivalente de 51,2  $\mu$ seg, que en este caso (10 Mbps) corresponde a los 64 bytes ó 512 bits.

El estándar 802.3 ha experimentado (y aún experimenta) muchas modificaciones, una de las más importantes es la inclusión del **IFG** (InterFrame Gap) que establece un tiempo mínimo **entre tramas**, que en el caso de Ethernet 802.3 de 10 Mbps es de 9.2  $\mu$ seg, otra es la emisión de una señal especial llamada de "**jamming**" ó "**jam signal**" que se emite apenas se detecta una colisión para alertar a las demás estaciones de este hecho.

La inclusión del IFG mejora el rendimiento de 802.3 y además asegura que una estación que transmite una trama ó paquete con éxito, si tiene más que transmitir, las sucesivas tramas **no sufrirán colisión**.

Por lo tanto CSMA/CD funcionará ahora así:

1. **CS, Carrier Sense** o detección de portadora, significa que antes de transmitir la estación "escucha" el canal, a fin de determinar si alguien lo está usando.
2. Pero de estar el canal libre, aquí esta la primer diferencia, no transmite de inmediato, sino que espera un tiempo dado por el IFG, si al cabo de ese tiempo el canal aún está libre comienza a transmitir.
3. Si el canal está ocupado, la estación lo monitorea hasta que esté libre por un tiempo igual a IFG, entonces transmite.
4. **CD, Collision Detection** o detección de colisiones, las colisiones ocurren si dos ó más estaciones "escuchan" a la red, esperan el IFG y comienzan a transmitir al mismo tiempo ó con diferencias pequeñas que no permitieron la detección de la otra(s) señal(es) que estaban aún viajando por la red. Ethernet monitorea el canal mientras transmite para determinar si lo que "oye" es diferente de lo que emitió, de serlo hubo otra señal(colisión).
5. Detectada la colisión inmediatamente cesa la transmisión y la estación envía una señal de **jamming**(de confusión) a fin de alertar a las demás estaciones de esta colisión. Las otras estaciones trasmitiendo hacen lo mismo.
6. Comienza un período de espera, llamado **backoff**, antes de que las estaciones comiencen a transmitir, este período es diferente para las diferentes estaciones y es dado por un algoritmo aleatorio especial.

La Tabla que sigue ilustra las características más importantes de Ethernet 802.3 10 Mbps.

Parámetro	Valor
Tiempo de ranura	512 tiempos de bit
InterFrame Gap	9.2 $\mu$ seg
Límite de intentos	16
Límite de backoff	10(exponente)
Dimensión de la señal <b>jam</b>	32 bits
Máxima dimensión del paquete	1518 octetos
Mínima dimensión del paquete	512 bits
Longitud de la dirección	48 bits

En Ethernet de 10 Mbps el tiempo de bit es de 0.1  $\mu$ seg

### 6.10.3.-Token ó Testigo/ IEEE 802.4,802.5 y FDDI.

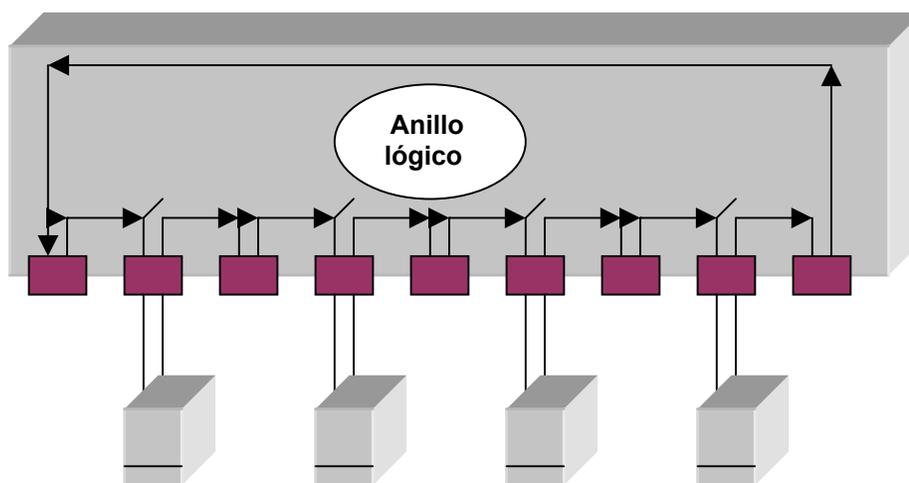
El concepto de token desarrollado por IBM y General Motors,ha sido descrito en la **Sección 6.8.4.**

La norma **IEEE 802.4** se refiere a **paso de testigo en bus(token bus)[5][7]**,en ella la topología física es lineal, pero la lógica es en anillo. Cada estación conoce la dirección de la estación ubicada a su "izquierda" y "derecha",cuando el anillo lógico se inicia la estación que tiene el mayor número es la que puede enviar la primera trama, despúes que esta lo hizo pasa autorización a su vecino inmediato, mediante una trama especial llamada **testigo** para que esta a su vez pueda transmitir información, el testigo se propaga a través del anillo lógico, de tal forma que solo su poseedor está autorizado para transmitir tramas, esto hace que no haya posibilidad de colisiones. Obsérvese que el orden físico en que están conectadas las estaciones no es importante.

El protocolo 802.4 de MAC es bastante complejo, cada una de las estaciones tiene que mantener 10 temporizadores diferentes y más de una docena de variables de estados internos.,la 802.4 ocupa más de 200 páginas. El cable utilizado es de 75  $\Omega$ ,la norma contempla cable sencillo y dual,y están autorizados tres diferentes tipos de modulación analógica.

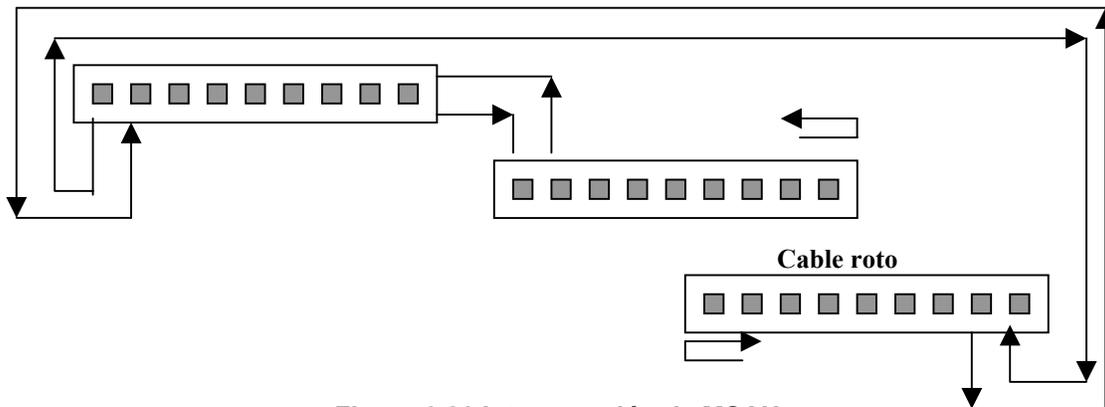
La norma **IEEE 802.5** se refiere a **paso de testigo en anillo(token ring)** y de ese tipo fueron las primeras comercializaciones de IBM a 4 Mbps a mediados de los 80.La red físicamente es estrella pero lógicamente es un anillo pues internamente las señales viajan alrededor de la red de una estación a la siguiente, ya con relación a la **Figura 6.14** se describió el funcionamiento básico de este tipo de LAN, recuérdese que el elemento básico es el MSAU(Multi Station Access Unit),que algunos autores llaman MAU(Multistation Access Unit) lo que produce cierta confusión con un equipo de siglas similares en Ethernet.

Las tarjetas de token ring están disponibles en 4 Mbps y 16 Mbps, está ultima velocidad es una mejora de IBM impulsada por los 10 Mbps de Ethernet.



**Figura 6.25.MSAU ó Unidad de acceso multiestación,que es un anillo colapsado**

La **Figura 6.25** muestra la estructura de la MSAU que es un anillo colapsado donde los estaciones activas están conectadas y los demás puertos unidos para asegurar la continuidad del anillo.



**Figura 6.26.** Interconexión de MSAU.

Varios MSAU pueden conectarse para aumentar el número de estaciones en el anillo, a configuración debe conservar la estructura lógica de anillo, tal como se vé en la **Figura 6.26**, el cable que interconecta los MSAU tienen múltiples pares de hilos de manera que si un cable se rompe, los MSAU involucrados lo detectan y forman un bucle de vuelta que mantiene la red "viva".

Las especificaciones de cables para token ring son de IBM y hay cables desde tipo 1 hasta 9, existen también conectores, cables adaptadores, cables alargadores, filtros, etc, el número de estaciones en el anillo es de 260 para cable apantallado y 72 para cable sin pantalla, la longitud máxima desde una estación de trabajo a MSAU es de 101 metros para cable Tipo 1, para más detalles ver las publicaciones de IBM.

Las **tramas de testigo en anillo** son de dos tipos: la **trama testigo** y la **trama de transferencia de información**, estas tramas se ven en la **Figura 6.27**.

#### Trama testigo

Delimitador de comienzo	Control de acceso	Delimitador final
1 byte	1 byte	1 byte

#### Trama de transferencia de información

SD	AC	FC	DA	SA	Datos	FCS	ED	FS
1	1	1	2 ó 6	2 ó 6	Variable	4	1	1

**Figura 6.27.** Tramas de token ring.

Donde:

- ◆ **Delimitador de comienzo(SD)**, tiene un código único para diferenciarlo de los datos.
- ◆ **Control de acceso(AC)**, contiene información sobre la prioridad de la trama y sobre la necesidad de futuras reservas del testigo, para que las demás estaciones lo concedan si tienen una prioridad más baja.
- ◆ **Control de trama(FC)**, define el tipo de trama bien sea de información para el Control de Acceso al Medio(MAC) ó información para una estación determinada. Esto indica que el número de tipos de trama es mayor, en realidad hay 4 tipos de tramas token ring, las tres mencionadas y una llamada Abort Sequence. Si la trama es una trama MAC la leen todas las estaciones del anillo, si contiene información únicamente la leerá la estación de destino.
- ◆ **Dirección de destino(DA)**, se puede direccionar a todas las estaciones del anillo.
- ◆ **Dirección de la fuente(SA)**.
- ◆ **Datos**, si la trama es una MAC este campo puede contener información de control adicional.
- ◆ **Secuencia de verificación de trama(FCS)**, para control de errores.
- ◆ **Delimitador de final(ED)**.
- ◆ **Estado de trama(FS)**, proporciona indicación de si una ó más estaciones en el anillo reconocen la trama, si la trama se copió ó si la estación de destino no está disponible.

En estas redes de testigo en anillo, el testigo es pasado de una estación a otra siguiendo el anillo lógico, esto se hace con un sistema llamado de "1 bit" que significa que cada uno de los bits que llegan a la interfase se copian en una memoria temporal de 1 bit, para luego ser copiado de nuevo sobre el anillo, este proceso de copiado produce un retardo de 1 bit en cada interfase que se adiciona al retardo de propagación.

Si una estación desea transmitir, debe esperar que llegue un testigo(token), cuando eso ocurre toma posesión del testigo, cambia uno de los bits del byte de control de acceso y convierte la **trama testigo** en **trama de transferencia de información**, esta se va propagando (retransmitiendo) bit a bit en cada estación, cada una de estas verifica si es destinataria del mensaje, de no serlo lo retransmite, si lo es lo lee de estar todo esta bien cambia 1 bit para indicar ACK y lo reenvía, cuando la estación originaria lo recibe, lo compara con los datos enviados para verificar la confiabilidad del anillo, reconstruye el testigo y lo reintroduce en el anillo.

Existen prioridades y mecanismos para respetarlas, así como para deshechar tramas dañadas que de otro modo quedarían circulando permanentemente en el anillo.

Token ring no es muy eficiente bajo carga ligera, funciona como mesa redonda en carga alta, se pueden implementar prioridades y reservaciones, se puede garantizar ancho de banda, hay que mantener el token y ello hace ineficiente a la red, su uso ha sido impulsado por IBM pero no ha alcanzado la difusión de Ethernet. Algunos fabricantes han introducido **token-ring switches** que sirven para dividir(segmentar) redes token-ring en redes más pequeñas y dar a cada usuario más velocidad de datos.

**FDDI(Fiber Distributed Data Interface)[5][7][8]**, es un protocolo aprobado por ANSI(X3T9.5), que sigue la filosofía de token ring, utiliza fibra óptica monomodo y multimodo, a muy altas velocidades(100 Mbps), aunque hay versiones con UTP y STP propuestas por Cabletron y Crescendo y aprobadas por ANSI en 1993(con lo que las distancias se reducen considerablemente, es llamado CDDI por Copper[5]), y está diseñada para redes LAN y MAN, las características más importantes cuando se usa fibra son:

- ◆ La topología de anillo es física y usa anillo dual en los que la información viaja en sentidos opuestos.
- ◆ El token ring es implementado de manera diferente, ya que para permitir una velocidad de transmisión alta puede tener varias tramas circulando por el anillo a la vez(tal como sucedía en versiones primitivas de token ring).
- ◆ Utiliza el sistema de codificación 4B/5B, lo que significa que transmite 5 bits por cada 4 bits de información, por ello el reloj de una red FDDI opera a 125 Mbps para 100 Mbps de velocidad de datos. Los bits están codificados como NRZ-1.
- ◆ Se usan LEDs ó láseres operando a 1300 nm.
- ◆ Soporta hasta 1000 nodos.
- ◆ La red puede tener hasta 100 Km(62 millas).
- ◆ Soporta nodos separados de hasta 2 kilómetros(1,25 millas) cuando se utiliza fibra multimodo. Y hasta 40 Km(25 millas) con fibras monomodo.
- ◆ Soporta redes híbridas, que pueden ser creadas conectando una subred(por ejemplo una colección de estaciones agrupadas en estrella ó árbol)al anillo utilizando un concentrador.
- ◆ Tiene dos variantes FDDI I y FDDI II
- ◆ Las dimensiones máximas de la trama de datos es 4500 bytes de datos más 8+ bytes de preámbulo.

La arquitectura de FDDI es utilizada en troncales(backbone)en los que la arquitectura FDDI conecta varias redes, aquí se aprovecha el ancho de banda de la fibra, también se emplean como redes posteriores\*(back-end network)conectando mainframes, minicomputadores y periféricos y como redes anteriores(front-end network)para conectar estaciones de trabajo especiales(máquinas gráficas ó de ingeniería).

Existen varias **versiones de FDDI**, la original llamada retrospectivamente FDDI-I, es **asincrónica** utilizando conmutación de paquetes y no establece ningún tipo de prioridad, se le agregó luego la posibilidad de manejar tráfico **síncrono** estableciendo priorización de tráfico sensible al tiempo, pero este sistema no garantiza el flujo uniforme de datos requerido por la voz, el video ó ciertos flujos de datos, por ello se creó FDDI-II que admite tanto conmutación de paquetes como conmutación de circuitos y en este utiliza técnicas de multiplexión de frecuencia en circuitos dedicados que pueden crear hasta 16 circuitos separados que trabajan dentro de los márgenes de velocidad establecidos entre 6.144 Mbps y 99.072 Mbps cada uno. Lamentablemente FDDI-I y FDDI-II no son compatibles y se requiere que **todos** los nodos usen FDDI-II(llamado oficialmente *hibrid ring control HRC*)de otro modo la red se convierte en FDDI-I, además las tarjetas son diferentes.

---

\* La nomenclatura que emplea back-end y front-end corresponde a informática cliente-servidor[5].

La operación de FDDI requiere:

- **Configurar el anillo dual**, como hay dos anillos uno de ellos se denomina **anillo primario** donde circula normalmente el tráfico, el otro anillo se denomina **anillo secundario** esta como reserva y en él los datos circulan en sentido contrario respecto al primario.
- **Cada estación debe ser identificada**, esto implica una única dirección, asignación de prioridades, etc. Existen dos tipos de estaciones\*\*:
  - ▶ **DAS**(dual-attachment station),que tiene dos transreceptores conectados al primer y segundo anillo respectivamente, se denominan también estaciones clase A.
  - ▶ **SAS**(single-attachment stations) con un solo transreceptor conectado al anillo primario **a través de un concentrador**(llamado DAC,dual attachment concentrator)que permite varios SASs. No es permitido conectar un SAS directamente al anillo y esto se hace para que una falla en el SAS sea contenida por el concentrador y no interrumpa la red, asimismo permiten la conexión del SAS al anillo secundario cuando sea necesario, los SAS se denominan estaciones clase B. Existen también SACs(single-attachment concentrator),tal como ilustra la **Figura 6.28**.
- Inicialmente la red comienza a operar en el modo **básico**(solo pasará al modo **híbrido** cuando lo solicite una estación),en este:
  - Un token circula de nodo a nodo.
  - Al llegar el token a un nodo pueden ocurrir dos situaciones: que no desee transmitir, en cuyo caso retransmitirá inmediatamente el token;si la estación desea transmitir, retiene el token, transmite su trama e inmediatamente transmite el token.
  - La trama llega al nodo siguiente,si está destinada a él la lee, cambia un bit(en el campo FS)y la reenvía con destino a la estación original, si la trama no está destinada a él simplemente la retransmite sin cambios.
  - Seguidamente el nodo recibe el token, si desea transmitir lo retiene, introduce su trama y libera el token. Si no desea transmitir sólo retransmite el token.

---

\*\* Los puertos también son clasificados en A,B,M y S,ver[7].

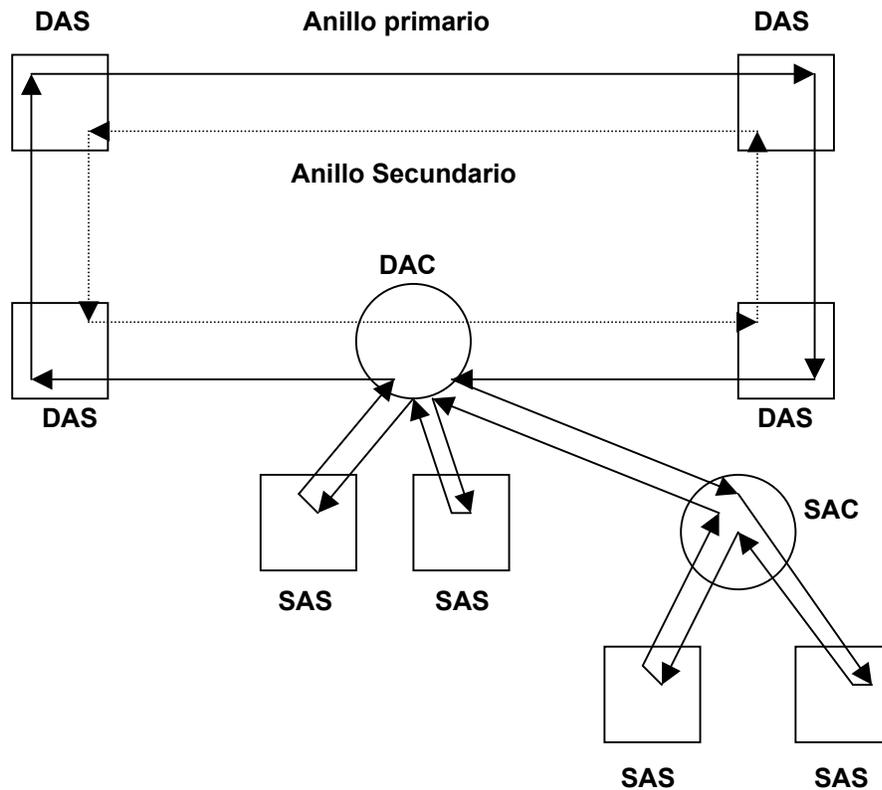


Figura 6.28. Red FDDI trabajando normalmente.

Las tramas de FDDI son de tres tipos: **testigo(tokens)**, **comando** y **datos**, las tramas de datos y comando tienen la misma estructura sólo que el campo de datos en la trama de comando tiene 0 bits, las instrucciones de comando van el campo FC, la **Figura 6.29** muestra dos de las tramas de FDDI.

Trama testigo

Preámbulo 64 bits	SD 8 bits	FC 8 bits	ED 8 bits
----------------------	--------------	--------------	--------------

Trama de datos

Preámbulo 64 bits	SD 8 b	FC 8 b	DA 16 ó 48 b	SA 16 ó 48 bs	Datos 8+ bits	FCS 32 b	ED 4 b	FS 12 b
----------------------	-----------	-----------	-----------------	------------------	------------------	-------------	-----------	------------

Figura 6.29. Tramas testigo y de datos en FDDI.

Los campos de estas tramas tienen las siguientes características:

- ◆ **Preámbulo**, consiste en 64(ó más bits)con un valor predefinido y sirve como señal de reloj para “enganchar”(sincronizar)el receptor.
- ◆ **SD(Starting Delimiter)**,delimitador de inicio.
- ◆ **FC(Frame Control)**,tiene dos versiones:
  - ❖ **Trama testigo**: se usan solo los dos bits más significativos, un valor 1000 000 indica testigo sin restricciones que puede ser utilizado sin restricciones por sistemas asíncronos y síncronos, un valor 1100 0000 indica testigo restringido, cuyo uso en sistemas asíncronos tiene limitaciones.
  - ❖ **Trama datos**: provee la siguiente información: si la trama es parte de una transmisión asincrónica ó síncrona(1 bit),si la trama tiene direcciones de 2 ó 6 bytes(1 bit),si la trama es de datos(capa LLC) ó comando(capa MAC)(2 bits),y el tipo de comando, si la trama es de comando,(4 bits).
- ◆ **DA(Destination Address)**,dirección de destino.
- ◆ **SA(Sender Address)**,dirección de origen.
- ◆ **Datos**,puede tener una longitud máxima de 5601 nibles(un nibble=4 bits).
- ◆ **FCS(Frame Check Sequence)**,para control de errores con CRC.
- ◆ **DE(End Delimiter)**,delimitador de final.
- ◆ **FS(Frame Status)**,sirve para indicar el resultado del viaje de la trama por el anillo, el destinatario indica en este campo si ha recibido correctamente la trama, un FS sin cambios indica que no fue encontrado el nodo de destino.

A pesar que FDDI significó una gran mejora en velocidad de datos, los requerimientos de los usuarios han crecido en forma continua, el Comité ANSI X3T9.3 produjo en estándar **Fibre Channel**, que trabaja a velocidades hasta 1 Gbps sobre distancias de 10 Km[8], existe otro estándar llamado **FFOL(FDDI Follow-On LAN)** que también opera a 1 Gbps.

#### 6.10.4.-Resumen comparativo de las LAN de baja velocidad.

El cuadro siguiente compara las tecnologías LAN de 10 Mbps.

Atributos	Ethernet	Token-Ring
Estándar	<ul style="list-style-type: none"> <li>◆ IEEE 802.3</li> <li>◆ Ethernet DIX v2</li> </ul>	◆ IEEE 802.5
Topología	Lineal(bus)	Anillo
Método de acceso	CSMA/CD	Paso de testigo
Medio	10 Base 5(Thicknet) 10 Base 2(Thinnet) 10 Base-T(UTP) Fibra	UTP STP Fibra
Parte del Mercado	Alrededor del 50%	Alrededor del 35%
Costo	1/3 de Token-Ring	2 a 3 veces Ethernet

### 6.11.-Otros estándares para LANs.

Además de las implementaciones ya mencionadas de los estándares IEEE 802.3,802.4,802.5 y FDDI existen muchos otros cuya cobertura detallada excede los alcances de este Capítulo,sin embargo mencionaremos algunos con una breve descripción:

- ◆ **FOIRL(Fiber Optic Inter-Repeter Link)[8]**,es una implementación en fibra óptica de la norma IEEE 802.3 y precursora del estándar 10 Base-FL.
- ◆ **10 Base F**,es la especificación IEEE 802.3 para Ethernet sobre fibra que incluye 10 Base-FP,10 Base-FB y 10 Base-FL<sup>2</sup>.
- ◆ **IsoEthernet**,es un estándar(IEEE 802.9a)que utiliza UTP categoría 2 y codificación 4B/5B con lo que logra trabajar a 16 Mbps con división por tiempo del ancho de banda, 6 Mbps para voz y video y 10 Mbps para paquetes de datos.
- ◆ **10 BROAD36**,es otra implementación de IEEE 802.3 sobre cable coaxial de 75 Ω y muy similar a un sistema de CATV,esta red usa 12 MHz ó dos canales en cada dirección de transmisión y recepción.
- ◆ **LAN Inalámbrica(WLAN,WireLess LAN)**,corresponde al estándar IEEE 802.11 y últimamente han tenido gran difusión.La norma cubre tres modos de transmisión excluyentes entre sí:DSSS(Direct Sequence Spread Spectrum),FHSS (Frequency Hopping Spread Spectrum)y DFIR(Diffused Infrared).

Con esto no hemos agotado el tema, debemos referirnos ahora a una familia muy importante que es la de los estándares que operan a 100 Mbps pero sobre líneas de cobre.

#### 6.11.1.-FastEthernet.

Con el nombre de **FastEthernet** se engloba una serie de especificaciones desarrolladas por IEEE para hacer la 802.3 compatible con el funcionamiento de LANs a 100 Mbps, como siempre el desarrollo inicial vino de la industria a través de Grand Junction Networks,3Com, SybOptics,Intel HP y otros, lo que dio lugar a varios tipos de FastEthernet, la razón de crearla es que la redes switchadas resolvían el problema de la congestión pero cada puerto estaba limitado a 10 Mbps, mayor velocidad se obtenía con FDDI pero los equipos son caros.

Básicamente han sobrevivido dos versiones de FastEthernet: 100 Base-X y 100VG-AnyLAN(también existe una 100 Base FX que es una implementación en fibra óptica de Ethernet y compatible con la capa MAC 802.3), veamos:

##### 100 Base-X[5][6].

Esta norma, conocida como 100 Base-T, es parte de la IEEE 802.3u, adoptada en Mayo de 1995,mantiene buena parte de las ideas de Ethernet, ello la hace muy atractiva pues además de tener la misma conocida filosofía, muchas de las herramientas de administración y análisis trabajan sin problemas, las características principales son:

- ◆ Velocidad de transmisión de 100 Mbps.
- ◆ Utiliza Cable UTP Categoría 3, 4 , 5 y STP tipo 1.
- ◆ Topologías: medio compartido y estrella con todos los cables conectados a un hub(switche).
- ◆ Sigue utilizando el método CSMA/CD.
- ◆ Las tarjetas NIC de 100 Base-T trabajan a 10 Base-T.
- ◆ Como 10 Base-T permite full-duplex.

<sup>2</sup> 10Base FP especifica un red que usa la fibra en topología estrella, 10Base FB usa la fibra en backbone y 10Base FL se refiere a una red que usa la fibra para conectar un nodo a un concentrador,ver [7,pag.346]

Con esta norma se implementa, el apilado de concentradores(hubs) y el “Cableado Estructurado” de EIA/TIA de el que ya hemos hablado y al que volveremos dentro de poco. Ver **Figura 6.30**

Recuerdese que se mencionó en relación a CSMA/CD que cuando la velocidad era 10 Mbps la dimensión mínima de la trama resulta de 512 bits y su duración 51.2  $\mu$ seg, ahora esa duración se divide por diez y pasa a ser 5.12  $\mu$ seg, asimismo el IFG mínimo cambia a 0.96  $\mu$ seg.

Para **10Base-T** la distancia máxima de un segmento(distancia de la estación de trabajo al concentrador es 100 metros(norma EIA 568),y se mantiene la norma de 4 repetidores/5 segmentos de 10Base5,en **100Base-T** se mantiene la distancia de 100 metros con mínima dimensión del paquete 512 bits, pero solo permite que dos repetidores sean conectados en cascada(norma 802.3u).

Como la mayoría de los concentradores para 100Base-T tienen 16 ó 32 puertos y solo se permiten 2 repetidores en cascada, el número de estaciones de trabajo es limitado.

Dentro de la 100 Base-X hay tres versiones:

- ◆ **100BaseT4:** Ethernet de 100 Mbps implementada usando cables categoría 3,4 ó 5(aunque es frecuente referirse a él como Fast Ethernet para UTP 3)de 4 hilos y no permite operación full-duplex, utiliza codificación 8B/6T.La capa MAC es compatible con la homónima de la norma 802.3.
- ◆ **100BaseTX:** Ethernet de 100 Mbps implementada sobre cables categoría 5 y tipo 1,utiliza señalización multinivel(MTL-3) y codificación 4B/5B en lugar de Manchester de 10 Base T . La capa MAC es compatible con la homónima de la norma 802.3.
- ◆ **100Base FX:** utiliza dos hilos de fibra multimodo (62.5/125 $\mu$ m) ó fibra monomodo (hay diferencias en cuanto a la máxima longitud),conectores SC, MIC ó ST, codificación 4B/5B.

A pesar de la brevedad de esta discusión 100 Base-T es de gran importancia, su bajo costo, la transición desde tecnologías conocidas, es soportada por los mayores suplidores de 10 Base-T y su uso se incrementa continuamente, ver referencia [6].

### 100VG-AnyLAN[5]

Es la especificación IEEE 802.12 que fue inicialmente desarrollada por Hewlett Packard y AT &T entre 1991 y 1994,sus características principales son:

- ◆ Velocidad de 100 Mbps.
- ◆ Funciona con cable UTP categorías 3,4, 5 de cuatro pares y tipo 1.
- ◆ La capa MAC **no** es compatible con su homónima de la norma 802.3 pues utiliza un nuevo método de acceso propietario denominado prioridad bajo demanda permitiendo que aplicaciones críticas en lo que hace al tiempo se transmitan por delante de los paquetes no críticos.
- ◆ Utiliza una arquitectura lineal con paso de testigo, por lo tanto no usa CSMA/CD y no hay colisiones.
- ◆ Puede utilizar tramas de formato Ethernet ó Token-Ring.

Esta tecnología no ha podido penetrar en el mercado debido a que solo la soporta un suplidor: Hewlett Packard, además no es Ethernet, no hay switches disponibles por lo que solo opera con medio compartido y no permite full duplex limitando su velocidad a 100 Mbps.

### 6.11.2.-Gigabit Ethernet.

Gigabit Ethernet es obviamente una Ethernet que se desea opere a 1 Gigabit, hay tres razones que impulsaron este nuevo estándar:

- **Troncales más rápidos:** con FastEthernet imponiéndose rápidamente, se necesitan troncales (backbones) más rápidos
- **Sistemas más rápidos,** a medida que la tecnología madure Gigabit Ethernet migrará hacia las estaciones de trabajo que son cada día más poderosas y por lo tanto capaces de requerir velocidades del Gbps.
- **Compatibilidad con 100Base T,** se desea utilizar el cableado ya instalado y efectuar una transición sin traumas de las 120 millones de redes Ethernet..

Fue otra vez IEEE quien liderizó el proceso creando la Gigabit Task Force P 802.3z, que trabajó duramente para escalar la operación de las redes Ethernet a 1.000Mbps reteniendo las características que han hecho de Ethernet la tecnología dominante en redes de área local(LANs).

El resultado de estos esfuerzos culminó en Junio de 1998 con la aprobación del estándar 802.3z que utiliza fibra óptica y cobre, los **1000Base-X**.

Los 1000Base-X son tres:

- **1000Base-SX,** que utiliza transreceptores con láseres de 850 nm y fibra óptica multimodo, la de diámetro 62.5  $\mu\text{m}$  con una distancia máxima de 260 metros y la de 50 $\mu\text{m}$  con 550 metros, usando conectores SC.
- **1000 Base-LX,** con transreceptores de 1300nm y fibra optica multimodo, aquí las longitudes máximas son 440 m con fibra de 62.5  $\mu\text{m}$  y 550m con fibra de 50  $\mu\text{m}$ , también con conectores SC, si se usa fibra monomodo de 9  $\mu\text{m}$  la distancia máxima sube a 3Km.
- **1000Base-CX,** con cable de cobre blindado(twin) y longitud máxima de 25 metros.

La subcapa de codificación física, PCS(Physical Coding Sublayer)del 1000Base-X se parece al estándar ANSI X3T11 Fiber Channel pues utiliza el código 8B/10B.

Gigabit Ethernet incluye full-duplex con un nuevo MAC(Media Access Control) y half-duplex, en este segundo caso retiene el método de acceso CSMA/CD.

De la implementación con **UTP5** llamado **1000Base-T** se ocupó un grupo especial, el 802.3ab.Su propuesta, aprobada en Junio de 1999, se conoce bajo esa misma sigla, utiliza cuatro pares balanceados de UTP5 y permite autonegociación entre 100 Mbps y 1000 Mbps lo que facilita la transición de uno a otro.

La tabla siguiente resume este nuevo estándar

	1000 Base LX			1000 Base-SX		1000 Base-CX	1000 Base-T
Tipo de cable	Fibra Multimodo	Fibra Multimodo	Fibra Monomodo	Fibra Multimodo	Fibra Multimodo	Cable Twin	Cable UTP5
Diámetro del núcleo	62.5 $\mu\text{m}$	50 $\mu\text{m}$	9 $\mu\text{m}$	62.5 $\mu\text{m}$	50 $\mu\text{m}$		
Distancia	440m	550m	3 Km	260m	550m	25m	100m

La información de última hora sobre Gigabit Ethernet debe buscarse en Internet <http://www.gigabit-ethernet.org> ,las referencias [9] y [10] también son útiles.

### 6.11.3.-10 Gigabit Ethernet.

La necesidad de mayores velocidades ha llevado a IEEE a constituir, en 1999, un grupo de trabajo, el 802.3ae 10 Gigabit Ethernet Task Force, a fin de establecer un estándar Ethernet a 10 Gbps que atienda a LAN, MAN y WAN. El 13 de Junio del 2002 IEEE aprobó la propuesta del comité 802.3ae que involucró el aporte de cientos de empresas en todo el mundo.

El nuevo estándar, que ofrece una actualización directa para los backbones de Gigabit Ethernet, especifica fibra óptica como medio de transmisión y utiliza operación full-duplex. Sus interfaces ópticas proveen distancias de hasta 40 Km para fibras monomodo y 300m para fibras multimodo. Se utiliza la misma arquitectura de los estándares Ethernet precedentes lo que permitirá a los usuarios migrar hacia 10Gbps reutilizando software, cableado, etc.

El estándar va más allá de la Ethernet tradicional y permite conexiones simples con otras tecnologías de redes. Una capa física opcional WAN permite que los enlaces de 10 Gbps se extiendan sobre distancias MAN y WAN. La capa WAN PHY inserta las tramas Ethernet en una carga SONET/SDH (Synchronous Optical Network/ Synchronous Digital Hierarchy), como resultado los proveedores de servicio pueden crear enlaces Ethernet de larga distancia a un costo competitivo utilizando la infraestructura ya instalada.

Con esto se asegura una convergencia extremo a extremo a alta velocidad permitiendo a los usuarios elegir velocidades de 10 Mbps a 10 Gbps y todavía tener un modelo de manejo de redes familiar y consistente entre redes de diferente velocidad.

Este nuevo estándar ya fue probado por la industria y rápidamente comenzará a instalarse, para más detalles ver <http://www.ieee802.org/>

### 6.12.-El Sistema de Cableado Estructurado.

En una organización sea esta una empresa ó una universidad el nivel más bajo de interconexión de redes es el que enlaza "grupos de trabajo" interconectados por switches ó por hubs, ó bien redes tipo bus ó token ring que deseamos interconectar. Pudieramos llamar sub-LANs a una colección de grupos de trabajo ó redes agrupadas por piso, área ó por otras razones, y LAN al conjunto del edificio, escuela ó facultad, pues estamos en un área geográfica limitada.

Se ha dicho anteriormente que en estos casos lo que se hace es una **distribución ó conexión ó cableado estructurado**, que es una organización de las conexiones para minimizar el costo y simplificar los cambios frecuentes que se producen en una organización.

La interconexión entre las sub-LANs se hace por medio de "backbones" de área local.

Tenemos entonces en este caso tres elementos importantes:

- **el acceso horizontal**, que conecta grupos de trabajo ó redes de un mismo piso ó área a un "armario de comunicaciones", en el que habrá un switch ó router, a su vez conectado con sus homólogos de otros pisos.
- **el backbone de área local**, que hace la conexión piso a piso ó entre áreas.
- **La conexión(MAN)a otros edificios.**

El backbone de área local puede tomar diferentes configuraciones, las dos más comunes son: **backbone distribuído** y **backbone colapsado**, tal como muestra la **Figura 6.30**.

El **backbone distribuído** es una técnica de encadenamiento, así por ejemplo en un edificio de diez pisos, la LAN incorpora los diez pisos, cada uno con una sub-LAN que puede estar constituída por varios grupos de trabajo, y el sótano donde se encuentran los servidores.

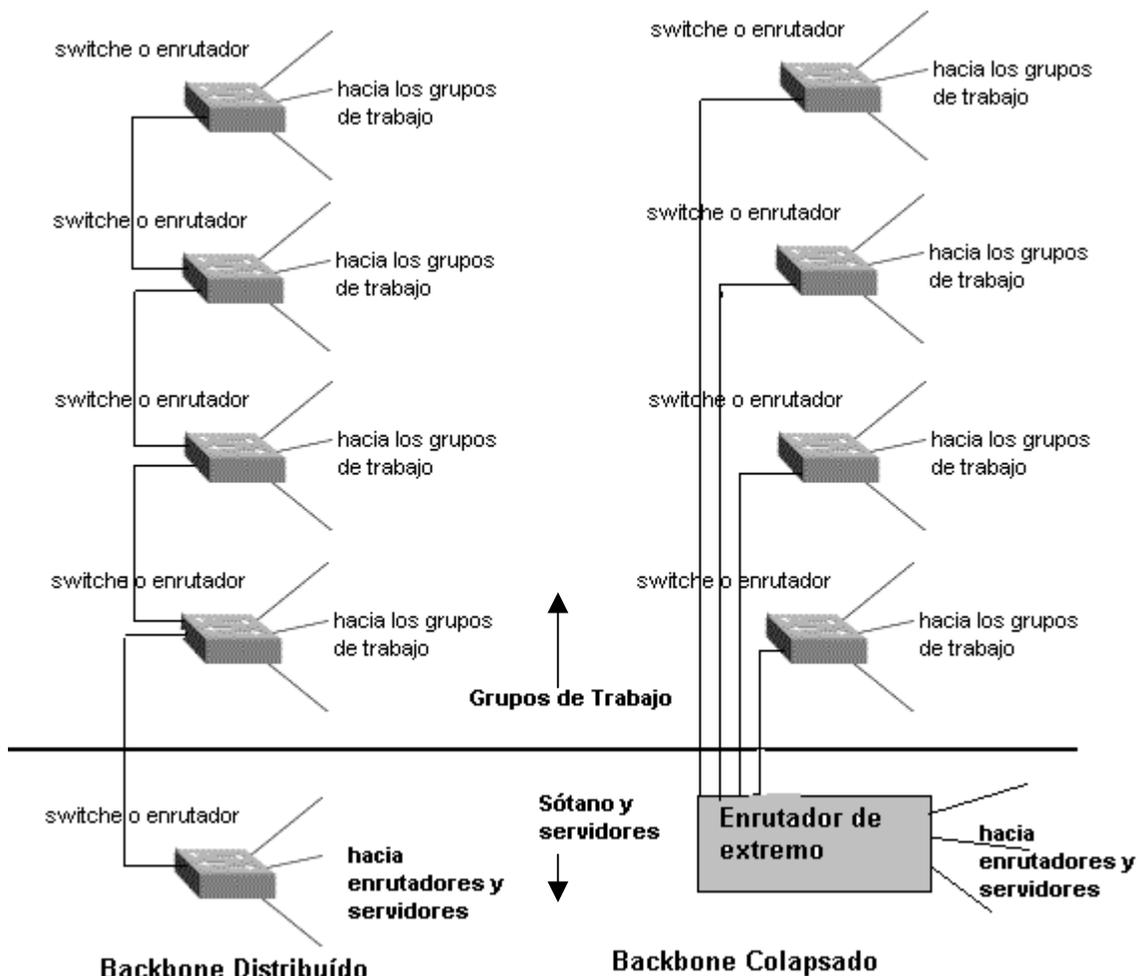
El **backbone colapsado** se instala cuando los retardos a través de los switches ó routers del backbone distribuído se hacen muy grandes, y consta de un high end router que se conecta directamente con cada sub-LAN.

Se observa que el backbone distribuído no requiere de high end router, por lo que es más económico, a lo que contribuye una menor longitud de conductores del backbone, sin embargo las latencias producidas al tener que pasar varias escalas hace que su performance sea inferior que la del backbone colapsado.

En el backbone colapsado, generalmente el router recibe y envía muchos paquetes por lo que no le queda tiempo para filtrar y enrutar paquetes a la WAN, por lo que se usa un router adicional llamado "standalone" conectando el router del collapsed backbone con la WAN, esto encarece esta arquitectura de red LAN.

**Figura 6.30. Fast Ethernet**

Durante muchos años las empresas como AT&T, Northern Telecom, Digital Equipment y Hewlett Packard introdujeron sus especificaciones de cableado estructurado llamadas **Premises Distribution Systems (PDS)**, en 1991 la EIA (Electronics Industry Association) y la TIA (Telecommunications Industry Association) comenzaron a publicar estandares para cableado e instalaciones con UTP, el EIA/TIA 568 Commercial Building Cabling Standard acoge los PDS, y a su vez fue incorporado a la norma 802.3 $\mu$  de IEEE para Fast Ethernet.



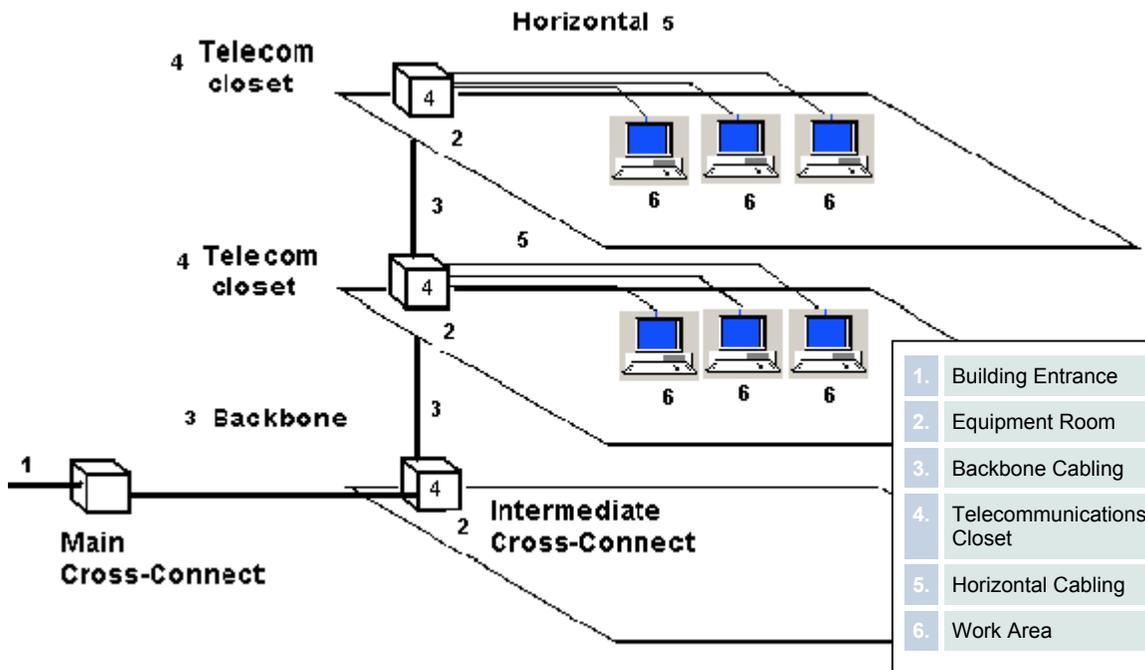
Además del estándar EIA/TIA 568(ver <http://www.anixter.com> ) existen:

- ◆ El EIA/TIA 568A que fue desarrollado como parte del 568 para UTP, esta variante se diseñó para asegurar compatibilidad con USOC, que es una secuencia de conexión creada por las empresas de teléfono.
- ◆ El EIA/TIA 568B,también parte de la 568,asegura la compatibilidad con el PDS de AT&T.
- ◆ EIA/TIA 569A Telecommunications Wiring Pathways and Spaces.
- ◆ EIA/TIA 570 Light Commercial and Residential Telecommunications Cabling.
- ◆ EIA/TIA 606 Telecommunications Cabling System Administration.
- ◆ EIA/TIA 607 Telecommunications System Grounding and Bonding Requirements.

Por otra parte se han publicado varios Boletines Técnicos de Servicio(TSB, Technical Service Bulletins), para aclarar algunos puntos del estándar, ellos son:

- TSB-36 UTP Categories 3, 4, and 5 Defined.
- TSB 40A UTP Connecting hardware for Category 3, 4, 5.
- TSB-53 Additional specifications for STP (shielded twisted pair) hardware.
- TSB-67 Transmission performance specification for field testing UTP network cabling.
- TIA/TSB-72: Centralized Optical Fiber Cabling Guidelines.
- TSB-75 Defines "zone distribution systems" for horizontal wiring.

La norma inicial EIA/TIA 568 contempla seis subsistemas que son descritos en la **Figura 6.31a y b**,en la segunda se muestra en rojo el backbone y en azul el cableado horizontal, se observa también el "Equipment Room" y el "Telecomunicaciones Closet"



**Figura 6.31a. La norma inicial EIA/TIA 568 contempla seis subsistemas**

La **Figura 6.31** y las subsiguientes no incluyen, a pesar de que aparece en la norma EIA/TIA 568,el coaxial de 50 ohms(10 Base 2),tanto en el cableado horizontal como en el backbone, por otra parte debe observarse que en el "Building Entrance" ó "Entrance Facilities" puede estar el equipo de interconexión entre edificios(de existir esa conexión).



**Figura 6.31b Cableado estructurado**

### 1. Building Entrance.

Building entrance facilities provide the point at which outdoor cabling interfaces with the intrabuilding backbone cabling. The physical requirements of the network interface are defined in the TIA/EIA-569-A standard.

### 2. Equipment Room

The design aspects of the equipment room are specified in the TIA/EIA-569-A standard. Equipment rooms usually house equipment of higher complexity than telecommunications closets. Any or all of the functions of a telecommunications closet may be provided by an equipment room.

### 3. Backbone Cabling

The backbone cabling provides interconnection between telecommunication closets, equipment rooms and entrance facilities. It consists of the backbone cables, intermediate and main cross-connects, mechanical terminations and patch cords or jumpers used for backbone-to-backbone cross-connection. This includes:

- Vertical connection between floors (risers).
- Cables between an equipment room and building cable entrance facilities
- Cables between buildings (interbuilding)

Cabling Types Recognized	Maximum Backbone Distances
100 ohm UTP (24 or 22 AWG)	800 meters (2625 ft) Voice*
150 ohm STP	90 meters (295 ft) Data*
Multimode 62.5/125 $\mu\text{m}$ optical fiber	2,000 meters (6560 ft)
Single-mode 8.3/125 $\mu\text{m}$ optical fiber	3,000 meters (9840 ft)

**\*Note:** Backbone distances are application-dependent. The maximum distances specified above are based on voice transmission for UTP and data transmission for STP and fiber. The 90-meter distance for STP applies to applications with a spectral bandwidth of 20 MHz to 300 MHz. A 90-meter distance also applies to UTP at spectral bandwidths of 5-16 MHz for CAT 3, 10 MHz for CAT 4, and 20-100 MHz for CAT 5.

Lower-speed data systems such as IBM 3270, IBM System 36, 38, AS 400 and asynchronous (RS232, 422, 423, etc.) can operate over UTP (or STP) for considerably longer distances-typically from several hundred feet to more than 1,000 feet. The actual distances depend on the type of system, data speed and the manufacturer's specifications for the system electronics and the associated components used (e.g., baluns, adapters, line drivers, etc.). Current state-of-the-art distribution facilities usually include a combination of both copper and fiber optic cables in the backbone.

### Other Design Requirements

- Star topology
- No more than two hierarchical levels of cross-connects
- Bridge taps are not allowed
- Main and intermediate cross-connect jumper or patch cord lengths should not exceed 20 meters (66 feet)
- Avoid installing in areas where sources of high levels of EMI/RFI may exist
- Grounding should meet the requirements as defined in TIA/EIA-607

**Note:** It is recommended that the user consult with equipment manufacturers, application standards and system providers for additional information when planning shared-sheath applications on UTP backbone cables.

Specified Backbone Cabling Topology: Star

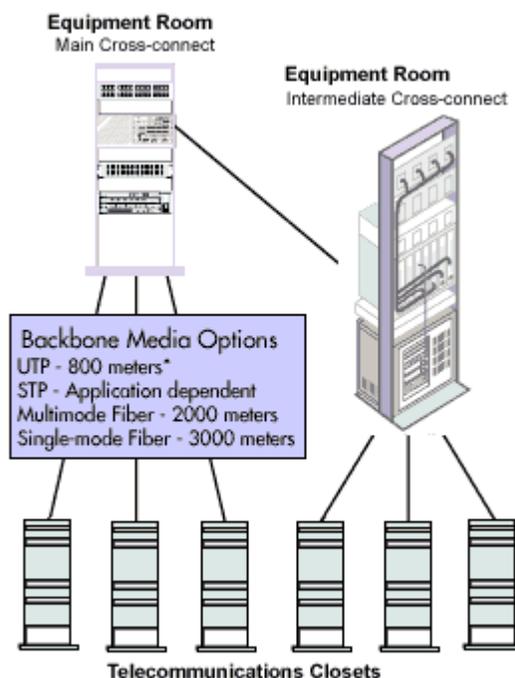


Figura 6.32. Topología Estrella

## 4. Telecommunications Closet

A telecommunications closet is the area within a building that houses the telecommunications cabling system equipment. This includes the mechanical terminations and/or cross-connect for the horizontal and backbone cabling system. Please refer to [TIA/EIA-569-A](#) for the design specifications of the telecommunications closet.

### 5. Horizontal Cabling —(Specified Horizontal Cabling Topology: Star)

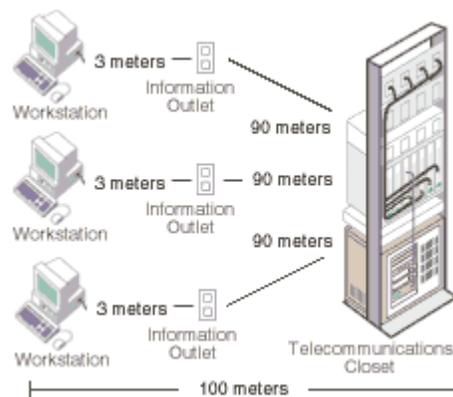
The horizontal cabling system extends from the work area telecommunications (information) outlet to the telecommunications closet and consists of the following:

- Horizontal Cabling
- Telecommunications Outlet
- Cable Terminations
- Cross-connections

Three media types are recognized as options for horizontal cabling, each extending a maximum distance of 90 meters:

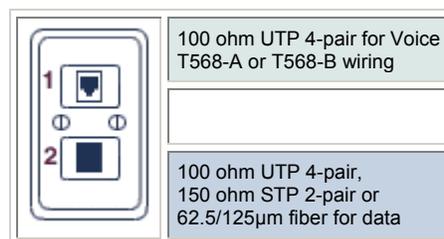
- 4-pair, 100-ohm UTP cable (24 AWG solid conductors)
- 2-pair, 150-ohm STP cables
- 2-fiber, 62.5/125- $\mu$ m optical cable

**Note:** At this time, 50-ohm coaxial cable is a recognized media type. It is not, however, recommended for new cabling installations and is expected to be removed from the next revision of this standard.



**Figura 6.33a. Maximum Distances for Horizontal Cabling**

In addition to the 90 meters of horizontal cable, a total of 10 meters is allowed for work area and telecommunications closet patch and jumper cables.



**Figura 6.33b. Telecommunications Outlet**

Each work area shall have a minimum of TWO information outlet ports, one for voice and one for data. The cabling choices are indicated in the diagram above.

**8-Position Modular Jack Pair Assignments for UTP****Application Specific Pair Assignment for 8-Position****Pin # Conductor Color Code**

1	white/green
2	green
3	white/orange
4	blue
5	white/blue
6	orange
7	white/brown
8	brown

**Pin # Conductor Color Code**

1	white/orange
2	orange
3	white/green
4	blue
5	white/blue
6	green
7	white/brown
8	brown

**Figura 6.34****6. Work Area**

The work area components extend from the telecommunications (information) outlet to the station equipment. Work area wiring is designed to be relatively simple to interconnect so that moves, adds and changes are easily managed.

**Work Area Components**

- Station Equipment — computers, data terminals, telephones, etc.
- Patch Cables — modular cords, PC adapter cables, fiber jumpers, etc.
- Adapters (baluns, etc.) — **must be external to telecommunications outlet**

El material de páginas 52 a 55 está tomado de <http://www.anixter.com/standards>, ver también la Referencia [14].

**BIBLIOGRAFÍA**

- [1] **Tanenbaum Andrew**, "Redes de Ordenadores", Segunda Edición, Prentice Hall Hispanoamericana.
- [2] **Freeman Roger L.**, "Telecommunication Transmission Handbook", Third Edition, John Wiley Interscience.
- [3] **Rodriguez Ricardo y Godoy Victor**, "Sistemas VSAT", Trabajo Especial de Grado presentado ante la Universidad de Carabobo, ver el Tutorial respectivo.
- [4] **Ramírez Ramón y García Rodolfo**, "Sistema de Packet Radio e implementación para la interconexión de redes de computadoras", Trabajo Especial de Grado presentado ante la Universidad de Carabobo.
- [5] **Sheldon Tom**, "Enciclopedia de Redes, Networking", Osborne McGraw-Hill.
- [6] **Breyer R. and Riley S.**, "Switched and Fast Ethernet: How It Works and How to Use It", Ziff-Davis Press.
- [7] **Feibel Werner**, "Novell's Complete Encyclopedia of Networking", Novel Press.
- [8] **Enck J. & Beckman M.**, "LAN to WAN Interconnection", Mc Graw-Hill.
- [9] **"Frame Bursting. A Technique for Scaling CSMA/CD to Gigabit Speeds"**, Molle M., Kalkunte M. & Kadambi J., IEEE Network July/August 1997.
- [10] **"Gigabit Ethernet: A Technical Assessment"**, Axner D, Telecommunications March 1997.
- [11] **IEEE Communications Magazine**, Número Especial "Wireless Networks", August 1997.
- [12] **Tomasi Wayne**, "Sistemas de Comunicaciones Electrónicas", Prentice Hall 1996.
- [13] **Lathi B.P.**, "Modern Digital and Analog Communication Systems", Second Edition, Holt, Rinehart y Winston Inc, 1989.
- [14] **Anixter**, "The Anixter Standards Reference Guide", January 2001.