

SIGLAS

ANS	American National Standard
ANSI	American National Standard Institute
ASK	Amplitude-Shift Keying
CATV	Community Antenna Television
CBX	Computerized Branch Exchange
CCITT	Consultative Committee on International Telegraphy and Telephony
CRC	Cyclic Redundancy Check
CSMA	Carrier-Sense Multiple Access
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection
DCE	Data Circuit-Terminating Equipment
DES	Data Encryption Standard
DOD	Department Of Defense
DTE	Data Terminal Equipment
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
FDM	Frequency-Division Multiplexing
FNP	Front-End Network Processor
FSK	Frequency-Shift Keying
HAM	Hybrid Access Method
HDLC	High-Level Data Link Control
HSLN	High-Speed Local Network
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	International Standards Organization
LAN	Local Area Network

LBT	Listen Before Talk
LCC	Lost Calls Cleared
LCD	Lost Calls Delayed
LDDI	Local Distributed Data Interface
LLC	Logical Link Control
LWT	Listen While Talk
MAC	Medium Access Control
NBS	National Bureau of Standards
NCC	Network Control Center
OSI	Open System Interconnection
PABX	Private Automatic Branch Exchange
PBX	Private Branch Exchange
PCM	Pulse Code Modulation
PDN	Public Data Network
PSK	Phase-Shift Keying
SAP	Service Access Point
SNS	Secondary Network Server
TCP	Transmission Control Protocol
TDM	Time-Division Multiplexing
TIU	Trusted Interface Unit
TMS	Time-Multiplexed Switching
TP	Transport Protocol
TSI	Time-Slot Interchange
VAN	Value-Added Network
VTP	Virtual Terminal Protocol

ESCUELA UNIVERSITARIA DE TELECOMUNICACIONES DE LAS PALMAS

TITULO: INTRODUCCION AL DISEÑO DE REDES LOCALES

AUTOR:

TUTOR:

EFREN HERNANDEZ

GONZALEZ

~~ROBERTO~~ DOMINGUEZ

RODRIGUEZ

PROLOGO:OBJETIVO DEL PROYECTO

La decision de realizar mi proyecto de fin de carrera sobre Redes Locales fue la consecuencia del interés que el tema despertó en mí a lo largo del último curso en la Escuela de Telecomunicaciones de Las Palmas. De hecho, ese mismo año realicé un trabajo de comunicación entre ordenadores en el marco de la asignatura de Transmisión de Datos (4º). Dicha experiencia resultó muy positiva y me decidió a encaminar mi proyecto hacia ese campo.

En una primera fase de recopilación de informacion a cerca de las Redes Locales, me dí cuenta de que, desgraciadamente, en nuestro país hay poca y en muchos casos desfasada. Me ví en la necesidad de "importar" la información del extranjero, más concretamente de EE.UU.

Mi objetivo era, en principio, sólo uno: dar una guía práctica, un conjunto de pautas a seguir, a cerca del diseño de Redes de Area Local a medida. Un primer contacto con el mundo de las LAN's me obligó a marcarme unos objetivos más ambiciosos.

Me dí cuenta de que para lograr mi objetivo original debía lograr antes otro más básico: dar una visión completa y técnicamente estricta de lo que son las LAN's, y de todas las técnicas que confluyen para que dichas redes sean una realidad. Esto solo, de por sí, podía haber contituido la totalidad de mi proyecto, pero lo que a mí me interesaba era el diseño, la práctica, la aplicación de esos conocimientos teóricos imprescindibles para el manejo de esta técnica de transmisión de datos.

Obviamente, el tratar de condensar los conocimientos a cerca de las LAN's que son necesarios dominar para el diseño de una red no ha sido tarea fácil. No obstante, creo haberlo conseguido tratando en todo momento de ser estricto, dejando sin tratar a fondo sólo aquellos aspectos que no son imprescindibles.

Teniendo en cuenta que este espíritu está presente a lo largo de todo el trabajo, se puede decir que las técnicas básicas utilizadas (a todos los niveles) en las Redes de Area Local figuran en la PARTE I del mismo.

La PARTE II pretende dar una orientación de cómo debe pensar el futuro diseñador de la red. Para ello se describen las características de los elementos que forman una red (Topología,MAC,...),las diferentes combinaciones de los mismos y se detallan las ventajas e inconvenientes de las redes más usadas y conocidas del mercado. Esta es, sin duda, la parte central del proyecto. Si el lector capta la filosofía de diseño de redes, puede (haciendo uso de los conocimientos adquiridos en la PARTE I y los de su formación profesional) intentar el diseño a medida de una red, con ciertas garantías de éxito.

Una vez llegado a este punto de mi trabajo, y para no dejarlo incompleto, decidí entrar en la compleja cuestión del rendimiento de las redes. Este aspecto del diseño es de una gran importancia y bien merecería la dedicación de un trabajo entero sobre el tema. En la PARTE III de mi proyecto doy una visión general de las condiciones de rendimiento de las LAN's/HSLN's, haciendo incapié en las cotas derivadas de la interrelación de los parámetros más importantes de la red.

En esta parte también incluyo una serie de apuntes sobre la metodología de conexión de varias redes ya formadas; lo que en el argot informático se denomina "Internetworking".

Para cerrar esta PARTE III y como punto final a mi proyecto, he elaborado el diseño práctico a medida de una Red de Area Local para un μ VAX II y 10 PC's de la Escuela de Telecomunicaciones de Las Palmas. En el mismo, he tratado de aplicar todos los conocimientos de redes que he detallado a lo largo de mi trabajo, así como la filosofía de diseño contenida en él. Como parte de éste diseño incluyo un presupuesto actual del coste total de la red.

INDICE

PROLOGO: OBJETIVO DEL PROYECTO	
EVOLUCION HISTORICA.....	1

***** PARTE I *****

CAPITULO 1:

INTRODUCCION.....	12
1.1 - DEFINICION DE REDES LOCALES.....	12
1.2 - REDES DE ORDENADORES.....	17
1.3 - REDES EN SALAS DE ORDENADORES.....	19
1.4 - BENEFICIOS Y ESCOLLOS.....	20
1.5 - APLICACIONES.....	24

CAPITULO 2:

TOPICOS A CERCA DE LAS COMUNICACIONES Y REDES DE

ORDENADORES.....	26
2.1 - COMUNICACION DE DATOS: CONCEPTOS.....	26
Comunicaciones analógica y digital.....	26
TECNICAS DE CODIFICACION DE DATOS.....	32
Datos digitales en señales analógicas.....	32
Datos digitales en señales digitales.....	36
Datos analógicos en señales digitales.....	39
Multiplexado.....	41
Transmisiones síncronas y asíncronas.....	43
2.2 - TECNICAS DE CONMUTACION EN LA COMUNICACION.....	46
Circuit Switching.....	48
Message Switching.....	50
Packet Switching.....	53
Técnicas de conmutación para redes locales.....	61
2.3 - REDES DE ORDENADORES. Arquitectura de	
comunicaciones.....	61
Motivación.....	61
Protocolo.....	70
Capa física.....	73
Capa de enlace de datos.....	74
Capa de red.....	80
Capa de transporte.....	83
Capa de presentación	85
Capa de aplicación.....	85

CAPITULO 3:

TECNOLOGIA DE LAS REDES LOCALES.....	86
INTRODUCCION.....	86
3.1 - TOPOLOGIAS.....	87
Topología Estrella.....	89
Topología Anillo.....	90
Topología Bus y Arbol.....	91
Elección de topología.....	92
3.2 - MEDIOS DE TRANSMISION.....	94
PAR TRENZADO.....	96
Descripción física.....	96
Características de transmisión.....	97
Conectividad.....	98
Alcance geográfico.....	99
Inmunidad a ruidos.....	99
Coste.....	100
CABLE COAXIAL.....	100
Descripción física.....	100
Características de transmisión.....	101
Conectividad.....	103
Alcance geográfico.....	103
Inmunidad a ruidos.....	104
Coste.....	104
CABLE DE FIBRA OPTICA.....	104
Descripción física.....	104
Características de transmisión.....	105

Conectividad.....	111
Alcance geográfico.....	111
Inmunidad a ruidos.....	111
Coste.....	112
LA ATMOSFERA COMO MEDIO.....	112
LA ELECCION DEL MEDIO DE TRANSMISION.....	114
3.3 - RELACION ENTRE EL MEDIO DE TRANSMISION Y LAS	
TOPOLOGIAS.....	116
Combinaciones.....	116
Disposición (Layout).....	118
3.4 - CLASES DE REDES LOCALES.....	123
Redes de área local (LAN).....	124
Redes locales de alta velocidad (HSLN).....	125
Redes locales de Circuit Switching.....	126
La elección del tipo de red.....	127

***** PARTE II *****

CAPITULO 4:

REDES DE AREA LOCAL: TOPOLOGIA Y MEDIOS DE	
TRANSMISION.....	128
4.1 - TOPOLOGIA BUS/ARBOL.....	129
Características de las LANs de Bus/Arbol.....	129
Sistemas de Banda Base.....	132
Banda Base coaxial.....	133

Banda Base con par trenzado.....	139
Sistemas de Banda Ancha.....	141
Banda Ancha con FDM.....	142
Sistemas de Banda Ancha de canal único.....	151
Banda Ancha por líneas de potencia.....	152
Banda Base versus Banda Ancha.....	153
4.2 - TOPOLOGIA ANILLO.....	155
Descripción.....	155
Beneficios del Anillo.....	160
Problemas potenciales del Anillo.....	161
Timing Jitter (inestabilidad de la base de tiempos).....	164
La arquitectura de Estrella-Anillo.....	167
4.3 - LANs DE FIBRA OPTICA.....	173
Beneficios.....	174
Estrella pasiva.....	177
Estrella activa.....	180
Anillo de fibra.....	182
Bus de fibra.....	184
CAPITULO 5:	
REDES DE AREA LOCAL: PROTOCOLOS.....	188
5.1 - PROTOCOLOS PARA LAN.....	189
Modelos de referencia.....	189

Control de acceso al medio (MAC) para	
redes locales.....	193
Round Robind.....	195
Reserva.....	196
Contención.....	196
El formato de Frames de la IEEE 802.....	197
5.2 - PROTOCOLOS DE LA CAPA DE ENLACE EN LANs.....	200
Principios.....	200
Control lógico de enlace de IEEE 802.....	205
Servicios del LLC.....	206
Protocolo LLC.....	212
Interface LLC-MAC.....	217
5.3 - CONTROL DE ACCESO AL MEDIO: BUS/ARBOL.....	218
CSMA/CD.....	219
Precursores.....	219
Descripción del CSMA/CD.....	225
El estandar CSMA/CD de IEEE 802.....	232
Token Bus.....	234
Descripción.....	234
El Token Bus de la IEEE 802.....	236
CSMA/CD versus Token Bus.....	247
Reserva centraliada.....	250
5.4 - CONTROL DE ACCESO AL MEDIO: ANILLO.....	253
Inserción en registro.....	254
Anillo particionado.....	259

Token Ring.....	262
Descripción.....	262
El Token Ring de la IEEE 802.....	264
Mantenimiento del Token.....	270

CAPITULO 6:

REDES LOCALES DE ALTA VELOCIDAD.....	272
6.1 - SISTEMAS DE CABLE COAXIAL.....	274
Bus Banda Ancha de canal único.....	276
Bus de Banda Base.....	278
Estrella pasiva.....	279
6.2 - SISTEMAS DE FIBRA OPTICA.....	280
Codificación de datos.....	281
Timing Jitter.....	285
Fiabilidad.....	286

CAPITULO 7:

REDES LOCALES DE COMUNICACION DE

LINEAS (ó CIRCUITOS).....	287
7.1 - PBX (EVOLUCION).....	288
Requerimientos para el proceso de llamadas telefónicas.....	291
Requerimientos para la conmutación de mensajes.....	295
Arquitectura de la PBX digital.....	296
Componentes de la PBX digital.....	297

Arquitectura distribuida.....	300
Arquitectura modular.....	301
Centrex.....	303
7.2 - PBX DIGITAL VERSUS LAN.....	304

CAPITULO 8:

INTERFACE DE RED.....	309
8.1 - EL REQUERIMIENTO.....	310
8.2 - INTERFACE PARA CONMUTACION DE PAQUETES.....	313
Procedimiento de enganche	
a una LAN/HSLN.....	313
La unidad de interface de red.....	316
8.3 - INTERFACE PARA LA CONMUTACION DE CIRCUITOS.....	319
8.4 - INTERFACES PARA DISPOSITIVOS ANALOGICOS.....	320

***** PARTE III *****

CAPITULO 9:

RENDIMIENTO DE LAS REDES: LAN/HSLN.....	322
9.1 - CONSIDERACIONES DE RENDIMIENTO	
EN LAN/HSLN.....	323
Medidas de rendimiento.....	323
Efectos del retardo de propagación	
y la velocidad de transmisión.....	326
Factores que afectan al rendimiento.....	336

9.2 - RENDIMIENTO DE LAS LANs.....	338
Límite sobre el rendimiento.....	338
Comparación de rendimiento en CSMA/CD y Token....	351
Rendimientos comparativos de los protocolos en Anillos.....	361
9.3 - RENDIMIENTO DE LAS HSLN.....	366
9.4 - RENDIMIENTO DE EXTREMO A EXTREMO.....	361

CAPITULO 10:

INTERNETWORKING.....	377
10.1 - ENFOQUES ARQUITECTONICOS.....	378
10.2 - REDES LOCALES HOMOGENEAS.....	381
10.3 - REDES HIBRIDAS.....	383
Ethernet y PBX.....	387
Ethernet y concentrador de terminales de larga distancia.....	389
Token Ring y concentrador.....	390
Ethernet, Token Ring y PBX.....	390
Ethernet, Token Ring y Ethernet.....	391

APENDICE A: EJEMPLO DE DISEÑO

PRACTICO DE UNA RED LOCAL.....	392
GLOSARIO.....	400
BIBLIOGRAFIA.....	424

EVOLUCION HISTORICA

Los ordenadores personales han revolucionado nuestras vidas. En los años sesenta la computerización era relativamente simple; un juego de tarjetas era introducido por el operario, y el resultado lo obteníamos en unas pocas horas ó al día siguiente. Un error en una tarjeta podría provocar el aborto del programa, lo que significaba la repetición del proceso previa revisión de las tarjetas, y la pérdida de uno ó dos días. Los setenta se convirtieron en la década de los minicomputadores y los ochenta se están revelando como los años de la microcomputadora. Aunque los computadores de hoy en día parecen más difíciles de usar, en realidad son más simples.

Los microcomputadores que empezaron como juguetes de "hobby", están generando el comienzo de una nueva era en el proceso distribuido de datos. En cuanto esta era llegue a su madurez, las "redes" jugarán un papel primordial en la consecución de una compartición de datos de forma transparente, a través de un enjambre de dispositivos.

Sin embargo, la revolución de las computadoras ha sido frenada por la incapacidad de integrar estos computadores en sistemas globales. Los microcomputadores ocupan un nivel bajo (básico) mientras que los computadores centrales (hosts computers) ocupan la cima, el nivel superior. Ambos están conectados mediante un sistema complejo con numerosas dependencias para los diferentes protocolos y formatos de datos. A estas ramificaciones se adhieren una serie de capas (layers) para soportar los requerimientos no coincidentes hardware ó de sistema operativo.

En muchas aplicaciones de negocios ó industriales los computadores personales no conectados a ningún otro dispositivo (ó red) son cada vez menos usados. La conectividad entre computadores empieza a ser la llave de la eficiencia y productividad en nuestra sociedad actual basada en la captación de información. Cada día es más indispensable que los computadores se comuniquen con grupos de usuarios y compartan sus fuentes de datos.

Los problemas surgen cuando se conectan diferentes tipos de procesadores para el intercambio de información.

Un procesador puede ser extraño a los demás y debe ser conectado a través de un protocolo industrial estándar. La conexión puede ser llevada a cabo mediante pares de cables, Ethernet, una red privada ó una Gateway. Aunque los computadores de hoy en día son simples de manejar, pueden ser conectados de una serie de modos que puedan parecer complejos. Una de estas formas es la red local (local Network).

En los últimos años, las redes de área local (LANs) han tomado una gran importancia. Las LANs son sistemas de comunicación de datos, que cubren un área física limitada (generalmente menos de una milla ó dos); con una comunicación con un ancho de banda elevado (usando un rango de frecuencia de varios MHz); a través de un medio no muy caro (generalmente cable coaxial o par trenzado); que proporciona la capacidad de "switching" (la posibilidad que tienen los usuarios de conectar unos con otros de forma selectiva); y que pertenecen, por lo general, al usuario.

Tres de los atributos físicos - área limitada, ancho de banda grande y propiedad del usuario - hacen a las LANs substancialmente diferentes de las redes de computadoras existentes. Estas operan a través de las redes telefónicas internacionales, donde las distancias son grandes, el ancho de banda es estrecho, y donde la propiedad recae sobre compañías con licencia ó en las agencias estatales. Salvando las diferencias, los

problemas a los que se enfrentan ambos tipos de redes son similares: la red ha de ser planificada por adelantado, las facilidades elegidas deben ser adquiridas e instaladas, el tráfico de datos debe ser estimado previamente a la monitorización. En ambos tipos de red, la arquitectura no individual, el medio de transmisión ó las técnicas de "switching" son apropiadas para todas las aplicaciones.

Aparte de las diferencias físicas entre las redes convencionales y las redes de área local, hay una gran diferencia en la aplicación. ambos tipos de red permiten a sus usuarios el acceso compartido a los bancos de datos, pero los **LANs** van más allá, permitiendo a sus usuarios tener acceso compartido a muchos recursos de hardware/software, como dispositivos de almacenamiento, de entrada/salida y de comunicación. Esta capacidad de acceder a los recursos de forma compartida, es una de las características mas importantes de las **LANs**.

Para entender la importancia que las **LANs** tienen en el mundo de la informatización es necesario dar un vistazo a la evolución e historia de los sistemas anteriores.

La mayor parte de la informatización que se llevaba a cabo en los últimos veinte años se realizaba en sistemas de tiempo compartido y en sistemas **batch**. Con un sistema de tiempo compartido el usuario puede escribir y correr programas desde un terminal. En cambio los "batch system" requieren la introducción de tarjetas y esperar varias

horas para saber si el programa ha tenido éxito ó no. Los sistemas de tiempo compartido han tenido mucho mayor éxito en la mayoría de las aplicaciones, pues hacen perder menos tiempo y son menos frustrantes que los batch. Los sistemas batch se siguen utilizando en aplicaciones que requieren el tratamiento de cantidades grandes de información con una mínima intervención del hombre.

Dado el éxito de los sistemas de tiempo compartido, el número de usuarios a menudo crecía hasta el punto de hacer que la respuesta del sistema se hiciese lenta y por lo tanto inoperante. La única solución a largo plazo es aumentar la potencia del computador.

El aumentar la potencia del computador puede ir acompañado por el aumento de la capacidad de gestión central ó por colocar más poder de gestión directamente en las manos del usuario.

Incrementar la capacidad de gestión central no es siempre fácil de hacer. En algunos casos, el fabricante del sistema de tiempo compartido que se está usando, no posee un modelo superior, con lo que tendríamos que acudir a otra marca. Como el cambio de marca significa un cambio de software, el cambio es traumático para la mayoría de los usuarios. En otros casos, el modelo siguiente es más potente y más costoso de lo que se desearía. Una posible solución es comprar un segundo ordenador de las mismas dimensiones y marca. La mitad de los usuarios se conectarían a uno, y la otra mitad al otro. Los problemas

comienzan cuando el usuario de uno de los ordenadores con capacidad en el suyo, no puede usarla pues sus archivos están en el otro ordenador. Este problema desaparecería si ambos ordenadores tuviesen acceso a los mismos ficheros.

Una red simple para conseguir acceso a los mismos ficheros desde dos ordenadores se muestra en la figura 1, pero tiene dos inconvenientes principales.

Una primera dificultad reside en el hecho de que cada ordenador emplea una porción de su tiempo transfiriendo ficheros al otro ordenador, para servir a aquellos

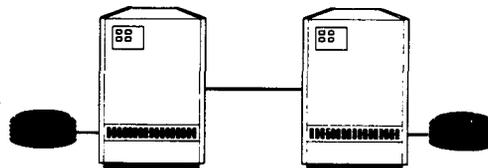


FIGURE 1

usuarios que han enganchado en el ordenador que no tiene sus ficheros. La segunda, y la más seria, es que la figura 1 no es aplicable a un número mayor de ordenadores. Necesitamos pues otro tipo de interconexión. Dos ejemplos los podemos ver en las figuras 2 y 3.

En la figura 2, el coste de los interfaces de comunicación y en algunos casos el coste de las líneas de comunicación es muy alto y se incrementan de forma notable cada vez que es añadida a la red otra computadora. En la figura 3, el coste de los interfaces y las líneas de comunicación son bajos, pero cada ordenador emplea tanto

tiempo transfiriendo información a los demás ordenadores, como dedica a sus usuarios. En realidad este sistema es poco recomendable ya que el fallo de un solo ordenador ó de una unión, dividirían el sistema en dos partes no comunicadas.

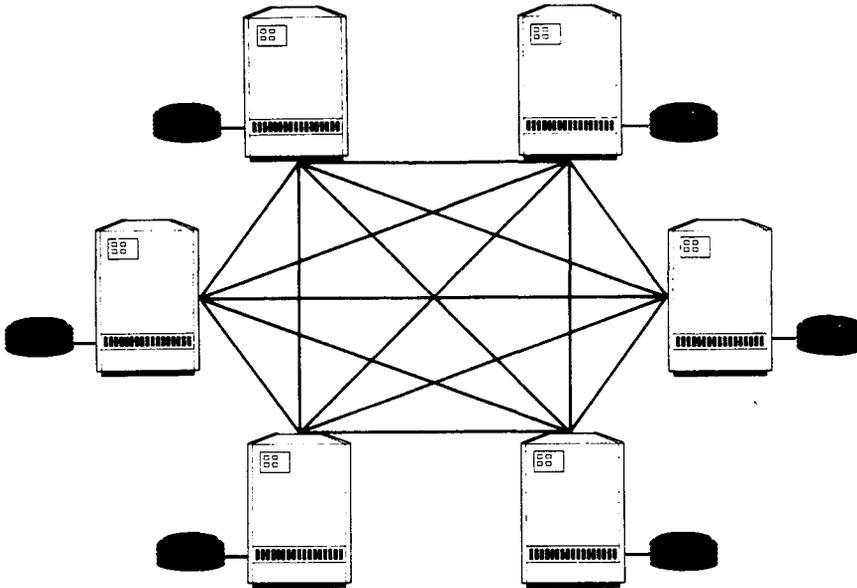


FIGURE 2

Hasta ahora hemos discutido los problemas asociados al incremento de la capacidad central de operación.

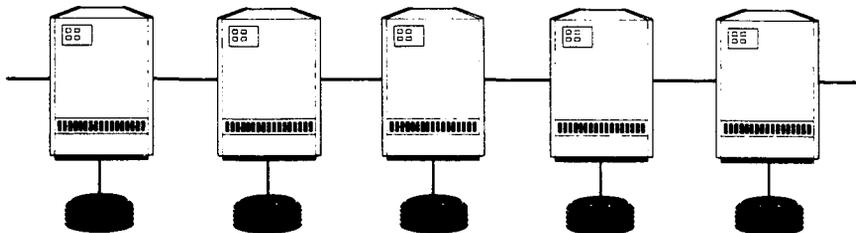


FIGURE 3

Esta era una de las dos alternativas mencionadas para la obtención de mayor poder de procesamiento. La segunda alternativa era colocar el mayor poder de procesamiento directamente en las manos del usuario, ésto es, incrementar la capacidad del terminal del usuario.

La capacidad de procesamiento de los terminales ha aumentado bastante en la última década, debido primordialmente a los cambios en la tecnología de la fabricación de los terminales. Con la aparición de los microprocesadores de muy bajo costo, muchos de los circuitos mas complejos usados en los terminales pueden ser ahora implementados con microprocesadores de forma más fácil y barata. Una vez un terminal tenga en su interior un microprocesador, el convertirlo en un pequeño ordenador es una cuestión trivial. La adición de memoria suficiente puede llevarse a cabo mediante chips de bajo costo; un disco Winchester puede proporcionarnos gran capacidad de almacenamiento de datos; y una impresora de bajo costo nos puede dar información impresa.

Una vez los terminales de usuarios han sido transformados en ordenadores personales con posibilidad de almacenamiento masivo de información, los requerimientos para la transmisión de datos cambian de las velocidades lentas necesarias para transmitir datos de teclado y pantalla, a las altas velocidades necesarias para la transmisión de ficheros. Es más, la recepción y transmisión ya no dependen del ordenador central, sino de

cualquiera de ellos. Se necesita pues, una verdadera red de ordenadores como los de las figuras 2 y 3. Pero su diseño debe ser mejorado dado el gran número de puntos conectados. Más adelante veremos los tipos de redes y las topologías que existen.

No obstante, el crear una red de ordenadores personales no es un caso particular de unir en cadena ordenadores más potentes. Por razones económicas y de otra índole, algunos servicios que son proporcionados en cada máquina de una red de grandes sistemas de tiempo compartido, debieran ser repartidos entre los usuarios de una red de ordenadores personales. Por ejemplo el acceso a los servicios de ficheros, de impresión, y de comunicación. Aunque el concepto de servicio de red (Servers) lo explicaremos más adelante, vamos a tratar varios motivos por los que es necesario tener servicios de red.

La necesidad de servicios de ficheros y de impresoras viene como consecuencia de problemas logísticos asociados con impresoras y discos. Los discos se pueden estropear, lo que hace necesario el copiarlos periódicamente. Usando un servicio de discos administrados centralmente se soluciona este problema. Hay entonces una tarea asignada a alguien encargado de hacer copias, de manera que los discos estén siempre seguros y bien cuidados.

La existencia de un ordenador equipado con un almacenamiento masivo (discos) que proporcione una

facilidad de acceso a ficheros centralizados es conveniente para los usuarios, pues un usuario puede acceder al dato deseado desde cualquier ordenador de la red. El usuario no tiene que buscar un determinado diskette en ningún cajón. Este sistema también acaba con el problema de la duplicidad de datos almacenados (no como en las bases de datos distribuidas). Es mucho mejor que todos trabajen en la misma base de datos y que la pongan todos al día.

El tener una impresora para cada ordenador personal resulta excesivamente caro. Por otro lado la calidad de estas es baja. Los usuarios de impresora necesitan de ellas, pero también de las impresoras centrales, las cuales les proporcionan un gran rendimiento y calidad.

Por último hay que tener en cuenta que las LANs no se limitan al campo de los ordenadores personales. Los ordenadores centrales o principales (mainframes computers) tienen un papel importante en las LANs.

Primero, algunos problemas no pueden ser resueltos en máquinas pequeñas. Sobre todos aquellos que llevan consigo el procesamiento de una gran cantidad de datos con una alta velocidad y precisión. Conectando una de estas computadoras centrales a una LAN y utilizando el software adecuado, podemos hacer que esta capacidad de procesamiento esté disponible para todo el mundo en la red.

Segundo, El poder de procesamiento de un equipo crece

al cuadrado del precio que se paga por él. Es decir, por el doble de dinero podemos tener un equipo cuatro veces más potente.

Resumiendo, las **LANs** son interesantes y tienen éxito pues permiten a sus usuarios con terminales, pequeños ordenadores y grandes computadoras compartir el acceso a recursos como almacenamiento, dispositivos de comunicaciones y de entrada/salida. Además, pueden compartir la misma información y comunicarse entre ellos.

PARTE I

INTRODUCCION

1.1

DEFINICION DE REDES LOCALES.

Para formular una definición del término Red Local (Local Network), y para caracterizar el propósito de tales redes, es importante comprender las causas que han motivado el uso de este tipo de redes.

Lo más importante es el dramático y continuo descenso de los costos del hardware, acompañado de un incremento en la capacidad de éste mismo hardware. Hoy en día un microprocesador tiene la velocidad, los juegos de instrucciones y la capacidad de memoria de los mejores minicomputadores de hace unos años. Esto ha producido una serie de cambios en cómo la información es recopilada, procesada y organizada. Hay un incremento de uso de

sistemas de una sola función, como procesadores de texto y pequeñas computadoras de negocios, y de microcomputadoras de uso general como las computadoras personales y las estaciones de trabajo (Workstations) multiusuario. Estos sistemas pequeños y discretos son más accesibles para el usuario, más rentables y más fáciles de usar que un sistema central de tiempo compartido.

Todos estos factores nos llevan a un número mayor de sistemas en un sólo sitio: un edificio de oficinas, una factoría, un centro de operaciones, etc... Al mismo tiempo ha surgido un deseo de interconectar estos sistemas debido a un buen número de razones, incluyendo:

- * Compartir e intercambiar datos entre sistemas.
- * Compartir recursos caros, dividiendo así los costos.

Esta facultad de intercambio de datos entre ordenadores obliga a la interconexión de sistemas de diferentes naturalezas. los usuarios individuales de ordenadores no trabajarán más aislados, pudiendo retener los beneficios que proporciona un sistema central. En estos beneficios se incluye la posibilidad de cruzar mensajes con otros usuarios, acceder a datos de muchas fuentes diferentes y la capacidad para varios usuarios de compartir información de un fichero común.

La segunda razón antes apuntada se explica si consideramos que aunque el coste de Hardware destinado al proceso de datos ha descendido, el de los equipos electromecánicos esenciales, tales como los elementos de

almacenamiento o las impresoras lineales, permanece alto.

Llegado a este punto, podemos dar ya la siguiente definición de Red Local:

Una Red Local es una red de comunicaciones que hace posible la interconexión de una variedad de dispositivos de comunicación de datos dentro de un área reducida.

Hay tres elementos significativos en esta definición.

Primero, una Red Local es una red de comunicaciones. Esto es, nos dá la posibilidad (facultad) de mover bits de datos de un sistema unido a ella, a otro también unido a la misma. El Software a nivel de aplicación y los protocolos necesarios para enganchar (conectar) dispositivos de una manera que trabajen de una forma cooperativa los veremos y detallaremos más adelante. En esta definición que hemos dado, no se incluyen los conjuntos de dispositivos interconectados mediante uniones punto-a-punto.

Segundo, vamos a considerar los "dispositivos de comunicación de datos" (de la definición) como dispositivos que se comunican a través de un medio de transmisión. Ejemplos:

- * Computadores.
- * Terminales.
- * Dispositivos periféricos.
- * Sensores (Temperatura, Humedad, ...).
- * Teléfonos.
- * Transmisores y receptores de TV.

* Fascimil.

Hay que tener en cuenta que no todos los tipos de Redes de Area Local son capaces de soportar todos estos dispositivos.

Tercero, El radio de acción de una Red Local es pequeño. Lo más corriente es que la red se confine a un sólo edificio. Aunque también son muy usuales las que se extienden a varios edificios, como un campus universitario o una base militar. Su radio de acción puede prolongarse a unas pocas decenas de kilómetros.

Otro elemento que puede ser añadido a la definición es que generalmente las redes locales son propiedad privada. Aunque no es extraño que una organización sencilla englobando ante la red, como los dispositivos conectados a ella.

Algunas de las características típicas de una red de área local son:

- * Alta velocidad de transmisión (0.1 a 100 Mbps).
- * Distancias cortas (0.1 a 25 Km.).
- * Baja tasa de error (10^{-8} a 10^{-11}).

Los dos primeros parámetros sirven para diferenciar las redes locales de dos "primos" suyos: los sistemas multiprocesadores y las redes de largo alcance (Long-Haul Networks). Esto está ilustrado en la figura 1.1. Dicha figura indica tres tipos de redes locales: redes de área local, redes locales de alta velocidad y la PBX ó *Private Branch Exchanges* (Teléfonos). Todas ellas serán definidas

con posterioridad.

Existe otra diferencia entre las redes locales y sus dos primos. Diferencia que va a influir mucho en el diseño y operación de la misma. Las redes locales tienen menos errores de transmisión y menor coste que las redes de transporte. De este modo los costes de funcionamiento y utilización son sensiblemente diferentes. Incluso, como habitualmente la red local pertenece a la misma organización a la que pertenecen los dispositivos conectados a ella, es posible conseguir una gran integración entre la red y los dispositivos conectados.

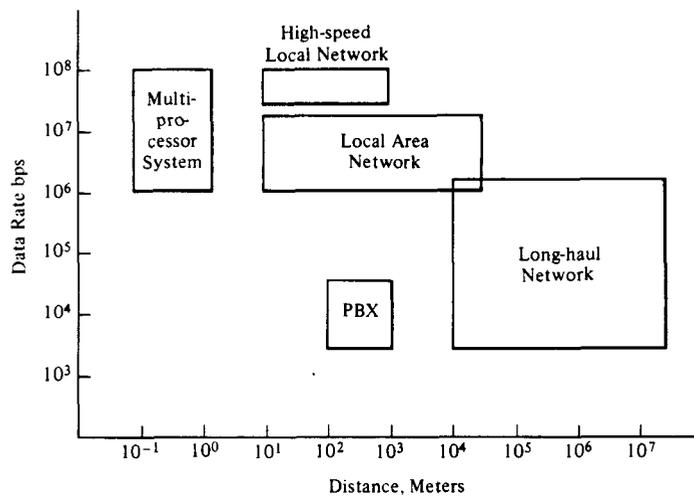


FIGURE 1-1. Comparison of Multiprocessor Systems, Local Networks, and Long-Haul Networks

REDES DE ORDENADORES PERSONALES.

Comenzaremos por un extremo; un sistema diseñado para soportar microcomputadores tales como ordenadores personales. Con éste bajo coste, un gerente puede organizar estos equipos para que cada uno cubra en solitario una aplicación determinada. Hoy en día los ordenadores personales incorporan los procesadores, el almacenamiento de ficheros, los lenguajes de alto nivel y las herramientas para solventar problemas en un sólo paquete. La razón, pues, para adquirir este sistema es clara.

Pero una colección de procesadores independientes no solventan todas las necesidades de una organización compleja. Se requieren facilidades de procesamiento central. Algunos programas, como modelo de proyectos de economía, no pueden correr en computadoras pequeñas. Los extensos ficheros de una corporación como sus cuentas y las nóminas, requieren un tratamiento centralizado, pero pueden ser accesibles a un número de usuarios. También existen una serie de archivos que, aunque especializados, deben ser compartidos por un determinado número de usuarios. Yendo más lejos, hay poderosas razones para conectar estaciones de trabajo inteligentes e individuales entre sí. Por ejemplo, si los miembros de un proyecto ó de

un equipo de organización necesitan compartir información y trabajo, la forma mejor de hacerlo es electromecánicamente.

La figura 1.2 es un ejemplo de una red local de ordenadores personales para un hipotético grupo de ingenieros aeroespaciales ó departamento. La figura muestra cuatro tipos de usuarios que tienen ordenadores personales, cada uno equipado con una aplicación particular.

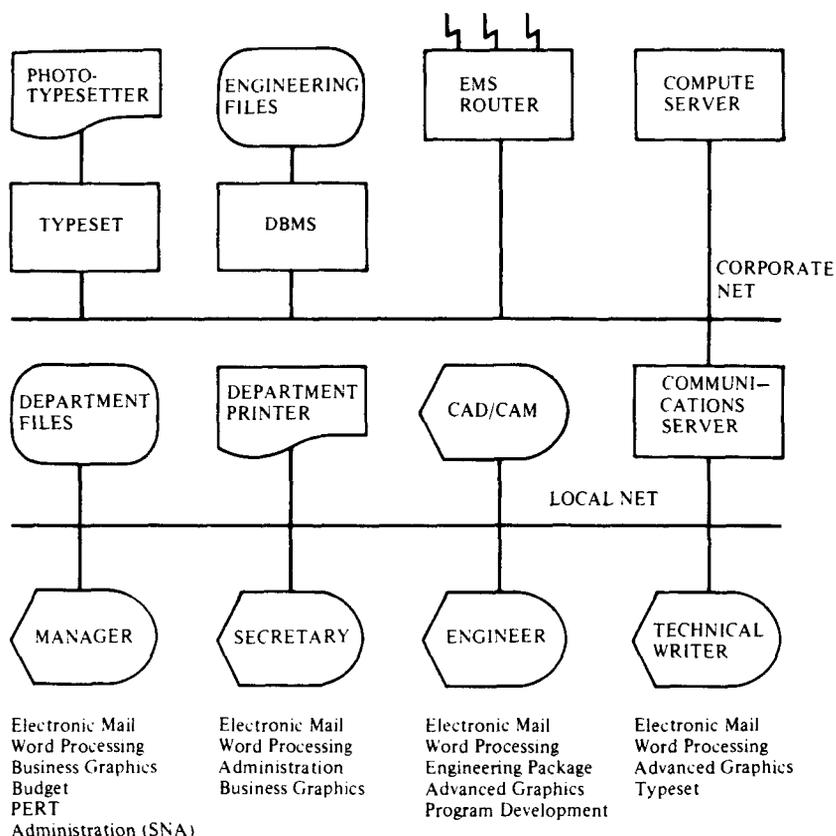


FIGURE 1-2. Personal Computers in Support of a Working Team

Cada tipo de usuario está equipado con correo electrónico y procesador de textos para proporcionarle la eficiencia de la creación y distribución de mensajes, memos e informes. Los gerentes tienen también a su disposición una serie de programas de utilidades y herramientas para elaborar presupuestos de gerencia. Con la automatización que suministran los ordenadores personales, las herramientas como el calendario electrónico y el soporte gráfico se vuelven de gran valor para estos trabajadores. Del mismo modo, los ingenieros pueden ser provistos de equipos a medida.

Ciertos recursos caros, como los discos ó la impresora, pueden ser compartidos por todos los usuarios de la red. Además, la red puede ser enlazada a otra red mayor de la corporación. Un *server* de comunicación se encargaría de controlar el acceso a estos recursos.

Un requerimiento clave para el éxito de una red de este tipo es el bajo coste. El coste de conexión de dispositivos a la red será próximo al precio del dispositivo a conectar.

1.3

REDES EN SALAS DE ORDENADORES.

En el otro extremo de las redes de ordenadores personales hay una diseñada para ser usada en una sala de

ordenadores en la que hay grandes y caros *Mainframe Computers*. Este es un ejemplo de lo que llamaremos más adelante red local de alta velocidad (HSLN ó High-speed Local Network). La HSLN tiene aplicación en lugares de gran volumen de procesamiento. Normalmente estos lugares son grandes compañías ó instalaciones de investigación con un gran presupuesto para el proceso de datos. Dado el nivel en el que se mueven dichas compañías, una pequeña diferencia en la productividad, puede suponer millones de dólares. Es más, aunque las HSLN son escasas en número, el coste colectivo del equipo que soportan es muy alto.

1.4

BENEFICIOS Y ESCOLLOS.

La tabla 1.1. muestra algunos de los beneficios principales de las redes locales. Que éstos de produzcan o no depende, por supuesto, de la habilidad y sabiduría de aquellos encargados de la selección y manejo de la red local.

Uno de los beneficios potenciales se refiere a la evolución de sistemas. En una instalación sin red, como un sistema de tiempo compartido, todo el procesamiento de datos se encuentra en uno o unos pocos sistemas. A la hora de renovar el Hardware, el Software de aplicación existente debe ser convertido al nuevo Hardware ó

reprogramado, con el riesgo de error en cualquier caso. Incluso añadiendo nuevas aplicaciones al mismo Hardware, ó rehaciendo las ya existentes, se tiene el riesgo de introducir errores y de reducir el rendimiento del sistema entero. Con una red local, es posible reemplazar gradualmente las aplicaciones ó los sistemas, evitando el "todo ó nada". Otra faceta de esta capacidad es que el equipo viejo puede ser dejado en el sistema, para que se encargue de una determinada aplicación sí el coste del traslado de dicha aplicación a la nueva no está justificado.

Una red local tiende a dar la fiabilidad, disponibilidad y mantenibilidad propios de la facilidad del proceso de datos. Con múltiples sistemas interconectados, la pérdida de un sistema simple, tendría un impacto mínimo. Es más, un sistema puede ser diseñado de forma redundante, de tal manera que otros sistemas puedan hacerse cargo de la situación en caso de fallo.

El compartir recursos no incluye solamente a los caros dispositivos periféricos, sino también a los datos en sí. Estos datos pueden ser almacenados y controlados desde un punto, pero via red, estar disponibles a muchos usuarios.

Las redes locales nos proporcionan la capacidad de conectar a ellas dispositivos de diferentes marcas, lo que supone una gran flexibilidad y poder de elección. No obstante, nos proporciona un nivel de interconexión más

bien bajo. Esto es, que para el correcto funcionamiento de la red necesitamos un Software para nuestra red de alto nivel.

Estos son, junto a los demás que se listan en la tabla 1.1, los beneficios más sobresalientes de las redes locales.

TABLE 1.1 Benefits and Pitfalls of Local Networks

Potential Benefits

System evolution: incremental changes with contained impact
Reliability/availability/survivability: multiple interconnected systems disperse functions and provide backup capability
Resource sharing: expensive peripherals, hosts, data
Multivendor support: customer not locked in to a single vendor
Improved response/performance
User needs single terminal to access multiple systems
Flexibility of equipment location
Integration of data processing and office automation

Potential Pitfalls

Interoperability is not guaranteed: software, data
A distributed data base raises problems of integrity, security/privacy
Creeping escalation: more equipment will be procured than is actually needed
Loss of control: more difficult to manage and enforce standards

También hay que hacer incapié en los escollos ó escollos potenciales con lo que podemos tropezar. Como ya hemos mencionado, las redes locales no garantizan que dos dispositivos puedan ser usados de modo cooperativo, un concepto que se conoce como "Interoperability". Por ejemplo, dos procesadores de texto de diferentes marcas

pueden ser conectados a una red local, y quizás puedan intercambiar datos. Pero probablemente use diferentes formatos de ficheros y diferentes caracteres de control así que no es posible, directamente, tomar un fichero de uno, y editarlo en el otro. Se necesita un Software de conversiones de formato.

Con una red local, es posible que los datos sean distribuidos, o por lo menos, que el acceso a los datos vengan de muchas fuentes. Esto plantea dudas de integridad (Ej.: dos usuarios tratando simultáneamente de poner al día su base de datos) y de seguridad.

Otro escollo a superar es el denominado "Creeping Escalation". En una gran corporación, cada gerente de departamento puede hacer los pedidos de equipo que considere necesarios. En un momento dado, si todos los departamentos obran igual, la totalidad de pedidos de la corporación pueden exceder sus necesidades reales. Tenemos pues un problema de pérdida de control. Vemos pues que la primera virtud del interconexionado por red, es también su primer peligro. Es difícil manejar estos recursos para dar fuerza al Software estándar y a los datos, y para controlar la información disponible en la red.

Terminaremos este apartado con un sumario reflejado en la tabla 1.2, basado en una encuesta hecha a usuarios de redes locales. Mientras unos usuarios notan efectos positivos, un número similar informan de manera negativa de la instalación de la red local. Las exageradas y

conflictivas exigencias de los vendedores de equipos pueden llevar al posible usuario a la confusión y al desengaño.

TABLE 1.2 Organizational Effects of Local Networks

Affected Area	Positive Effects	Negative Effects
Work quality	Wider data accessibility; fewer "lost" items. Wider participation in creating and reviewing work	Indeterminate or mediocre data quality; reduced independence and initiative
Productivity	Increased work load handled by more powerful office-systems equipment	Greater resources used to perform inconsequential work
Employee changes	Improved skill levels in current staff More challenging work Reduced status distinctions	Fewer jobs for marginal performers Less personal interaction Insufficient status distinctions
Decision-making effectiveness	Quicker availability of relevant facts Greater analytic capability More people involved in hypothesis building and testing	Factual component of decision making becomes too high "Forest and trees" problem could encourage "group think"
Organizational structure	More effective decentralization	Decentralization can get out of control
Costs	Overall cost reduction	Overall cost increase; soft benefits used as justification
Total impact	Permits the planning of new business approaches	Creates increased complexity and poorly functioning dependence relationships

1.5

APLICACIONES.

El rango de aplicaciones a las redes locales es muy amplio. La tabla 1.3 muestra algunas de las aplicaciones potenciales. Es preciso repetir que no todas las redes locales son capaces de soportar todas las aplicaciones.

TABLE 1.3 Local Network Applications

Data Processing	Energy management
Data entry	Heating
Transaction processing	Ventilation
File transfer	Air conditioning
Inquiry/response	Process control
Batch/RJE	Fire and security
Office automation	Sensors/alarms
Document/word processing	Cameras and monitors
Electronic mail	Telephones
Intelligent copying/facsimile	Teleconferencing
Factory automation	Television
CAD/CAM	Off-the-air
Inventory control/order entry/shipping	Video presentations
Monitor and control of factory floor equipment	

TOPICOS A CERCA DE LAS COMU- NICACIONES Y REDES DE ORDENA- DORES

2.1

COMUNICACION DE DATOS: CONCEPTOS.

Comunicaciones Analógica y Digital:

No es necesario explicar aquí el significado de los términos analógico y digital, pues su significado es bien conocido por todo aquel que esté medianamente iniciado en el mundo de la electrónica. Ambas acepciones se usan mucho en tres contextos:

- Datos.
- Señales.
- Transmisión.

Brévemente, definiremos el término "dato" (data), como entidades que llevan consigo un significado. El término "dato" tiene que ver con la forma de algo; el término "información" tiene que ver con el contenido ó interpretación de esos datos. Las "señales" son codificaciones eléctricas ó electromagnéticas de datos. La "señalización" (signaling) es el acto de propagar la señal a lo largo de un medio adecuado. Por último, "transmisión" es la comunicación de datos a través de la propagación y posterior procesamiento de señales.

Los datos analógicos toman valores continuos en algunos intervalos. Por ejemplo la voz ó la señal de video, tienen patrones de intensidad continuamente cambiantes. Los datos digitales toman valores discretos.

En un sistema de comunicaciones, los datos se propagan de un punto a otro por medio de señales eléctricas. Una señal eléctrica es una onda electromagnética que varía constantemente y que puede ser transmitida por una amplia variedad de medios, dependiendo de la frecuencia; por ejemplo por medio de cables, por fibras ópticas ó por la atmósfera y el espacio. Una señal digital es una secuencia de pulsos de voltaje que pueden ser transmitidos a través de cable; un nivel positivo constante representa un 1 binario, mientras que un nivel negativo constante representa un 0 binario.

La ventaja principal de la señal digital frente a la analógica, es que es más barata y más inmune al ruido que

ésta. Pero su principal inconveniente es que las señales digitales sufren mayor atenuación que las analógicas.

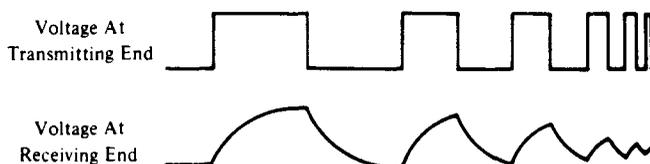


FIGURE 2-1. Attenuation of Digital Signals

La figura 2.1 muestra la forma de la información al ser transmitida y al recibirse. Debido a la atenuación ó a la disminución del ancho del pulso a altas frecuencias, los pulsos en la recepción se vuelven pequeños y redondeados. Es obvio pensar que ésto puede significar la pérdida de la información contenida en la señal.

Ambos datos, analógicos y digitales, pueden ser representados y propagados por medio de señales analógicas o digitales. Esto se ilustra en la figura 2.2. Generalmente, los datos analógicos son una función del tiempo y ocupan un espectro de frecuencias limitado. Estos datos pueden ser representados directamente por una señal electromagnética del mismo rango de frecuencias. El mejor ejemplo de ésto son los datos de voz. Como ondas de sonido los datos de voz se mueven entre los 20 Hz y los 20 KHz. No obstante, la mayoría de la energía cae en una banda más estrecha, entre 300 y 3400 Hz. El teléfono usa este rango

de frecuencias para propagar de forma inteligible y clara la conversación. Para todo sonido de entrada comprendido entre 300 y 3400 Hz, se produce una señal electromagnética con la misma amplitud de frecuencia. El proceso se invierte para convertir la energía electromagnética en sonido.

Los datos digitales también pueden ser representados por señales analógicas usando un Modem (modulador / demodulador). El modem convierte una sucesión de pulsos (de dos valores) en una señal analógica, modulando una frecuencia portadora (Carrier Frequency). La señal resultante ocupará un cierto espectro de la voz, así éstos pueden ser propagados a través de las líneas ordinarias de teléfonos. Otro modem al final de la línea se encarga de demodular la señal analógica para recuperar los datos originales.

En una operación similar a la realizada por el modem, los datos analógicos pueden ser representados por señales digitales. El dispositivo que realiza esta función para los datos de voz se llama Codec (codificador / decodificador). En esencia el codificador aproxima la señal analógica a una sucesión de bits. Al otro lado de la línea un codificador reconstruye la señal analógica a partir de la sucesión de pulsos.

Por último, los datos digitales pueden ser expresados directamente, en forma binaria, por los niveles de voltaje. No obstante, los datos binarios son

codificados para mejorar sus características de propagación.

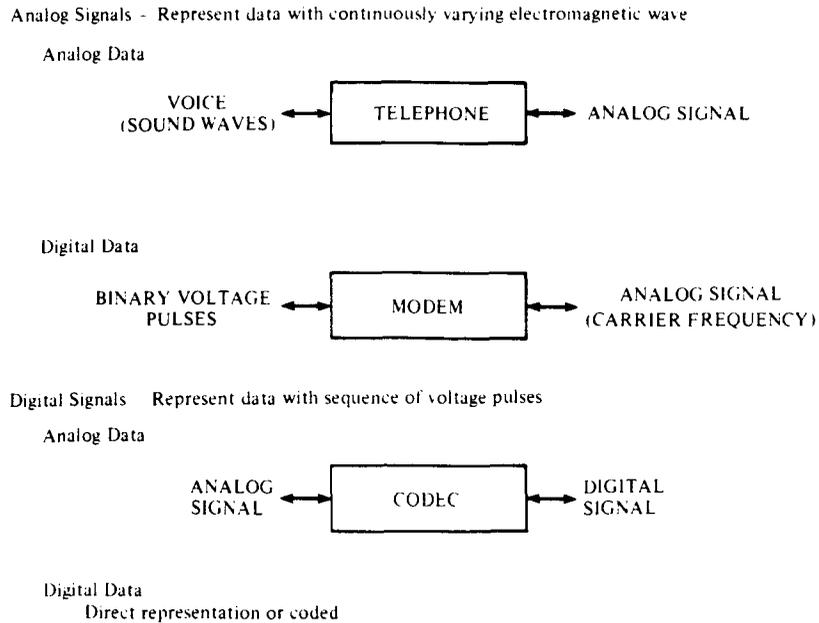


FIGURE 2-2. Analog and Digital Signaling for Analog and Digital Data

Debemos tambien indicar que tanto las señales analógicas como digitales deben ser transmitidas por un medio adecuado. El tratamiento que reciben las señales está en función del sistema de transmisión. En la tabla 2.1 tenemos un resumen de los métodos de transmisión. En ella, transmisión analógica es la transmisión de señales analógicas sin reparar en su contenido; pudiendo representar datos analógicos (voz) ó digitales (datos pasados a traves de un modem). En cualquier caso la señal se atenuará a partir de una cierta distancia. Para alcanzar mayores distancias tendríamos que añadir

amplificadores que incrementen la energía de la señal. Aunque un bit de error no afecta en nada a la señal analógica, hay que tener en cuenta que los amplificadores en cascada, si se usan con datos digitales, pueden introducir errores.

TABLE 2.1 Analog and Digital Transmission

(a) Treatment of Signals

	Analog Transmission	Digital Transmission
Analog Signal	Is propagated through amplifiers; same treatment for both analog and digital data	Assumes digital data; at propagation points, data in signal are recovered and new analog signal is generated
Digital Signal	Not used	Repeaters retransmit new signal; same treatment for both analog and digital data

(b) Possible Combinations

	Analog Transmission	Digital Transmission
Analog Data	Analog signal	Digital signal
Digital Data	Analog signal	Digital signal Analog signal

En la transmisión digital, por el contrario, hay que tener en cuenta el contenido de la señal, pues ésta sólo puede ser transmitida una cierta distancia antes de que la atenuación la degrade. Para alcanzar mayores distancias, es necesario usar repetidores. El repetidor recibe la señal, recupera la sucesión de 1's y 0's y transmite una nueva señal sin atenuación.

Se puede usar la misma técnica con la transmisión de señales analógicas en las que se transporte información digital. Se usarían entonces dispositivos de transmisión

en vez de amplificadores.

Para comunicaciones de larga distancia las señales digitales no son tan versátiles y prácticas como las analógicas. Por ejemplo, las señales digitales son imposibles de transmitir mediante satélites y sistemas de microondas. No obstante, en términos de costo y calidad, la transmisión de señales digitales es superior a la de señales analógicas. Lo que los sistemas de comunicaciones de larga distancia se hayan ido convirtiendo gradualmente en sistemas de transmisión digitales para voz y para datos digitales.

Veremos que en las redes locales, la tendencia no siempre es la misma que en las comunicaciones de larga distancia. Es cierto, en el contexto local, las técnicas digitales tienden a ser más económicas debido a la reducción de costo de los circuitos digitales. Sin embargo, las distancias limitadas con las que se trabaja en las redes locales, reducen los problemas de atenuación y de ruido, por lo que el coste y calidad de las técnicas analógicas se asemejan a las digitales. Por lo tanto hay un espacio de aplicación seguro para la aplicación de señales analógicas y transmisión analógica en las redes locales.

TECNICAS DE CODIFICACION DE DATOS:

Datos digitales en señales analógicas:

La base de la transmisión de señales analógicas es una señal continua de frecuencia constante conocida como la portadora. Los datos digitales son codificados mediante la modulación de una de las tres características de la portadora: amplitud, frecuencia y fase, ó alguna combinación de éstas. La figura 2.3 ilustra las tres formas básicas de modulación de señales analógicas para datos digitales:

- * Modulación en amplitud (Amplitude Shift-Keying) (ASK)
- * Modulación en frecuencia (Frequency Shift-Keying) (FSK)
- * Modulación en fase (Phase Shift-Keying) (PSK)

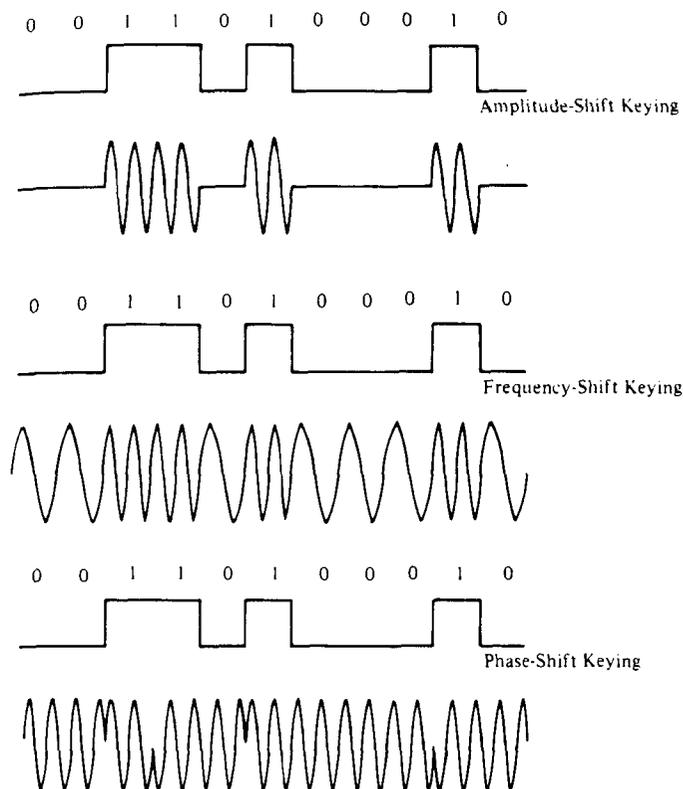


FIGURE 2-3. Modulation of Analog Signals for Digital Data

En cualquier caso, la señal resultante contiene un rango de frecuencias a ambos lados de la frecuencia portadora. Este rango se denomina "ancho de banda" de la señal.

En la modulación ASK, los valores binarios son representados con dos amplitudes distintas de la frecuencia portadora. En algunos casos, una de las amplitudes es cero; ésto es, uno de los dígitos binarios es representado por la presencia, con amplitud constante, de la portadora y el otro por la ausencia de la misma. ASK puede presentar cambios repentinos de ganancia, lo que hace de ello una técnica no muy eficiente.

En FSK, los dos valores binarios son representados por frecuencias diferentes cerca de la frecuencia portadora. Este tipo de modulación es más inmune a errores. Es usada en las transmisiones de radio de alta frecuencia (3 a 30MHz), y puede ser usada también en las altas frecuencias usadas en las redes locales que utilizan cable coaxial.

La figura 2.4 muestra un ejemplo del uso de FSK para la operación en *Full-Duplex* de una línea de voz (telefonía). "Full-duplex" significa que los datos pueden ser transmitidos en ambas direcciones al mismo tiempo. Una banda es usada para el envío y otra para la recepción. La figura 2.4 es una especificación de los modems de la serie 108 de Bell System. En una dirección (transmitir ó recibir) el modem pasa frecuencias en el rango que va

desde 300 a 1700 Hz. Las dos frecuencias usadas para representar los 1's y los 0's, están centradas en los 1.170 Hz, con un desplazamiento de 100 Hz a cada lado de la misma. Del mismo modo, para la otra dirección (recibir ó transmitir) el modem pasa de 1.700 a 3000Hz y usa una frecuencia central de 2.125 Hz. El área sombreada alrededor de cada par de frecuencias indica el ancho de banda de cada señal. Hay que hacer notar que hay un pequeño solapamiento y por tanto una pequeña interferencia.

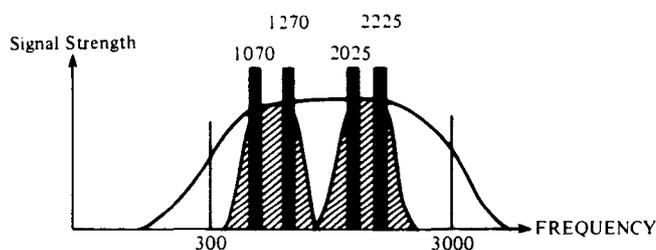


FIGURE 2-4. Full-Duplex FSK Transmission on a Voice-Grade Line

En PSK, la fase de la señal portadora es desplazada para representar datos. En la figura 2.3 hay un ejemplo de un sistema de dos fases. En este sistema, un "cero" es representado mediante el envío de un ciclo de señal con la misma fase que el anterior. Mientras que un "uno" es representado enviando un ciclo de señal de fase opuesta al anterior. La PSK es más inmune al ruido y más eficiente que la FSK.

Hay que señalar que las técnicas descritas

anteriormente pueden ser combinadas. Una combinación común es la PSK y ASK, donde algunos o todos los desplazamientos de fase, pueden ocurrir en dos amplitudes diferentes.

Datos digitales con señales digitales:

La manera más fácil y común de transmitir señales digitales, es usar dos voltajes diferentes para los dos dígitos binarios. Por ejemplo, la ausencia de voltaje se usa para representar el 0, mientras que un voltaje positivo y constante representa el 1. Es también muy común el uso de un nivel negativo (Low) para el 0, y un nivel positivo (High) para el 1. Esta técnica se denomina: *Non-Return to Zero (NRZ)* y se muestra en la figura 2.5a.

La transmisión NRZ tiene desventajas sensibles. Es difícil de determinar donde termina un bit y donde empieza el otro. Por ello es necesario tener sincronizados el receptor y el transmisor, tanto si se trata de una transmisión síncrona como asíncrona.

También hay una componente de corriente continua durante el tiempo de cada bit, que se acumula si predominan los 1's ó los 0's. Así, el acoplamiento de la corriente alterna, que usa un transformador y da un aislamiento eléctrico perfecto entre dispositivos de comunicación de datos y el medio que les rodea, no es posible. Es más, esta componente puede llegar a dañar los contactos de unión.

Hay un juego de técnicas de codificación, agrupadas

bajo el nombre de "bifase", los cuales no presentan estos problemas. Dos de estas técnicas, "Manchester" y "Differential Manchester" son usadas comunmente en las redes locales. Todos estos diseños bifásicos necesitan de al menos una transición por bit, pueden ser dos. Así que la velocidad máxima de modulación es del doble que para la NRZ; esto significa que el ancho de banda ó la capacidad consumida es mayor.

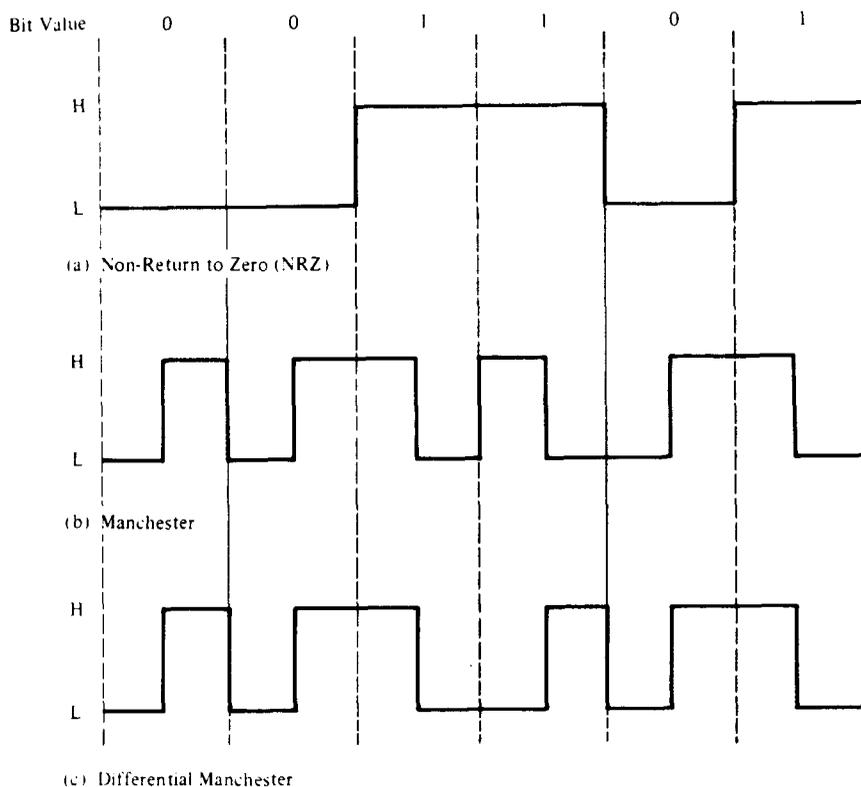


FIGURE 2-5. Digital Signal Encoding

Para compensar ésto, los diseños bifásicos tienen una serie de ventajas:

* Sincronización: Como va a haber una transmisión segura durante cada bit, el receptor puede sincronizar con

ella. Por esta razón los códigos bifásicos son conocidos como códigos Auto-Clocking (autosincronizados).

* No tienen componente DC: Pues hay una transición en cada bit.

* Detección de errores: La ausencia de una transición esperada puede utilizarse para la detección de errores. El ruido en la línea tendría que invertir la señal dos veces, antes y después de la transición esperada, para provocar un error no detectado.

En el código Manchester (figura 2.5b), hay una transición en medio del periodo de cada bit. Esta transmisión a mitad del bit sirve tanto de reloj como de dato: una transición de alto a bajo (H→L) representa un 1, y una transición de bajo a alto (L→H) representa un 0. En el código Differential Manchester (figura 2.5c), la transición en mitad de cada bit se usa solamente para la sincronización. La codificación de 0 (1) es representada por la presencia (ausencia) de una transición al comienzo del periodo del bit.

La Differential Manchester muestra una ventaja adicional. En esta codificación, la señal es decodificada comparando la polaridad de los elementos adyacentes de la señal, en vez del valor absoluto de un elemento de la señal. Una ventaja de este diseño es que puede ser fiable detectar una transmisión en presencia de ruido, que comparar un valor con una tensión umbral.

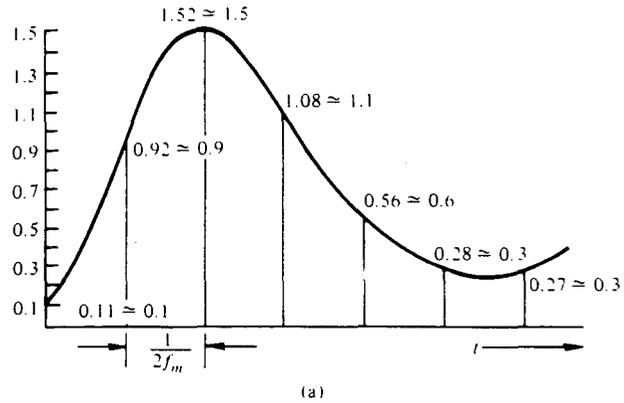
Datos analógicos en señales digitales:

El ejemplo más común del uso de señales digitales para codificar datos analógicos es la modulación de código de pulso (Pulse Code Modulation) (PCM), que es usada para la codificación de señales de voz.

La PCM está basada en el teorema que estableció en 1.985 E. Jordan:

Sí una señal $f(t)$ es muestreada a intervalos regulares de tiempo y a una velocidad mayor a dos veces la frecuencia de la señal más significativa, entonces el muestreo contiene toda la información de la señal original. La función $f(t)$ puede ser reconstruida a partir de estos muestreos por medio de un filtro paso bajo.

Sí la voz está limitada a frecuencias de 4.000 Hz, haciendo 8.000 muestreos por segundo podríamos caracterizar la señal de voz. Hay que tener en cuenta que éstos son muestreos analógicos. Para convertirlos en digitales, cada uno debe tener asignado un código binario. La figura 2.6 muestra un ejemplo en el cual cada muestreo es aproximado, mediante cuantización, a uno de los 16 niveles. Cada muestreo puede ser pues representado por cuatro bits. Ahora podemos ya reconstruir de manera exacta la señal. Sí usamos un muestreo de 7 bits, que permite 128 valores diferentes, la calidad de la señal reconstruida es comparable a la recibida por vías analógicas. Esto implica que a una velocidad de muestreo de 8.000 muestras por segundo, por 7 bits de muestreo, se necesitan 5 Kb/seg.



Digit	Binary equivalent	Pulse-code waveform
0	0000	
1	0001	
2	0010	
3	0011	
4	0100	
5	0101	
6	0110	
7	0111	
8	1000	
9	1001	
10	1010	
11	1011	
12	1100	
13	1101	
14	1110	
15	1111	

(b)

FIGURE 2-6. Pulse Code Modulation

La PCM puede ser usada, desde luego, para otro tipo de señal analógica a parte de la voz. Por ejemplo, la señal de TV tiene un ancho de banda útil de 4.6 MHz, y se puede obtener una calidad razonable con muestreos de diez bits, para una velocidad de datos de 92 Mb/seg.

Otro tipo de modulación, menos usada, es la *Delta*

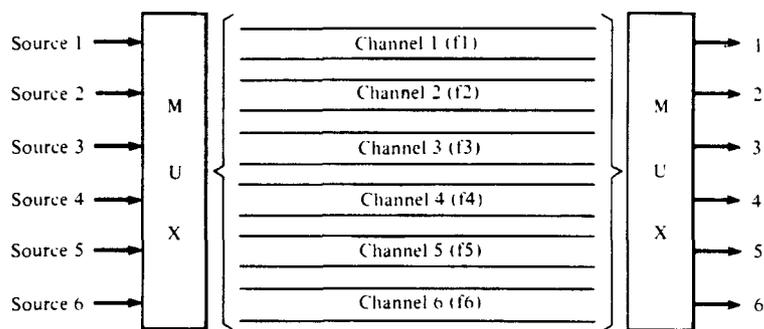
Modulación (DM). En ésta, se produce una cadena de bits al aproximar la derivada de una señal analógica, en vez de su amplitud. Se produce un 1 si el muestreo de corriente es en amplitud mayor que el inmediatamente precedente, y un 0 de lo contrario. Para las mismas velocidades de datos, la DM es comparable a la PCM en calidad de señal. Pues mientras en PCM se necesitan 8.000 muestras por segundo, en DM se necesitan 56.000. No obstante los sistemas DM son más baratos y menos complejos que sus equivalentes en PCM.

Multiplexado:

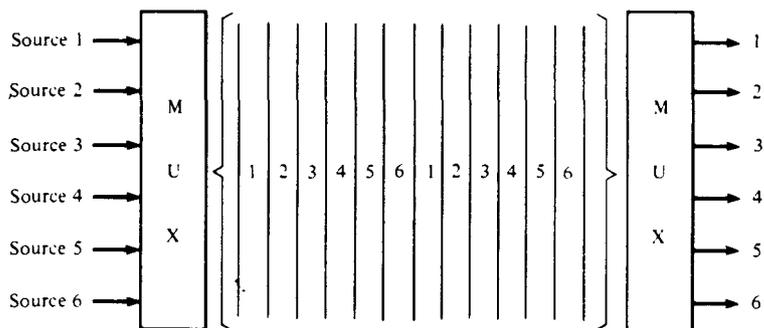
Tanto en las comunicaciones locales como en las de larga distancia, la capacidad del medio de transmisión excede las necesidades de la transmisión de una sola señal. Para hacer rentable el sistema se transmiten muchas señales simultáneamente por el mismo medio. A esto se le denomina Multiplexación, y hay dos técnicas en uso: *Frequency - Division Multiplexing (FDM)* y *Time - Division Multiplexing (TDM)*.

FDM parte de la base de que el ancho de banda útil del medio excede al ancho de banda de la señal a transmitir. Un buen número de señales pueden ser transportadas simultáneamente si cada señal es modulada a una frecuencia portadora diferente, y si estas frecuencias están separadas lo suficiente para que los anchos de banda de las señales no se solapen. Un ejemplo de FDM es la transmisión *Full-Duplex FSK* (figura 2.4). Un caso genérico

de FDM se muestra en la figura 2.7a. Seis señales son introducidas en un multiplexor, el cual modula cada señal en una frecuencia diferente (f_1, \dots, f_6).



(a) Frequency-Division Multiplexing



(b) Time-Division Multiplexing

FIGURE 2-7. Multiplexing

Cada señal necesita un cierto ancho de banda centrado en su frecuencia de portadora, al que llamaremos canal. Para evitar interferencias, los canales están separados por bandas de protección, que són porciones no usadas del espectro.

La TDM parte del hecho de que la velocidad de bits

del medio excede la velocidad de datos necesaria para una señal digital. Muchas señales digitales pueden ser transportadas en un solo medio de transmisión, mandado por intervalos en el tiempo, porciones de cada señal. Los intervalos pueden ser a nivel de bit, en bloques de bytes o en cuantías mayores. Por ejemplo, el multiplexor de la figura 2.7b tiene seis entradas de, digamos, 9.6 Kb/seg. Si la línea (media) tiene una capacidad de 57.6 Kb/seg, Puede acomodar a las seis señales. De manera similar a la FDM, la secuencia de pistas de tiempo dedicadas a cada fuente en particular se denominan canales. Y un ciclo completo de pistas de tiempo (una por fuente), se le llama "Frame" (Estructura, marco).

El diseño TDM de la figura 2.7b es conocido como TDM síncrono, pues sus canales están preasignados y fijados. Por tanto el tiempo de transmisión desde varias fuentes está sincronizado.

La TDM no se limita a las señales digitales, También pueden ser tratadas señales analógicas. Incluso, con señales analógicas, es posible una combinación de TDM y FDM. Un sistema de transmisión puede hacer una división en frecuencia, teniendo un número determinado de canales, y cada uno de ellos ser dividido vía TDM. Esta técnica es posible en redes locales de banda ancha.

Transmisiones síncronas y asíncronas:

Una necesidad fundamental de la comunicación digital

de datos, (con señales digital ó analógica) es que el receptor sepa el momento de comienzo y duración de cada bit que reciba.

El primer diseño y más sencillo que cumplía este requisito fué la transmisión asíncrona. En ella, los datos son transmitidos caracter (de 5 a 8 bits) a caracter, con un bit de comienzo (0) y uno ó dos bits de Stop (1) (figura 2.8a). Cuando no hay datos que enviar el emisor transmite un 1 continuo, es decir un bit de Stop continuamente. El receptor identifica la llegada de un nuevo caracter por la transición de 1 a 0. Además debe tener un conocimiento exacto de la duración de cada bit, para luego poder recuperar todos los bits del caracter. De todos modos, un pequeño error no es muy importante, ya que el receptor se vuelve a sincronizar con cada bit de Stop. Esto nos indica que se trata de una transmisión simple y barata, pero necesita 2 ó 3 bits de más por caracter. Esta técnica se denomina asíncrona, pues cada caracter es enviado independientemente de los demás y porque pueden ser enviados a una velocidad no uniforme.

Una modalidad más eficiente es la transmisión síncrona. En ella son transmitidos bloques de bits ó de caracteres sin bits de Stop ni de Start, donde el momento exacto de partida y de llegada de cada bits son conocidos (predecibles). Para prevenir errores entre el emisor y el receptor, sus relojes deben estar, de algún modo, sincronizados. Una posibilidad es proveer al sistema de

una línea separada e independiente de reloj entre el receptor y el emisor. De otra manera, la información de sincronismo debe ser incluida en la señal de datos. Para señales digitales, esto se consigue con una codificación bifásica. Para señales analógicas, pueden utilizarse varios métodos. Con la misma portadora se puede sincronizar el receptor basándonos en la fase de la misma.

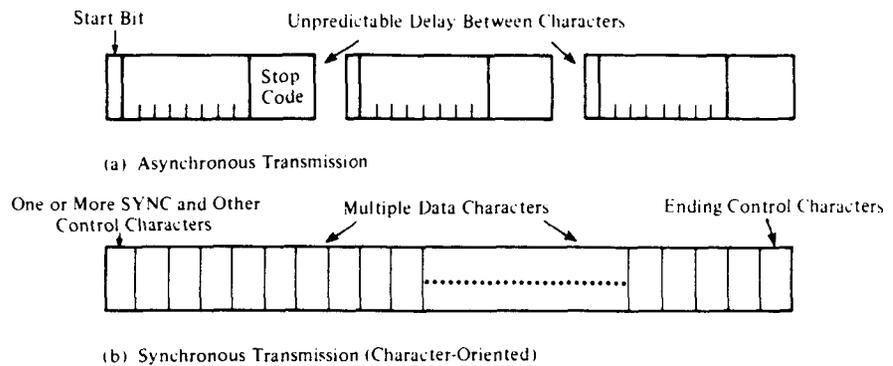


FIGURE 2-8. Asynchronous and Synchronous Transmission

En la transmisión asíncrona, es necesario también que el receptor sepa donde empieza y donde acaba cada bloque de datos. Para ello cada bloque lleva una serie de bits al comienzo y al final. La naturaleza de estos bits denominados globalmente *Frame*, viene dada por la naturaleza del bloque de datos.

Si se transmiten caracteres, cada bloque es precedido por uno ó más "caracteres de sincronización" (SYNC) (figura 2.8b). Este carácter de sincronización es elegido de tal manera que su patrón de bits será diferente a

cualquier caracter que se transmita regularmente. El caracter de sincronización del final de bloque es único. El receptor es, por tanto, advertido de la llegada de un bloque de datos por los caracteres SYNC y acepta datos hasta que recibe un caracter posterior, entonces el receptor queda a la espera del próximo SYNC.

2.2

TECNICAS DE CONMUTACION EN LA COMUNICACION.

Hasta ahora hemos hablado de como los datos pueden ser codificados y transmitidos a través de una unión de comunicaciones. En su forma más simple, la comunicación de datos tiene lugar entre dos dispositivos conectados directamente por algún medio de transmisión. Muy amenudo, no obstante, es imposible o poco práctico que dos dispositivos estén conectados directamente. Esto es debido a uno de los siguientes contingentes:

- * Los dispositivos están tan alejados uno del otro que sería excesivamente caro el tender una via de unión directa.
- * Hay un conjunto de dispositivos, cada uno de los cuales necesita comunicar con varios de los otros. Un ejemplo muy claro son los teléfonos de todo el mundo. Exceptuando algunos dispositivos, es imposible tender un cable entre

cada par de dispositivos.

La solución está en enganchar cada dispositivo a una red de comunicaciones. La comunicación es llevada a cabo transmitiendo los datos de origen a destino a través de nodos intermedios de la red. Estos nodos no tienen nada que ver con el contenido de los datos. Se limitan a proporcionar una capacidad de conmutación (Switching) que haga que la información se mueva de nodo a nodo hasta llegar a su destino.

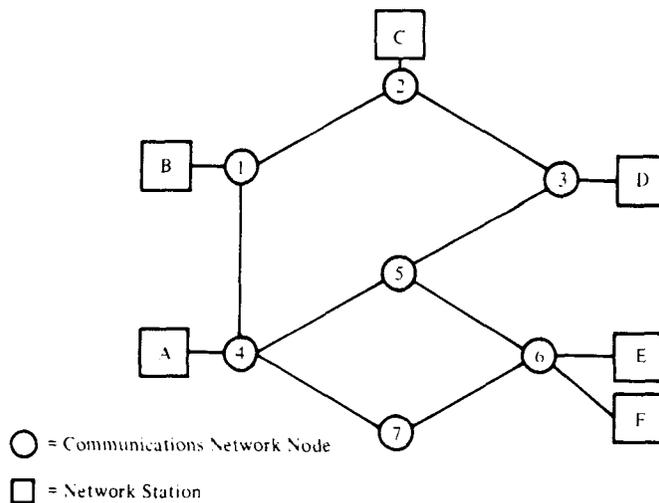


FIGURE 2-9. Generic Switching Network

La figura 2.9 ilustra la situación. Tenemos una serie de dispositivos que quieren comunicarse entre sí, a los que llamaremos estaciones (teléfonos, terminales, ordenadores,...). Y también tenemos unos dispositivos cuyo

cometido es facilitar la comunicación, a los que llamaremos nodos. Los nodos están conectados entre sí de alguna manera mediante un enlace de transmisión. Cada estación es conectada a un nodo. La colección de nodos es la red de comunicaciones. Si los dispositivos conectados son terminales y ordenadores, entonces la colección de nodos y estaciones se denomina red de ordenadores.

Hay tres técnicas de *Switching* (conmutación) de uso común:

- * **Circuit Switching.**
- * **Message Switching.**
- * **Packet Switching.**

Circuit Switching:

La comunicación vía *Circuit switching* (conmutación de circuitos), implica que existe un "camino de comunicación" asignado entre dos estaciones. Un "camino" es una secuencia de enlaces entre nodos. Se dedica un canal del medio físico para la conexión en cada enlace físico. El ejemplo más común de *Circuit Switching* es la red telefónica.

Este tipo de comunicación tiene tres fases, que pueden ser aplicadas tomando la figura 2.9 como referencia:

- 1.- Establecimiento del circuito: Antes de ser transmitidos los datos, ha de ser establecido un circuito de punto a punto. Por ejemplo, la

estación A hace una llamada al nodo 4 solicitando conexión con la estación E. Normalmente, el circuito de A a 4 es una línea fija y asignada. El nodo 4 debe encontrar la siguiente etapa que le dirija al nodo 6. Basándose en la información de encaminamiento (routing), de disponibilidad y de (a lo mejor) de coste, al nodo 4 selecciona el circuito al nodo 5. Asigna un canal libre (usando TDM ó FDM) en ese circuito y envía un mensaje pidiendo conexión a E. De este modo se ha establecido un camino desde A, a través de 4 a 5. El resto del proceso es similar. El nodo 5 asigna un canal al nodo 6 e internamente une éste con el canal que viene del nodo 4. El nodo 6 completa la conexión con E. Cuando la conexión ha sido terminada, se realiza un test para comprobar si E está ocupado ó si está listo para aceptar la conexión.

2.- Transferencia de datos: Las señales pueden ser ahora transmitidas a través de la red de A a E. Los datos pueden ser analógicos ó digitales, al igual que las señales. En cualquier caso el camino es:

- A - 4: circuito, conmutación interna a través de 4.
- 4 - 5: canal, conmutación interna a través de 5.

5 - 6: canal, conmutación interna a través de 6.

6 - E: circuito.

Generalmente la conexión es *Full-Duplex*.

3.- Desconexión: Después de un cierto tiempo de transferencia de información, la conexión se termina por la acción de una de las dos estaciones. Las señales pertinentes son propagadas al nodo 4, 5 y 6 para deshacer el camino creado.

Hay que ver que el camino de conexión es establecido antes de que la transmisión comience. Así que la capacidad del canal debe estar disponible y reservada entre cada par de nodos, y que cada nodo tiene que tener capacidad de conmutación interna para poder soportar la comunicación. Los interruptores (nodos) deben tener inteligencia para hacer estas selecciones y para idear un camino a través de la red. Una vez que el circuito es establecido la red es transparente. Los datos son transmitidos a la velocidad fijada sin más retardo que el producido por las líneas. El retardo que introduce cada nodo es despreciable.

Message Switching:

El *Circuit Switching* es una técnica fácil de usar y apropiada cuando se tiene un intercambio de datos continuo, como la voz (teléfono) y algunas señales telemétricas. Sin embargo tiene dos inconvenientes:

* Ambas estaciones deben estar disponibles al mismo tiempo para el intercambio de información.

* Los recursos deben estar disponibles y asignados a través de la red entre ambas estaciones.

Una solución válida para el intercambio de datos digitales, es el intercambio de unidades lógicas de datos, llamadas mensajes (messages). Esta es una técnica usada en los telegramas, correo electrónico, ficheros de ordenador, etc.

Con el **Message Switching** (conmutación de mensajes) no es necesario establecer un camino entre dos estaciones. Si una estación quiere enviar un mensaje, incluye una dirección de destino en el mismo. El mensaje es entonces pasado de nodo a nodo a través de la red. En cada nodo se recibe el mensaje entero, se almacena brevemente y es enviado al siguiente nodo.

En una red de circuitos conmutados, cada nodo es un dispositivo de conexión electrónico ó electromecánico que transmite bits tan pronto como los recibe. En una red de mensajes conmutados un nodo es un minicomputador de propósito general, con la suficiente capacidad de almacenamiento como para retener mensajes en cuanto llegan. El mensaje sufre en cada nodo el retardo suficiente para que lleguen todos los bits del mensaje, más un retardo adicional hasta tener vía libre para transmitirlo al siguiente nodo.

Otra vez, usando la figura 2.9, consideremos un mensaje de A a E, la estación A añade al mensaje la dirección de E y la envía al nodo 4. El nodo 4 almacena el mensaje y determina el próximo tramo de la ruta, (diagrama 5). El nodo 4 alinea el mensaje para ser transmitido en el enlace 4 - 5. Cuando dicho enlace está disponible, el mensaje es transmitido al nodo 5, el cual lo pasa al nodo 6 y finalmente éste a E. Este sistema es conocido como de "almacenamiento y envío" (Store and Forward). En algunos casos, el nodo al que se conecta la estación (ó algún nodo central), almacena el mensaje, creando una copia permanente.

A continuación se listan una serie de ventajas de la conmutación de mensajes frente a la conmutación de circuitos:

- * La eficiencia de la línea aumenta, pues con un sólo canal nodo a nodo podemos pasar muchos mensajes a lo largo del tiempo. Esto hace necesaria una menor capacidad para el mismo volumen de tráfico.
- * Podemos prescindir del envío y recepción simultánea, pues la red puede almacenar los mensajes en espera de la disponibilidad del receptor.
- * Cuando el tráfico es muy denso en un sistema de *Circuit Switching*, algunas llamadas se bloquean. En un *Message Switching* los mensajes

siguen siendo aceptados, sólo aumenta el retardo.

- * Un sistema de *Message Switching* puede enviar un sólo mensaje a varios destinos. Esto es de difícil consecución en el *Circuit Switching*.
- * Podemos establecer prioridades en los mensajes.
- * Una red de *Message switching* puede llevar a cabo conversiones de códigos y velocidades. Dos estaciones con diferentes velocidades de datos pueden conectarse sí, cada una es conectada a su nodo a su velocidad correspondiente. También puede convertir formatos (de ASCII a EBCDIC).
- * Los mensajes enviados a una estación no operativa pueden ser almacenados ó enviados de vuelta al origen (ó ambas cosas).

La desventaja principal de este tipo de conmutación es que no es ajustable a tráficos de tiempo real o interactivas, pues el retardo en la red es relativamente largo. Tampoco se puede usar para las conexiones de voz ni para conexiones interactivas entre un terminal y el ordenador central.

Packet Switching:

Esta técnica trata de combinar las ventajas de las dos anteriores, eliminando sus desventajas. Esto se consigue cuando hay un tráfico sustancial entre un buen número de estaciones.

La principal diferencia externa con el *Message Switching* es que la longitud de las unidades de datos que pueden ser transmitidas por una red de conmutación de paquetes es limitada. Típicamente de 1.000 a unos pocos de miles de bits. Los sistemas de conmutación de paquetes admiten unidades de datos mayores. Desde el punto de vista de la estación, un mensaje mayor que el límite ha de ser dividido en unidades menores y enviadas una a una. A estas unidades las llamaremos paquetes (packets).

Usando de nuevo la figura 2.9, vamos a suponer que transmitimos un sólo paquete de A a E. El paquete contiene datos y la dirección de destino. La estación A transmite el paquete a 4, el cual lo almacena brevemente y lo pasa a 5 quien lo pasa al 6 y de ahí a E. Una diferencia con el *Message Switching* es que aquí no se almacenan los paquetes. Pueden ser almacenados temporalmente con motivos de restaurar errores, pero eso es todo.

En principio, el *Packet Switching* puede parecer una manera extraña de proceder, sin ninguna ventaja sobre el *Message Switching*. Es más, el simple hecho de limitar el tamaño máximo de los datos a transmitir nos hace pensar en un dramático descenso del rendimiento. Antes de entrar en esto, vamos a definir dos modos de tratar mensajes completos a través de una red de *Packet Switching*.

El problema es éste. Una estación tiene un mensaje que enviar y éste es mayor que el tamaño máximo del paquete. Entonces divide el mensaje en paquetes y los

envía a su nodo. Pregunta: ¿Cómo manejará la red esta cadena de paquetes?. Hay dos soluciones: "Datagram", y "Virtual circuit".

En "Datagram" cada paquete se trata de manera independiente. Supongamos que la estación A tiene un mensaje de 3 paquetes que quiere enviar a E. La estación A envía uno a uno los tres paquetes al nodo 4. A la llegada de cada uno, el nodo 4 debe decidir por qué camino mandarlos. Llega el paquete 1 y el nodo 4 decide que el camino más oportuno y corto es enviarlo al nodo 5 en vez del 7, así que lo manda al 5. Lo mismo para el paquete 2. Pero para el paquete 3, el nodo 4 decide que es mejor el nodo 7 que el 5, luego lo manda al nodo 7. Tenemos entonces que todos los paquetes, todos con la misma dirección de destino, no han seguido la misma ruta. Es más, es posible que el paquete 3 llegue antes que el 2 al nodo 6, con lo que el mensaje podría llegar a la estación E en diferente orden. En ésta técnica, cada paquete (tratado independientemente) se denomina "Datagram".

En "Virtual Circuit", se establece una conexión lógica antes de que sean enviados los paquetes. Por ejemplo, supongamos que A tiene uno ó más mensajes que enviar a E. La estación A manda primero una petición de llamada (Call Request) en un paquete, al nodo 4, pidiendo conexión con E. El nodo 4 decide encaminar la petición (y por consiguiente los demás datos) hacia el nodo 5, el cual lo encamina a 6 y éste finalmente a E. Si E está preparado

para aceptar la comunicación, envía un paquete de aceptación de llamada (Call Acept) al nodo 6. Este paquete es pasado por nodos 5 y 4 hasta llegar a A. Ambas estaciones pueden ahora intercambiar datos a través de la conexión lógica o circuito virtual que se ha establecido. Cada paquete ahora tiene, además de datos, un identificador de circuito virtual. Cada nodo de la ruta establecida sabe donde dirigir estos paquetes; no es necesario la toma de decisiones. Cualquiera de las estaciones puede terminar la conexión con un paquete de petición de final (Clear Request). En cualquier momento, cada estación puede tener más de un circuito virtual con cualquier otra estación y puede tener circuitos virtuales con más de una estación.

La característica principal de esta técnica es pues, que la ruta entre dos estaciones se establece prioritariamente frente a la transferencia de datos. Esto no significa que se establezca un camino asignado como sucedía en el *Circuit Switching*. Un paquete es almacenado (Buffered) en cada nodo. La diferencia con la técnica de "datagram" es que en ella el nodo debe hacer una decisión de encadenamiento para cada paquete. En cambio, en el circuito virtual esto se hace sólo una vez cada conexión.

Esta técnica es muy ventajosa en el caso de que las estaciones deseen intercambiar datos durante un periodo de tiempo prolongado. En *Virtual Circuit* se pueden obtener un buen número de servicios, incluyendo secuenciamiento,

control de error y control de flujo. El secuenciamiento se refiere al hecho de que al seguir todos los paquetes la misma ruta, lleguen en el mismo orden. Control de error es un servicio que asegura no sólo que los paquetes lleguen ordenadamente, sino que lleguen correctamente. Por ejemplo, si un paquete de la secuencia no llega al nodo 6, ó llega con un error, él puede pedir que se vuelva a retransmitir ese paquete desde el nodo 4. Por último, el control de flujo es una técnica que asegura que el emisor no inunde de datos al receptor. Es decir; si la estación E almacena datos de A y prevee que se va a quedar sin espacio, hace una petición (via virtual circuit) a A de suspensión de la transmisión hasta nuevo aviso.

La técnica de *Datagram* es más flexible pues es más primitiva. Es por ello que es utilizada en las conexiones entre redes. Otra ventaja es que si un nodo falla, los paquetes encuentran siempre una ruta alternativa. En cambio en *Virtual Circuit*, si un nodo falla, todos los circuitos virtuales que pasen por él se pierden.

Volviendo a la cuestión del rendimiento, la figura 2.10 nos ilustra los diferentes rendimientos de estas técnicas. No obstante hay que tener en cuenta un buen número de factores, incluyendo:

- * El número de estaciones.
- * El número y disposición de los nodos.
- * La carga total del sistema.
- * La duración (en tiempo y datos) de un intercambio

típico entre dos estaciones.

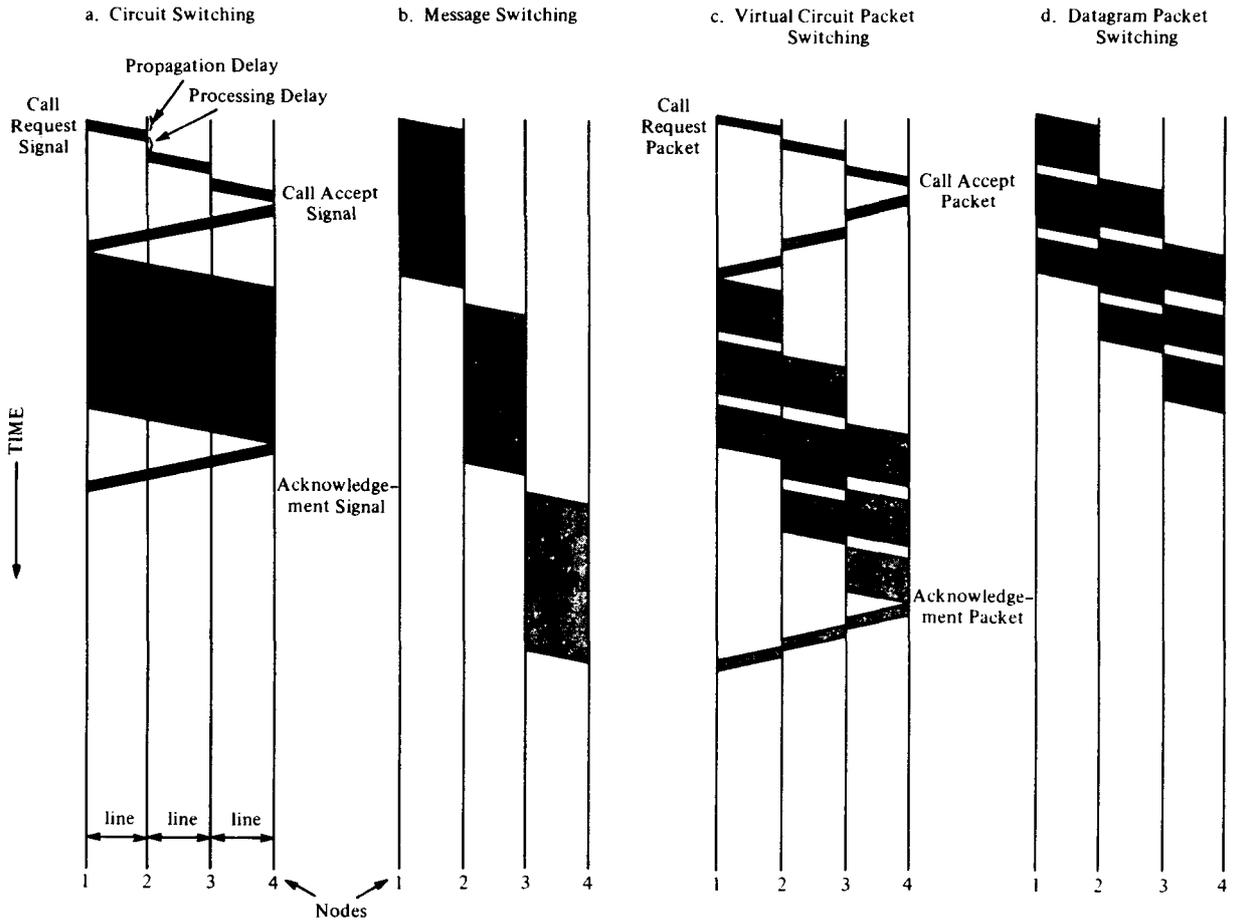


FIGURE 2-10. Event Timing for Various Communication Switching Techniques

Dada la dificultad que entraña la comparación de

estos métodos, hay que hacer unas observaciones importantes:

- * El *Message Switching* no es apropiado para tráfico interactivo.
- * Para cargas considerables entre dos estaciones, el alquiler de una línea de *Circuit Switching* es lo más rentable y efectivo.
- * El *Packet Switching* es la mejor elección cuando se tiene un conjunto de dispositivos que deben intercambiar un montante de moderado a alto de información; la utilización de la línea es más eficiente con esta línea.
- * El *Datagram Packet Switching* es bueno para mensajes cortos y para disponer de flexibilidad.
- * En cambio el *Virtual Circuit Packet Switching* es bueno para intercambios largos y para aliviar a las estaciones de la carga del procesamiento.

La tabla 2.2 resume las características principales de las cuatro técnicas que hemos visto.

Como punto final, vamos a mencionar una forma de hacer rentables las redes de *Packet Switching*, esto es, utilizando un sistema público de conexiones. En EE.UU. hay dos claros exponentes de este tipo de redes, son **TELENET** y **TYMNET**. La red consiste en nodos, propiedad del proveedor de los servicios de la red, unidos por canales alquilados a un transportista común como **AT&T**. Los abonados pagan una cuota por ser conectados a la red y por transmitir

paquetes a través de ella.

TABLE 2.2 Comparison of Communication Switching Techniques

Circuit Switching	Message Switching	Datagram Packet Switching	Virtual Circuit Packet Switching
Dedicated transmission path	No dedicated path	No dedicated path	No dedicated path
Continuous transmission of data	Transmission of messages	Transmission of packets	Transmission of packets
Fast enough for interactive	Too slow for interactive	Fast enough for interactive	Fast enough for interactive
Messages are not stored	Messages are filed for later retrieval	Packets may be stored until delivered	Packets stored until delivered
Path is established for entire conversation	Route established for each message	Route established for each packet	Route established for entire conversation
Call setup delay; negligible transmission delay	Message transmission delay	Packet transmission delay	Call setup delay; packet transmission delay
Busy signal if called party busy	No busy signal	Sender may be notified if packet not delivered	Sender notified of connection denial
Overload may block call setup; no delay for established calls	Overload increases message delay	Overload increases packet delay	Overload may block call setup; increases packet delay
Electromechanical or computerized switching nodes	Message switch center with filing facility	Small switching nodes	Small switching nodes
User responsible for message-loss protection	Network responsible for messages	Network may be responsible for individual packets	Network may be responsible for packet sequences
Usually no speed or code conversion	Speed and code conversion	Speed and code conversion	Speed and code conversion
Fixed bandwidth transmission	Dynamic use of bandwidth	Dynamic use of bandwidth	Dynamic use of bandwidth
No overhead bits after call setup	Overhead bits in each message	Overhead bits in each packet	Overhead bits in each packet

Como el tráfico de un abonado no es lo suficientemente

grande como para que la red resulte rentable, se recurre a este sistema. El volumen de todos los suscritos si proporcionan su rentabilidad. Estas redes son conocidas como redes de valor añadido (VANs).

Tecnicas de conmutación para redes locales:

La *Circuit Switching* es una técnica ampliamente usada en las redes locales. Los tipos de red que usan esta técnica son las de conmutador digital y las *Digital Private Branch Exchange* (PBX). Estas redes las trataremos en capítulos posteriores.

El *Packet Switching* es también usado en las redes locales. En muchos casos, no obstante hay un sólo camino (directo) de la fuente al destino. Por tanto, a menudo no hay funciones de encaminamiento (Routing) ó de conmutación (Switching). Se usa tanto el *Packet Switching* como el *Message Switching* para que ninguna fuente monopolice el medio.

2.3

REDES DE ORDENADORES. Arquitectura de comunicaciones.

Motivación:

Cuando un trabajo implica el utilizar más de un ordenador, se necesitan unos elementos adicionales: el Hardware y el Software para soportar la comunicación entre

los mismos. El Hardware de comunicación es razonablemente estandar y presenta, generalmente, pocos problemas. Sin embargo, cuando la comunicación se realiza entre dispositivos heterogéneos (diferentes fabricantes, ó diferentes modelos del mismo fabricante), el Software puede llegar a ser muy complejo. Cada fabricante utiliza diferentes formatos de datos y reglas para el intercambio de los mismos. Incluso si se trata de dos modelos diferentes del mismo fabricante, las diferencias pueden ser muy importantes.

El crear Software para cada una de las combinaciones entre equipos diferentes es obviamente inviable. Los fabricantes deben pues adoptar una serie de convenios. Esto deben realizarlo las organizaciones internacionales ó nacionales adecuadas. Este tipo de estandar tiene dos efectos:

- * Los fabricantes se ven forzados a implementar los standards ya que si no lo hacen, sus productos tendrían mucho menos mercado.
- * Los compradores desean que todos los fabricantes se acojan a estas reglas, para tener una gama completa y variada de marcas.

Está claro que una sólo "norma" puede prevalecer. La tarea de la comunicación de una manera realmente cooperativa entre aplicaciones en diferentes ordenadores, es demasiado compleja como para ser tratada como una unidad. El problema debe ser dividido en partes

manejables. Por lo tanto, antes de que alguien proponga un estandar, debe haber una "arquitectura" que defina las tareas de comunicación.

Esta línea de pensamiento fué la que hizo que la Organización Internacional de Estandarización (ISO), creará un subcomité encargado de desarrollar dicha arquitectura. El resultado fue el *Open System* Internacional (OSI), el cual representa un buen marco de trabajo para definir uniones entre ordenadores heterogéneos. El OSI proporciona las bases para conectar sistemas "abiertos" para el proceso de aplicaciones distribuidas. El término "abierto (Open) denota la viabilidad de la conexión entre dos sistemas conformes o similares al modo de referencia y a los estandars asociados.

Una de las técnicas de estructuración más extendida y la primera elegida por la OSI es el "Layering" (estratificación). Las funciones son divididas en un conjunto jerárquico de capas (Layers). Cada capa realiza un subconjunto de funciones requeridas para la comunicación con otro sistema. Estos recurren a la capa inferior para obtener funciones más primarias. Ello proporciona servicios a la capa inmediatamente superior. Idealmente, el concepto de "capa" se define de manera que los cambios en una no requiere cambios en las otras. De esta manera hemos descompuesto el problema en subproblemas más manejables.

La teoría OSI fué definir un juego de capas y los servicios que realizaban cada una de ellas. La partición debia ser por agrupación de funciones lógicamente, con el suficiente número de capas para que resulten manejables cada una de ellas, pero sin tener tantas capas que el montante de procesamiento se vuelva agobiador. El resultado fué el modelo de referencia OSI de 7 capas, las cuales están listadas, junto a una corta definición de cada una en la tabla 2.3.

TABLE 2.3 The OSI Layers

Layer	Definition
1. Physical	Concerned with transmission of unstructured bit stream over physical link; involves such parameters as signal voltage swing and bit duration; deals with the mechanical, electrical, and procedural characteristics to establish, maintain, and deactivate the physical link (RS-232-C, RS-449, X.21)
2. Data link	Provides for the reliable transfer of data across the physical link; sends blocks of data (frames) with the necessary synchronization, error control, and flow control (HDLC, SDLC, BiSync)
3. Network	Provides upper layers with independence from the data transmission and switching technologies used to connect systems; responsible for establishing, maintaining, and terminating connections (X.25, layer 3)
4. Transport	Provides reliable, transparent transfer of data between end points; provides end-to-end error recovery and flow control
5. Session	Provides the control structure for communication between applications; establishes, manages, and terminates connections (sessions) between cooperating applications
6. Presentation	Performs generally useful transformations on data to provide a standardized application interface and to provide common communications services; examples: encryption, text compression, reformatting
7. Application	Provides services to the users of the OSI environment; examples: transaction server, file transfer protocol, network management

La tabla 2.3 define, en términos generales, las

funciones que deben ser realizadas en un sistema para que se comunique. Por supuesto que como son necesarios dos sistemas para comunicar, este juego de funciones por capas debe estar en ambos. La comunicación se logra teniendo comunicadas las correspondientes capas (por partes) en ambos sistemas. Los pares de capas se comunican por medio de una serie de reglas ó convenios llamado "protocolo". Los elementos clave de un protocolo son:

- * Sintaxis: Incluye cosas como el formato de los datos y los niveles de señal.
- * Semántica: Incluye información de control para la coordinación y el tratamiento de errores.
- * Timing: Incluye el ajuste de velocidad y el secuenciamiento.

La figura 2.11a muestra el modelo OSI. Cada sistema contiene las 7 capas. La comunicación es entre aplicaciones en los sistemas marcados como APX y APY en la figura. Si APX desea mandar un mensaje a APY, éste invoca la capa de aplicación (capa 7). La capa 7 establece una relación de pareja con la capa 7 de la otra máquina, usando un protocolo de capa 7. Este protocolo requiere servicios de la capa 6, así que las dos capas 6 se unen mediante un protocolo propio, así hasta la capa física, en la cual se transmiten los bits por un determinado medio de transmisión.

Observar que no hay comunicación directa entre pares de capas a excepción de las capas físicas (unidas por un

"medio" físico).

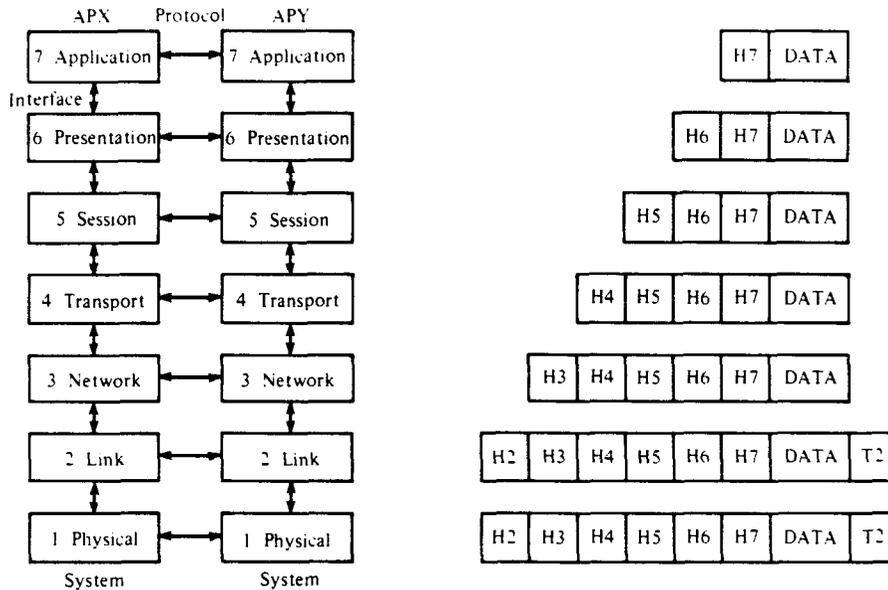


FIGURE 2-11. The OSI Model: Connection and Encapsulation

El atractivo del diseño OSI es que promete solventar el problema de comunicación entre ordenadores heterogéneos. Dos sistemas, no importa lo diferentes que sean, pueden comunicarse de manera efectiva, si tienen los siguientes puntos en común:

- * Ambos implementan el mismo juego de funciones de comunicación.
- * Dichas funciones estén organizadas en el mismo conjunto de capas. Las parejas de capas deben proporcionar las mismas funciones, pero no tienen que proporcionarlas de la misma manera.
- * Las capas de una pareja deben compartir un

protocolo común.

Necesitamos los estandars para asegurar ésto. Los estandards deben definir las funciones y servicios que debe facilitar cada capa (pero no como deben llevarse a cabo, puede diferir de sistema a sistema). Deben tambien definir los protocolos entre parejas de capas (cada protocolo debe ser idéntico para cada pareja de capas). El Modelo OSI, proporciona un marco de trabajo para definir estos estandars, al crear la arquitectura de 7 capas.

Una de las terminologías útiles de OSI es mostrada en la figura 2.12. Para mayor simplicidad, nos referimos a cualquier capa con la capa (N). Dentro de un sistema, hay una ó varias "entidades" activas en cada capa. La entidad (N) implementa funciones de la capa (N) y tambien el protocolo para comunicarse con entidades (N) de otros sistemas. Un ejemplo de "entidad" es un proceso en un sistema multiproceso. O bien puede ser simplemente una subrutina. Cada entidad se comunica con entidades de las capas inferior y superior a través de interface. El interface es realizado por uno ó más puntos de acceso a servicio (SAPs). Finalmente, para establecer una comunicación entre entidades (N), se define un punto de conexión final (CEP) para cada entidad (N), dentro de los SAPs.

Para clarificar estos términos tan bien como algunas funciones comunes a todas las capas, nos referimos de nuevo a la figura 2.11. Las funciones a tratar son:

- * Encapsulado.
- * Fragmentación.
- * Establecimiento de conexión.
- * Control de flujo.
- * Control de error.
- * Multiplexado.

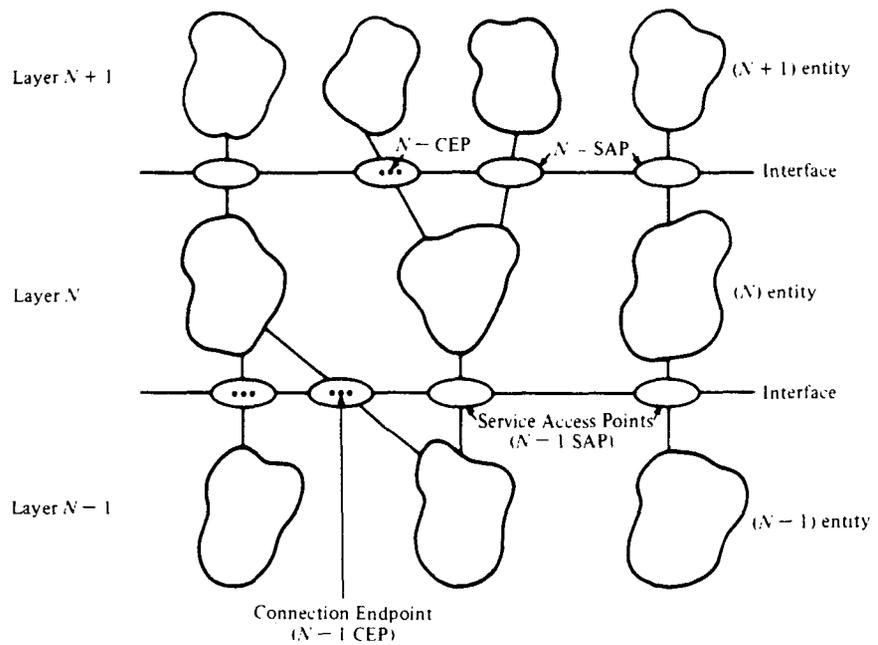


FIGURE 2-12. The OSI Model: The Layer Concept

Primero hay que ver el modo más corriente de realizar los protocolos, esto es, por el proceso de "encapsulado" (figura 2.11b). Cuando APX tiene un mensaje de APY, él transfiere esos datos a una entidad de la capa de aplicaciones. Se le añade un encabezamiento (Header) que contiene la información requerida por el protocolo de la

pareja de capas número siete; a esto se le denomina "encapsulado de datos". Los datos originales más el encabezado son ahora pasados como una unidad a la capa 6. La entidad en la capa 6 trata toda la unidad como datos, y le añade su propio encabezamiento (un segundo capsulado). Este proceso se repite hasta la capa 2, la cual, usualmente añade un encabezamiento y una coletilla. La unidad que resulta (en este nivel) se denomina *Frame* (cuerpo). Este *Frame* es transmitido por la capa física al medio de transmisión. Cuando el *Frame* es recibido por el sistema de destino, se produce el mismo proceso a la inversa. A medida que los datos ascienden, cada capa elimina el encabezamiento más exterior, actúa sobre la información de protocolo contenida en él, y pasa el resto a la capa inmediatamente superior.

En cada nivel de proceso, una capa puede fragmentar la unidad de datos que recibe de la capa superior en varias partes. Estas nuevas unidades de datos deben ser ensambladas de nuevo por la capa que hace pareja con ella, antes de pasar la información.

Cuando dos entidades (parejas) tienen que intercambiar datos, puede hacerse con o sin conexión previa. En cada capa de la jerarquía pueden existir conexiones. De manera abstracta, una conexión entre dos entidades (N) se establece identificando para cada entidad (N) un punto de conexión final (CEP ($N-1$)), dentro de un SAP ($N-1$). Una conexión facilita la posibilidad de

controlar los errores y el flujo. El control de flujo es una función realizada por una entidad (N) para limitar la cantidad ó velocidad de datos que recibe la otra entidad (N). Esta función es muy útil para evitar el desbordamiento (Overflow) de la entidad (N) que recibe los datos. El control de errores se refiere a mecanismos de detección y corrección de errores surgidos en la transmisión de unidades de datos entre parejas de entidades.

El multiplexado puede darse en dos direcciones. Si es ascendente, significa que muchas conexiones (N) son multiplexadas sobre, ó comparten, una sola conexión (N-1). En el descendente (ó Splitting), tenemos una sóla conexión (N) se construye en la cima de muchas conexiones (N-1), el tráfico en la conexión (N) se divide entre las varias conexiones (N-1).

Aunque esta parte pueda parecer abstracta en demasía no hay más remedio que tratarla así. En capítulos posteriores y con el estudio de protocolos concretos, estos conceptos quedarán claros.

Protocolos:

En esta sección veremos brevemente cada una de las 7 capas y, si procede, expondremos ejemplos de protocolos standards más importantes. Recordar que el modelo de capas de OSI no es standard; solamente procura un marco de trabajo para la realización de standards.

La CCITT (Comité Consultivo Internacional de Telegrafía y telefonía) ha desarrollado standards para la conexión de "equipos terminales de datos" (DTE) a una red de *Packet/Switching* que proporciona "equipo de circuito terminal de datos" (DCE ó DCTE). Estos términos corresponden a las estaciones y nodos de la figura 2.9.

El standard X25 corresponde al standard de CCITT para la capa 3. La capa 2 se denomina LAP-B (Link Acces Protocol/Balanced) y es practicamente idéntica a la HDLC (High-Level Data Link Control) de ISO y a la ADCCP (Advanced Data Communication Control Procedure) de ANSI.

ISO ha desarrollado standards para las capas 4 y 5, y en el proceso de elaboración, tambien han sacado varios para cubrir las capas 6 y 7. ISO tambien ha creado una subcapa de la capa 3 destinada al "Internetworking", es decir, a la comunicación a través de muchas redes.

Un protocolo de *Internetworking* ha sido desarrollado por el departamento de defensa (DOD) para sus propias necesidad, además de un protocolo de control de la transmisión (TCP). El TCP asume todas las funciones de la capa 4 más algunas de la 5.

Para el tipo de red local que definiremos como red de área local (LAN), el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), a través de su comité 802, ha creado una arquitectura de 3 capas que corresponden a las capas 1 y 2 del modelo OSI. De modo similar, un subcomite del Instituto Americano de Standards Nacionales (ANSI),

conocido como **ANS X3T9.5** ha creado una serie de standards para lo que tambien definiremos mas adelante como redes locales de alta velocidad (HSLN). Estos standards (uno por capa) corresponden exáctamente a las capas 1 y 2 del modelo OSI.

TABLE 2.4 Some Well-Known Layers

OSI	CCITT	ISO	DOD	IEEE 802	ANS X3T9.5
7. Application		Various	Various		
6. Presentation					
5. Session		Session			
4. Transport		Transport (TP)	TCP		
3. Network	X.25	Internet Sublayer	IP		
2. Link	LAP-B			Logical link control	Data link
1. Physical	X.21			Medium access control	Physical
				Physical	

Tal cantidad de standards puede hacer pensar la viabilidad de este sistema.

De todos modos, el panorama no es tan desolador como parece al mirar la tabla 2.4. Con la excepción de las redes locales, que deben ser tratadas por separado, los standards se ajustan muy bien a las capas de la 1 a la 3.

Por encima de éstas, hay una considerable cooperación entre los diferentes grupos, de tal manera que en muchos casos es posible hablar de uniformidad (ó casi).

Capa física:

La capa física cubre el interfase físico entre los dispositivos y las reglas por los cuales los bits son pasados de uno a otro. La capa física tiene cuatro características importantes:

- * Mecánicas.
- * Eléctricas.
- * Funcionales.
- * De procedimiento.

El standard más comúnmente usado hoy en día es la RS-232-C. Un uso típico de la RS-232-C es conectar un dispositivo digital a un modem, él cual se conecta a una línea telefónica. Nos referiremos a este standard cuando describamos las 4 características antes mencionadas.

Las características mecánicas se refieren al punto de demarcación. Por lo general éste es un conector enchufable. La RS-232-C especifica un conector de 25 pines, de tal manera que 25 cables independientes nos sirven para conectar dos dispositivos.

Las características eléctricas tienen que ver con los niveles del voltaje. Estas características determinan las velocidades y distancias a las cuales se pueden transmitir los datos.

Las características funcionales especifican las funciones que se realizan, dándole significado a varias señales. Para la RS-232-C, y para la mayoría de los standards de capa física, ésto se logra especificando las funciones de cada pin del conector.

Las características de procedimiento especifican la secuencia de acontecimientos para transmitir datos, basados en las características funcionales. Para la RS-232-C, la utilidad de varios pines está definida.

Capa de enlace de datos:

La capa física sólo proporciona una mera cadena de bits. La capa de enlace de datos (Data Link Layer) intenta hacer fiable el enlace físico y proporciona el significado a activar, mantener y desactivar el enlace. Un ejemplo de ésto son las técnicas de transmisión síncrona y asíncrona.

Ahora vamos a definir el HDLC, que es un protocolo de bit orientado síncrono. Lo haremos por dos razones:

- * El HDLC es el precursor del protocolo estandard de la capa de enlace de datos en las redes de área local (IEEE 802).
- * Muchos de los conceptos relativos a los protocolos se explican bien con él.

El HDLC, y los protocolos síncronos de bits orientados en general, intentan proporcionar las siguientes capacidades:

- * Transparencia (operación independiente del

código): El protocolo y los datos que él transporta son independientes.

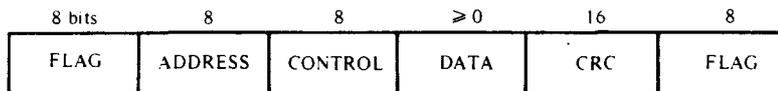
- * Adaptabilidad a varias aplicaciones, configuraciones, y darle uso de una manera consistente: Por ejemplo, punto a punto, *Multidrop* y *Loop* son configuraciones que podrían ser soportadas.
- * transferencias tanto alternado de dos caminos y simultáneo de dos caminos (Full-Duplex).
- * Alta eficiencia: El protocolo debería tener un mínimo de bits de más. Incluso debería funcionar eficientemente en líneas con grandes retardos en la propagación y en enlaces con grandes velocidades de transmisión.
- * Alta fiabilidad: Los datos no se deben perder, duplicar ó alterar.

Con estos conceptos en mente, volveremos a la definición de HDLC.

Tenemos tres modos de operación: El modo de respuesta normal (NRM), el modo de respuesta asíncrono (ARM) y el modo asíncrono balanceado (ABM). Los dos primeros pueden ser usados en configuraciones punto a punto ó multipunto. Para ambos hay una "estación primaria" y una ó más secundarias. La estación primaria es responsable de inicializar el enlace, controlar el flujo de datos desde y hacia las estaciones secundarias, de la recuperación de errores y de la desconexión lógica de las estaciones

secundarias. En **NRM**, una estación secundaria sólo puede transmitir como respuesta a una llamada (Poll) desde la estación primaria; en **ARM**, una estación secundaria puede iniciar una transmisión sin ninguna llamada. **NRM** es ideal para una línea "Multidrop", consistente en un ordenador central (Host) y un determinado número de terminales. **ARM** es apropiado para ciertas clases de configuraciones tipo *Loop* (circuito cerrado).

Frame Structure:



Control Field Structure

	1	2	3	4	5	6	7	8
Information	0	SEQ			P/F	NEXT		
Supervisory	1	0	TYPE		P/F	NEXT		
Unnumbered	1	1	TYPE		P/F	MODIFIER		

FIGURE 2-13. The HDLC Frame Structure

ABM se usa sólo en enlaces punto a punto en donde cada estación asume el papel tanto de primaria como de secundaria. Este modo es mas eficiente, pues no se necesitan llamadas (Polling) (encuestas) y cada estación puede iniciar una transmisión.

Los datos son transmitidos en Frames o formatos de seis campos (figura 2.13).

- * **Flag:** se utiliza para la sincronización. Este campo indica el comienzo y término de un campo

de datos. La patente de bits de los *Flags* es 01111110.

- * **Address:** En él se indica la estación de destino.
- * **Control:** En este campo se especifica la función y el propósito del cuerpo de datos a transmitir. Lo veremos con más detalle luego.
- * **Data:** Contiene los datos para transmitir.
- * **CRC:** Es un campo secuencial de revisión del campo de datos. Utiliza *Checkin* (ciclo) redundante de 16 bits. El campo CRC está en función de los campos de control, dirección y de datos. Es generado por el origen (de la transmisión) y después es generado de nuevo por el destino. Si este último es diferente al CRC, se ha producido un error de transmisión.

Hay tres tipos "Frames de datos", cada uno con un formato diferente del campo de control.

Cada campo de control se compone a su vez de 8 bits:

- * **Information:** Llevan los datos.
- * **Supervisory:** Proporcionan funciones básicas de control de los enlaces.
- * **Unnumbered:** Proporciona funciones de control de enlaces suplementarios.

Analizando en concreto la estructura de cada uno de ellos (figura 2.13), podemos decir que el bit P/F (Poll/final) se usa en los tres casos, por la estación primaria, para solicitar respuesta. como es posible que se

manden varios cuerpos de respuestas, el bit P/F indica tambien el último de ellos. En las estructuras "supervisory" y "Unnumbered", el bit P/F puede ser utilizado para formar una respuesta. Los campos SEQ y NEXT en la estructura "Information" proporciona una técnica eficiente para el control de flujo y de errores. Una estación enumera los *Frames* que envia secuencialmente en un módulo 8, usando el campo SEQ. Cuando una estación recibe un *Frame* de "Information" válido, reconoce la llegada de éste, mandando otro *Frame* de "Information" con el número del próximo cuerpo que espera recibir en el campo NEXT. Esto es conocido como "Piggybacked Acknowledgment", pues el reconocimiento (confirmación) de llegada (ACK) se manda en un *Frame* de "Information". Las confirmaciones tambien pueden ser desviadas en un *Frame* del tipo "Supervisory". Este esquema implica tres importantes funciones.

- * Control de flujo: una vez una estación ha enviado 7 cuerpos, no puede enviar un octavo, hasta que no reciba la aceptación del primero de ellos.
- * Control de error: si un *Frame* es recibido con error, una estación puede enviar "NAK" (Negative Acknowledgement) a través de un cuerpo "Supervisory", para especificar que se ha recibido un *Frame* erroneamente. Esto se lleva a cabo de dos maneras. En el "Go Back n Protocol",

la estación emisora retransmite el *Frame NAK* y todos los *Frames* que le seguían y hayan sido enviados. En el "Selective Repeat Technique" (técnica de repetición selectiva), la estación emisora retransmite sólo el cuerpo con error.

* **Pipelining:** Más de un cuerpo pueden estar en tránsito al mismo tiempo, esto permite un aprovechamiento mejor de las líneas con un gran retardo de propagación como los enlace vía satélite.

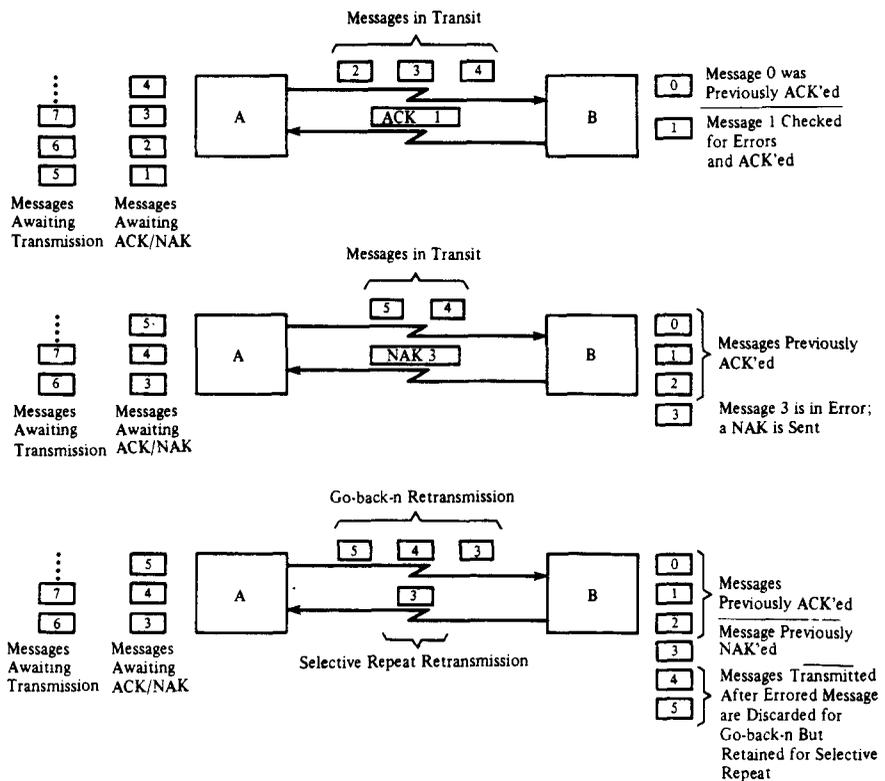


FIGURE 2-14. The Sliding-Window Technique

La técnica SEQ/NEXT es conocida como "Sliding-Window

Protocol", ya que la estación emisora mantiene una ventana de mensajes por enviar que gradualmente abanzan con la transmisión y las confirmaciones (ACK). El proceso se plasma en la figura 2.14.

Hay cuatro tipos de *Frames* supervisores:

- * **Receive Ready (RR)**: Usado para confirmar la correcta recepción de *Frames* por encima del **NEXT-1**. Alternativamente, es un comando de llamada (Poll) para decir a la estación secundaria que comience la transmisión con la secuencia **NEXT**.
- * **Receive Not Ready (RNR)**: Usada para indicar una condición temporal de ocupado.
- * **Reject (REJ)**: Se usa para indicar un error en el *Frame NEXT* y solicitar la retransmisión del mismo y de todos los que le siguen.
- * **Selective Reject (SREJ)**: Usado para solicitar la repetición de un sólo *Frame*.

Los *Frames* "Unnumbered" no tienen número de secuencia y son usados para un buen número de propósitos, como inicializar una estación, fijar un modo, desconectar una estación, y para rechazar (REJECT) un comando.

Capa de red:

Esta capa está diseñada para facilitar la comunicación de dos dispositivos a través de una red de comunicaciones. Es en este nivel donde el concepto de

protocolo se vuelve más borroso. La figura 2.15 ilustra 2 sistemas (DTEs) que están comunicándose, no vía enlace directo sino a través de una red. Los DTEs tienen enlaces directos a los nodos de la red (DCEs). Los protocolos de las capas 1 y 2 son protocolos DTE - DCE (locales). Los protocolos de las capas 4 - 7 son claramente protocolos entre entidades (N) en los dos DTEs. La capa 3 tiene un poco de ambos.

Para la especificación X.25, la capa 3 ha sido diseñada tanto para "Datagram" como para "Virtual Circuit". El diálogo principal es entre el DTE y su DCE, el DTE manda paquetes con dirección al DCE para que éste se ocupe de su gestión a través de la red. El también puede pedir una conexión de circuito virtual, usar la conexión para transmitir datos, y terminar la conexión. El DCE atiende el diálogo del DTE y a la vez atiende la gestión de la red; encaminamiento, establecimiento de circuitos virtuales, y entrega de paquetes. La X.25 se autodefine como un interface entre DTE y un DCE. En la terminología que hemos estado usando ahora se trata de un protocolo entre el DTE y el DCE. No obstante, como los paquetes son intercambiados entre dos DTEs, hay aspectos de protocolo para DTE - DTE.

A pesar de ello, la capa 3 de la X.25 es un protocolo con significado básicamente local (DTE - DCE). Esta no garantiza la fiabilidad y control en una comunicación entre puntos finales (END - TO -END) (DTE - DTE) por

supuesto, es posible proveer a la capa 3 con un protocolo con esta significación.

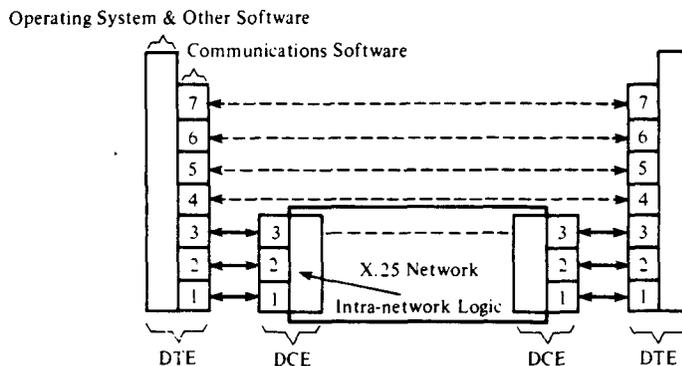


FIGURE 2-15. Communication Across a Network

El servicio básico de la capa de red, es dar una transferencia de datos transparente entre dos entidades de transporte. Esto evita a la capa de transporte la necesidad de saberlo todo sobre el medio de comunicación utilizado. En un extremo, cuando hay un enlace directo entre dos estaciones, no hay necesidad de una capa de red. Entre extremos, el uso más común que se le dá a la capa 3, es manejar los detalles de usar una red de comunicación de paquetes. En el otro extremo, dos dispositivos pueden querer comunicarse aunque no estén unidos a la misma red, pero están conectados a redes que, directa o indirectamente, están conectadas entre sí. Aunque éste caso lo veremos con más detalle en un capítulo posterior, podemos decir que para conseguir una transferencia de datos correcta en esta situación, debemos utilizar un

"Internet Protocol" (IP), el cual se sitúa por encima de un protocolo de red y es usado por un protocolo de transporte. IP es responsable del encaminamiento y fiabilidad del conexasión entre redes (Internet Working), y se apoya en las capas 3 de cada red para obtener servicios internos de cada red. Este protocolo es llamado también "capa 3.5".

Capa de transporte:

A partir de la capa 4, hay que hablar ya de "capas superiores". En estos niveles los protocolos son entre puntos finales (End-To-End) y no tienen nada que ver con las facilidades de comunicación de niveles inferiores.

El propósito de la capa 4 es proporcionar un mecanismo fiable de intercambio de datos entre procesos (procedimientos) en diferentes sistemas. La capa de transporte asegura que las unidades de datos están libres de errores, en su secuencia (orden) adecuada, sin pérdidas ni duplicaciones. Las características típicas de esta capa son:

- * Tipo de servicios: Tenemos conexión orientada ó sin conexión, de manera análoga a circuito virtual y Datagrama.
- * Grado de servicio: Esto permite a la entidad (5) especificar el error aceptable, los niveles de pérdida, el retardo deseado, la prioridad y la seguridad.

- * Manejo de la conexión: La capa 4 puede fijar unas conexiones de gestión (manejo) entre las entidades (5) a través de los CEPs (4) para el servicio de conexión orientada.

El tamaño y complejidad de un protocolo de transporte, depende del tipo de servicio que pueda obtener de la capa 3. Para una capa 3 fiable con capacidad para circuito virtual, se requiere una capa 4 mínima. Si la capa 3 no es fiable ó/y sí sólo soporta datagramas, la capa 4 debe incluir un extenso detector y corregidor de errores.

La capa de sesión proporciona un mecanismo de control del diálogo entre entidades de presentación. Como mínimo, esta capa facilita un modo de establecer y usar una conexión entre dos entidades de presentación. A esto se le denomina "sesión". Además puede facilitar los siguientes servicios:

- * Tipos de diálogo: Este puede ser de dos vías simultáneas, dos vías alternadas ó una vía.
- * Recuperación: La capa de sesión puede tener un mecanismo de "puntos de comprobación" (Check Pointing), y de tal manera que si se produce una pérdida o corte entre dos de estos puntos, la entidad de sesión puede retransmitir todos los datos desde el último punto de comprobación.

Capa de presentación:

Esta capa ofrece programas de aplicación y de gestión de terminales y servicios de transformación. Estos servicios son típicamente:

- * Traducción de datos: Traducción de código y de caracteres.
- * Formateo: Modificación de la disposición de los datos.
- * Selección de Sintaxis: Selección inicial y las subsecuentes modificaciones de las transformaciones usadas.

Un ejemplo de protocolo de presentación es el "Virtual Terminal Protocol". Este protocolo convierte las características específicas de terminal en el modelo virtual ó genérico usado por el programa de aplicación. Este tipo de protocolos lo veremos más adelante.

Capa de aplicación:

La capa de aplicación incluye aplicaciones que han de ser corridas en un ambiente distribuido. Ejemplos de este tipo de protocolos son el correo electrónico, los servicios de transacciones, etc...

TECNOLOGIA DE LAS REDES LOCALES

INTRODUCCION.

Los principales ingredientes tecnológicos que determinan la naturaleza de una red local son:

- * Topología.
- * Medio de transmisión.
- * Técnica de control del medio.

Todos juntos, determinan en gran medida el tipo de datos que pueden ser transmitidos, la velocidad y eficiencia de la comunicación, e incluso la clase de aplicaciones que una red puede soportar.

Este capítulo da un repaso a las topologías y medios de transmisión, apropiados para redes locales. También se incluye una clasificación de redes locales.

TOPOLOGIAS.

El término topología, en el contexto de una red de comunicación, se refiere a la manera en que se interconectan los puntos finales ó estaciones. Una topología es definida por la disposición de los enlaces de comunicación y los elementos de conmutación (Switching), y determina los caminos de datos que pueden ser utilizados entre un par de estaciones.

Para entrar en tema, consideremos el porqué se necesitan las redes de comunicación. De acuerdo con la definición que vimos en el capítulo 1, una red local proporciona un modo de conectar dispositivos en un área reducida. ¿Por que no suministrar un enlace directo entre cada par de dispositivos que necesiten comunicarse?.

El problema de esta sugerencia se ilustra en la figura 3.1. Cada dispositivo tiene un enlace directo llamado "enlace punto-a-punto", con cada uno de los dispositivos restantes. Sí hay N dispositivos, se requieren $N(N-1)$ enlaces y $(N-1)$ puertos de E/S. El coste del sistema en concepto de cableado y Hardware de E/S es N^2 .

La inviabilidad de este diseño, conocido a veces como "Mesh Topology" (red poligonal ó en enjambre), resulta mucho más clara en áreas más amplias. La solución

es introducir una red con nodos de conexión, crear enlaces lógicos y eliminar todos los enlaces físicos directos entre estaciones. Así, cada estación se conecta a un nodo de comunicaciones y comunica con otras estaciones vía red.

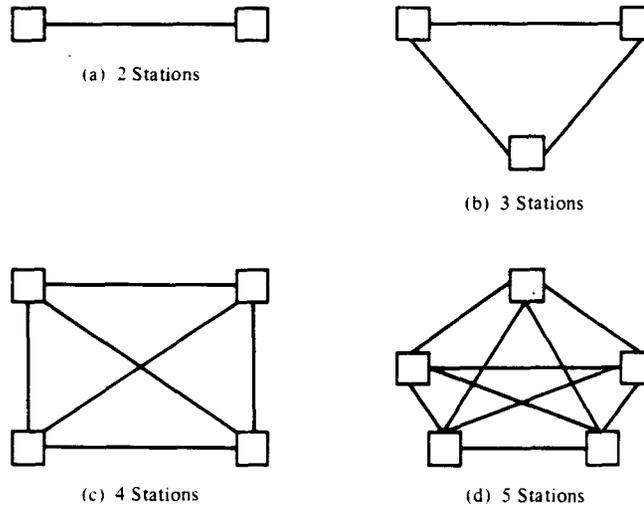


FIGURE 3-1. The Problem with Direct Connection or Mesh Topology.

Este último sistema no es muy utilizado en redes locales ya que al ser distancias cortas, el coste de los nodos resulta muy elevado. Las topologías han sido diseñadas para solucionar el problema de la "Mesh Topology" usando uno ó ningún nodo.

Describiremos a continuación cuatro topologías (las más importantes): Bus, Arbol, Anillo y Estrella. También pueden ser usadas en bloque como unidades de redes más complejas.

Topología Estrella:

En la topología Estrella, cada estación está conectada a un interruptor (Switch) común central mediante un enlace punto a punto (figura 2.3). la comunicación entre dos estaciones cualesquiera es vía *Circuit Switching*. Para que una estación pueda transmitir datos, debe enviar una petición al *Switch* central, pidiendo una comunicación con la otra estación. Una vez fijado el circuito, los datos pueden ser intercambiados por ambas estaciones como si estuviesen conectadas con un enlace punto a punto.

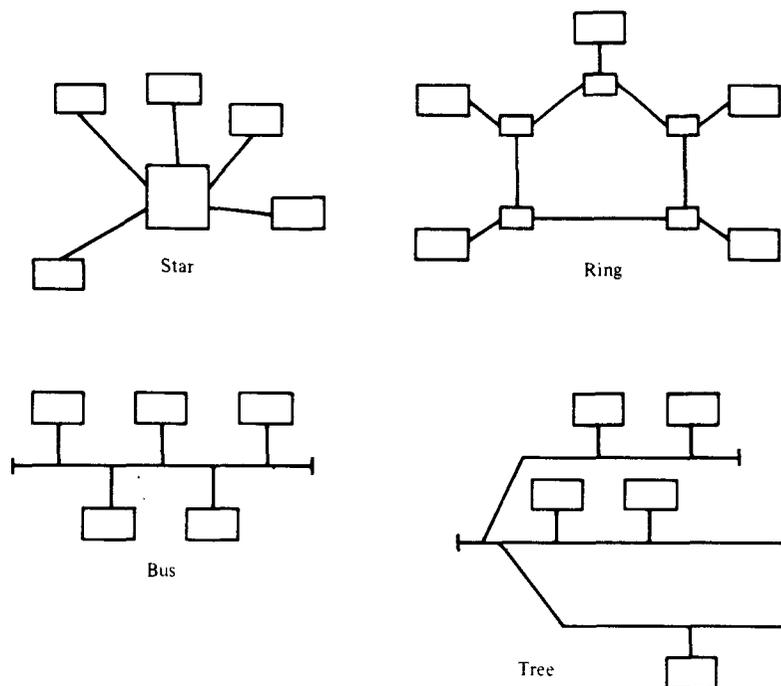


FIGURE 3-2. Local Network Topologies

Esta topología tiene una estrategia de control centralizado de la comunicación. Todas las comunicaciones son controladas por el Switch central, el cual debe fijar y mantener un buen número de caminos concurrentes. En consecuencia el nodo central debe ser complejo. Por otro lado, la carga de procesamiento en las estaciones es mínimo. A parte de una lógica rudimentaria de aceptación y petición de datos, las estaciones solo tienen que contemplar los requerimientos simples de comunicación con enlace punto a punto.

Topología Anillo:

En la topología Anillo, la red local consiste en una serie de "repetidores" unidos por enlaces punto a punto formando un circuito cerrado. Cada repetidor tiene dos enlaces. El repetidor es un dispositivo relativamente sencillo, capaz de recibir datos por un enlace y transmitirlos, bit a bit, por el otro enlace, tan pronto como son recibidos, sin retenerlos ni almacenarlos en el repetidor. Los enlaces son unidireccionales, es decir, que los datos son transmitidos en una sola dirección y orientados en la misma dirección. Los datos circulan en el anillo en una dirección.

Cada estación se conecta a la red a través de un repetidor. Los datos son transmitidos en paquetes. Así, por ejemplo, si la estación X desea transmitir un mensaje a la estación Y, ella divide el mensaje en paquetes. Cada

paquete contiene una parte de datos más alguna información de control, incluyendo la dirección de Y. Los paquetes son introducidos uno a uno en el anillo y circulan a través de los demás repetidores. La estación Y reconoce su dirección y copia los paquetes según pasan.

Como hay muchos dispositivos que comparten el anillo se necesita algún tipo de control que determine el momento en el cual cada estación puede insertar paquetes. Esto es casi siempre llevado a cabo mediante control distribuido. Lo estudiaremos en el capítulo 5.

Observar la diferencia entre la topología en Anillo y en Estrella. Mientras la topología Estrella exige un procedimiento complejo de la red y la mínima carga en las estaciones, la topología Anillo, los dispositivos de la red son simples repetidores. Pero las estaciones deben proporcionar la lógica de empaquetado y de control de acceso.

Topologías Bus y Arbol:

Con la topología Bus, la red de comunicación es simplemente el medio de transmisión (no hay ni nodos ni repetidores). Todas las estaciones se conectan mediante el apropiado interface de Hardware, directamente a un medio lineal de transmisión, ó "Bus". Cualquier transmisión de una estación se propaga a lo largo del medio y puede ser recibido por todas las estaciones.

La topología Arbol es una generalización de la

topología Bus. El medio de transmisión es un cable con ramas sin llegar a cerrarse. Para ambas topologías, el medio se denomina "multipunto" (Multipoint) ó de emisión (Broadcast).

Como todos los nodos comparten un enlace común, sólo un dispositivo puede transmitir a la vez. De nuevo se necesita algún tipo de control de acceso. Típicamente, (no siempre) este control es ejercido en forma de protocolo, de manera compartida por todos los nodos conectados (control distribuido). También se usa un fórmula de control central.

Como en el Anillo se suele usar una transmisión por paquetes. Una estación que desee transmitir un mensaje, lo divide en paquetes y lo introduce en el medio uno a uno, posiblemente intercalándolos con otros paquetes de otras estaciones. La estación de destino reconoce su dirección en los paquetes y los copia según pasan.

La red está libre de los cargos del procesamiento en la comunicación; desde el punto de vista de la comunicación, es un mero medio pasivo de la transmisión. La carga de procesamiento en las estaciones conectadas es de la misma magnitud que en la topología Estrella.

Elección de topología:

La elección de topología de una red depende de varios factores, incluyendo fiabilidad, expandibilidad y rendimiento. Esta elección es una parte de la tarea global

de diseño de una red local.

Las topologías Bus/Arbol parecen ser, a priori, las más flexibles. Es posible manejar un amplio rango dispositivo en términos de número de dispositivos, velocidades y tipos de datos. Es posible tener un ancho de banda alto. Como el medio es pasivo, podría parecer a simple vista, muy fiable. Como veremos más adelante, éste no es necesariamente el caso. En particular, una rotura del cable supondría la inutilización parcial ó total de la red.

Entre los repetidores de la topología Anillo podemos usar enlaces de alta velocidad (como fibras ópticas). Así pues, el anillo tiene el potencial de proporcionar la mejor transparencia de todas la topologías. Hay, sin embargo, limitaciones parciales en lo que se refiere al número de dispositivos y la variedad de datos. Finalmente, el problema de la fiabilidad es obvio: si falla un sólo repetidor, se viene a bajo toda la red.

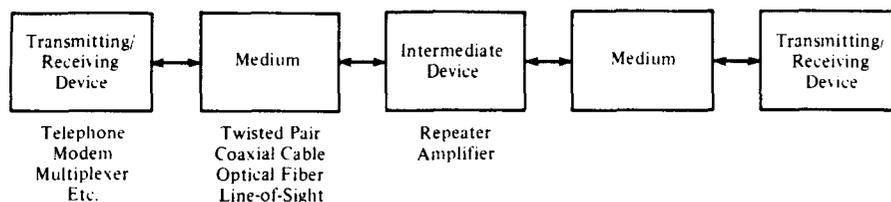
La topología Estrella usa *Circuit Switching* e integra fácilmente voz con tráfico de datos. Va bien con dispositivos de baja velocidad (≤ 64 Kb/seg.). La topología Estrella es buena para requerimientos intensos de terminal, debido a la carga mínima de procesamiento que impone a los dispositivos conectados a ella.

MEDIOS DE TRANSMISION.

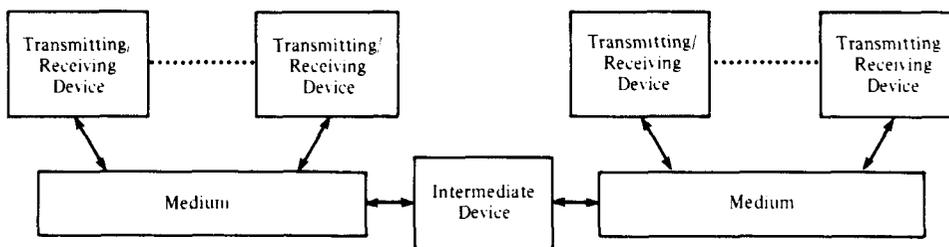
El medio de transmisión es el camino físico entre el transmisor y el receptor en una red de comunicaciones. La figura 3.3 muestra los elementos básicos de un sistema de transmisión. La configuración más común es un enlace punto a punto entre dos dispositivos transmisores/receptores, los cuales a través de los interfaces adecuados, insertan señales analógicas ó digitales en el medio. También puede usarse uno ó más dispositivos intermedios para compensar la atenuación u otro deterioro en el medio. Los enlaces punto a punto son usados en la topología Anillo para unir repetidores adyacentes y en la topología Estrella para conectar los dispositivos al Switch central. También pueden ser usados para unir dos redes en distintos edificios. Lo veremos más adelante. Los enlaces multipunto se usan para conectar muchos dispositivos, como en las topologías Bus y Arbol. Como los dispositivos se enganchan a la red en varios puntos, se hacen necesarios los repetidores (señales digitales) ó amplificadores (señales análogas) para agrandar la extensión del medio.

La transmisión puede ser clasificada en "guiada" ó "no guiada". En ambos casos hablamos de ondas electromagnéticas. Con un "medio guiado", las ondas son guiadas a lo largo de un camino físico. El par trenzado,

el cable coaxial y las fibras ópticas son medios guiados que se usan en redes locales.



(a) Point-to-point



(b) Multipoint

FIGURE 3-3. Simplified Transmission System Block Diagram

Las tablas 3.1 y 3.2 resumen las principales características de este medio cuando es usado en una configuración punto a punto y multipunto. Los valores dados no son límites. Representan lo comercialmente fiable y factible. La atmósfera y el espacio exterior son ejemplos de "medio no guiado" los cuales facilitan la transmisión de ondas electromagnéticas pero no las guía. Varias maneras de transmisión a través de la atmósfera, se utilizan para las conexiones entre edificios.

Vamos a estudiar estos medios, a partir de seis parámetros ó características:

- * Descripción física: La naturaleza del medio de transmisión.
- * Características de transmisión: incluyendo donde se usa señal analógica ó digital, técnicas de modulación, capacidad, y el rango de frecuencias en el que se transmite.
- * Conectividad: punto a punto o multipunto.
- * Alcance geográfico: la distancia mayor entre los puntos en la red.
- * Inmunidad al ruido: resistencia del medio a la contaminación de los datos transmitidos.
- * Costo relativo: basado en el costo de los componentes, instalación y mantenimiento.

PAR TRENZADO:

Es, con mucho el medio de transmisión más utilizado tanto para señales analógicas como digitales.

Descripción física:

Un par trenzado consiste en dos cables aislados dispuestos en espiral. Los cable son de cobre o de acero recubierto de cobre. El cobre proporciona conductividad; el acero la dureza. Un par trenzado actúa como un enlace único de comunicaciones. Normalmente se empaquetan varios de estos pares en un solo cable. El trenzado de cada par, minimiza las interferencias eletromagnéticas entre pares. Los cables de un par tienen un espesor desde 0.016 hasta

0.036 pulgadas.

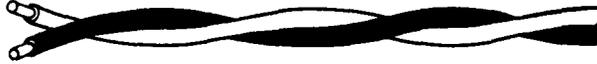


FIGURE 3a

Características de transmisión:

Los pares trenzados pueden utilizarse para la transmisión de señales analógicas y digitales. En la transmisión de señales analógicas se necesitan amplificadores cada 5 ó 6 Km. Para señales digitales los repetidores se ponen cada 2 ó 3 Km.

El uso más común del par trenzado es en la transmisión analógica de la voz. Aunque la mayoría de los componentes en frecuencia de la voz se encuentran entre los 20 Hz y los 20 KHz, se necesita un ancho de banda más estrecho para una reproducción inteligible de la misma. El ancho de banda estándar para un canal *Full-Duplex* de voz es de 300 a 3.400 Hz. Usando **FDM**, podemos multiplexar un buen número de canales de voz en un sólo par trenzado. Un ancho de banda de 4 KHz proporciona una separación adecuada entre canales. Un par trenzado tiene la capacidad de 24 canales de voz, usando un ancho de banda de 268 KHz.

Usando un modem, podemos transmitir datos digitales a través de un canal analógico de voz. Podemos, con un modem normal, alcanzar velocidades de 9.600 bps. usando **PSK**. En

un par de 24 canales de voz, la velocidad global (de datos) es de 230 Kbps.

Es también posible usar señales digitales o de banda-base en este tipo de medio. Bell ofrece su circuito T1 en el cual usa pares trenzados en 24 canales PCM de voz, con una velocidad global de 1.544 Mbps.

TABLE 3.1 Point-to-point Transmission Characteristics of Guided Media

Transmission Medium	Total Data Rate	Bandwidth	Repeater Spacing
Twisted Pair	4 Mbps	250 kHz	2–10 km
Coaxial Cable	500 Mbps	350 MHz	1–10 km
Optical Fiber	2 Gbps	2 GHz	10–100 km

TABLE 3.2 Transmission Media for Local Networks: Multipoint

Medium	Signaling Technique	Maximum Data Rate (Mbps)	Maximum Range at Maximum Data Rate (km)	Practical Number of Devices
Twisted pair	Digital	1–2	Few	10's
Coaxial cable (50 ohm)	Digital	10	Few	100's
Coaxial cable (75 ohm)	Digital	50	1	10's
	Analog with FDM	20	10's	1000's
	Single-channel Analog	50	1	10's
Optical fiber	Analog	10	1	10's

Conectividad:

El par trenzado puede ser aplicado en sistemas punto a punto y multipunto. Como medio para aplicaciones

multipunto es menos caro, de menor rendimiento que el cable coaxial, pero soporta menor número de equipos. Su uso en sistemas punto a punto es mucho más común.

Alcance geográfico:

El par trenzado puede facilitar una comunicación punto a punto de 15 Km. ó más. Este medio es usado dentro de un mismo edificio ó un par de ellos.

Inmunidad a ruidos:

Comparado con otro medio guiado, el par trenzado está limitado en ancho de banda, distancia y velocidad. El medio es bastante propenso a interferencias y al ruido debido a su fácil acoplamiento con campos magnéticos. Por ejemplo, un cable corriendo paralelamente a una línea AC de potencia tomará una energía de 60 Hz. Señales en pares adyacentes pueden interferir, un fenómeno que se conoce como "Crosstalk" (cruce de líneas).

Podemos tomar muchas medidas para evitar los inconvenientes. Recubriendo el cable con una trencilla ó forro metálico se reducen las interferencias. El trenzado de los pares reduce la interferencia a bajas frecuencias, y el uso de diferentes longitudes en pares adyacentes reduce el cruce de líneas. Estas medidas son eficaces para longitudes de onda mucho mayores que la longitud de cable. La inmunidad al ruido puede ser tan buena como en el cable coaxial para frecuencias de transmisión baja. No obstante

por encima de los 10 - 100 KHz, el cable coaxial es superior.

Coste:

El coste de este medio es menor que el del cable coaxial ó la fibra óptica en términos de coste por metro. No obstante, dada su limitación en la conectividad, los costes de instalación se aproximan a los de los otros medios.

CABLE COAXIAL:

Es el medio de transmisión más versátil para redes locales. Nosotros veremos dos tipos de cables coaxial usados comúnmente en las redes locales: El cable de 75 Ohm usado normalmente en antenas comunitarias de televisión (CATV) y el de 50 Ohm. Como se aprecia en la tabla 3.2, el cable de 50 Ohm. se usa sólo con señales digitales y se denomina banda/base (Base Band); El de 75 Ohm se usa para señales analógicas con FDM, y se le conoce por banda ancha (Broadband), y para señales digitales de alta velocidad y analógicas donde sea posible la FDM. Esta última se denomina *Single Chanel Broad Band* (Banda ancha de canal único).

Descripción física:

El cable coaxial, como el par trenzado, consta de dos conductores, pero está construido de diferente manera para

permitir un mayor rango de frecuencia. Consiste en un conductor hueco cilíndrico y exterior que rodea un único conductor interior. El conductor interior puede ser sólido ó acordado; el exterior puede ser sólido ó trenzado. El conductor interior es mantenido en su sitio por anillos aislantes regularmente espaciados ó por un material dieléctrico sólido. A su vez el conductor exterior va rodeado por una cubierta. El diámetro de un cable coaxial es de 0.4 a 1 pulgada.

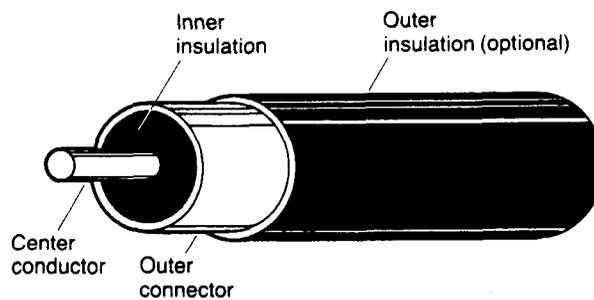


FIGURE 3b

Características de transmisión:

El cable de 50 Ohm. es usado exclusivamente para la transmisión digital. Se usa normalmente la codificación Manchester, y se pueden alcanzar velocidades de 10 Mbps.

El cable CATV se usa tanto para señales digitales como para analógicas. Para señales analógicas se puede conseguir frecuencias de 300 a 400 MHz. Los datos analógicos, como señales de video y audio, pueden ser

transmitidos por un cable CATV del mismo modo que lo hacen las emisoras de radio y televisión en el espacio libre. Los canales de TV ocupan 6 MHz cada uno del ancho de banda total; los canales necesitan mucho menos. Por lo tanto, en este tipo de cable se pueden habilitar un gran número de canales usando **FDM**.

Cuando se usa **FDM**, al CATV se le denomina "Broadband" (banda ancha). El espectro de frecuencias del canal se divide en canales, cada uno de los cuales lleva una señal analógica. También podemos llevar datos digitales por uno de estos canales. Hay varias técnicas de modulación para datos digitales, entre ellas la **ASK**, **FSK**, y **PSK**. La eficiencia del modem determinará el ancho de banda necesario para soportar una velocidad de datos dada. Una buena regla es suponer 1 Hz por bps para velocidades de 5Mbps ó mayores, y 2 Hz por bps para velocidades menores. Por ejemplo, una velocidad de 5 Mbps, teniendo en cuenta que un modem de 4.8 Kbps usa unos 20 KHz, puede lograrse con una red de TV de 6 MHz. Actualmente se pueden alcanzar velocidades de 20 Mbps; a estas velocidades la eficiencia del ancho de banda supera la relación 1 Bps/Hz.

Para lograr velocidades mayores de 20 Mbps, debemos hacer dos aproximaciones. Ambos requieren que la totalidad del ancho de banda del cable de 75 Hz se dedique a esta transferencia de datos; no se emplea **FDM**. Una aproximación es usar señal digital en el cable, como se hace en el de 50 Hz. DE este modo se pueden alcanzar velocidades de

hasta 50 Mbps. La otra alternativa es usar un simple sistema PSK.

Conectividad:

El cable coaxial es aplicable a configuraciones punto a punto y multipunto. Cada cable banda base de 50 Hz puede soportar el orden de 100 dispositivos por segundo, pudiendo formar sistemas mayores uniendo segmentos mediante repetidores. El cable banda ancha de 75 Hz puede soportar miles de dispositivos. El uso de este cable a altas velocidades (50 Mbps), pero introduce problemas técnicos (que trataremos más adelante) que limitan el número de dispositivos a 20 ó 30.

Alcance geográfico:

Las distancias típicas en un cable banda base se limitan a unos pocos kilómetros. Las redes con cables banda ancha pueden extenderse decenas de kilómetros. La diferencia tiene relación con la integridad relativa de las señales analógicas y digitales.

Los transmisores a alta velocidad (50 Mbps), digital ó analógica, se limitan a 1 Km. Dada la alta velocidad la distancia física entre señales en el bus es muy pequeña, por tanto, una atenuación ó ruidos muy leves pueden ser tolerados antes de que se pierdan los datos.

Inmunidad al ruido:

La inmunidad al ruido de un cable coaxial depende de su aplicación e implementación. En general es superior a la del par trenzado, para frecuencias altas.

Coste:

El coste de instalación de un cable coaxial está entre el del par trenzado y el de las fibras ópticas.

CABLE DE FIBRA OPTICA:

El descubrimiento más interesante en el campo de los medios de transmisión de las redes locales se sitúa en el área de las fibras ópticas. Dado que la tecnología está constantemente cambiando, vamos a dar solamente una idea actual de las capacidades de la fibra óptica.

Descripción física:

Una fibra óptica es un medio delgado (de 2 a 125 μm) y flexible, capaz de conducir un rayo óptico. Hay varios plásticos y cristales usados en la fabricación de estas fibras. las menores pérdidas se consiguen con fibras de sílice fundido ultrapuro. La fibra ultrapura es difícil de hacer; las fibras de cristal multicomponentes tienen mayores pérdidas pero son más económicas y proporcionan un buen rendimiento. La fibra de plástico es incluso más barata y puede ser usada para enlaces cortos, en donde las pérdidas moderadamente altas son aceptables. Un cable de

fibra óptica tiene forma cilíndrica y contiene tres secciones concéntricas: el núcleo, la cubierta y la funda. El núcleo es la sección más interior, y consiste en una o más hebras, ó fibras, de plástico ó cristal. Cada fibra está rodeada por su propia cubierta, que es un abrigo de plástico que posee propiedades ópticas diferentes de las que posee el núcleo. La capa más externa, que rodea una ó varias fibras cubiertas, es la funda. Esta última se compone de plástico y otros materiales que protegen el interior de la abrasión, humedad, ruptura y demás peligros ambientales.

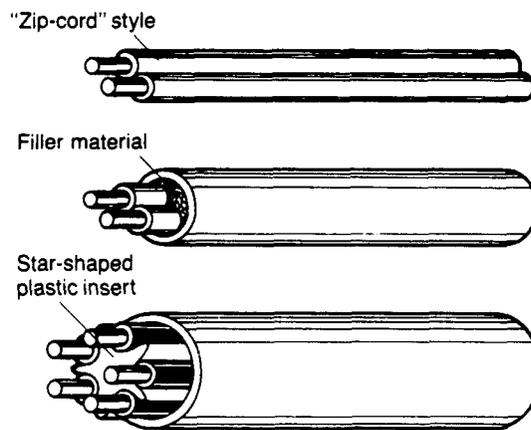


FIGURE 3c

Características de transmisión:

La fibra óptica transmite un haz de luz codificado por señal, gracias a su "reflexión interna total". La

reflexión interna total puede obtenerse en cualquier medio transparente que tenga un índice de refracción mayor que el del medio que lo rodea. Las fibras ópticas actúan como una guía de ondas para frecuencias de 10^{14} a 10^{15} Hz, la cual cubre el espectro visible y parte del infrarrojo.

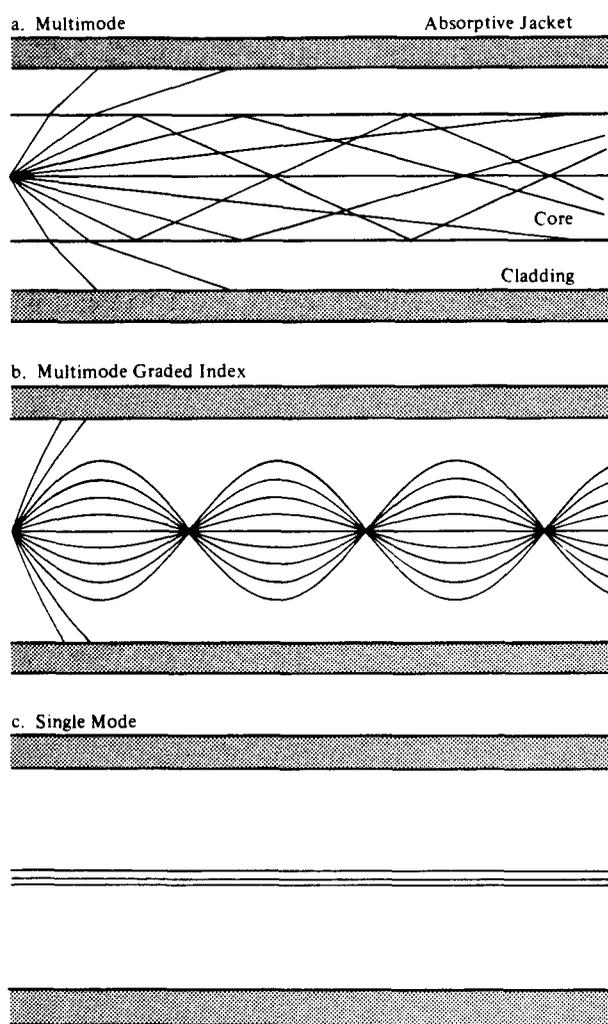


FIGURE 3-4. Optical Fiber Transmission Modes

La figura 3.4 nos muestra el principio de la transmisión a través de fibra óptica. La luz proveniente de una fuente entra en el núcleo cilíndrico de plástico ó cristal. Los rayos poco angulados son reflejados y propagados a lo largo de la fibra; otros rayos son absorbidos por el material de alrededor. Esta forma de propagación se denomina "multimodo" debido a la variedad de ángulos reflejados. Reduciendo el radio del núcleo al orden de la longitud de onda, sólo puede pasar un ángulo ó modo: el rayo axial. Este sistema da mayor rendimiento que el multimodo por la siguiente razón. Con la transmisión multimodo, existen muchos caminos de propagación, cada uno con una longitud distinta (debido al ángulo de cada rayo), y por tanto con un tiempo distinto para atravesar la fibra. Esto ocasiona el esparcimiento en el tiempo de los elementos de la señal, limitando la velocidad a la cual los datos son recibidos correctamente. Con la transmisión modo-único (Single-Mode), sólo hay un camino de propagación, por lo que no se dan este tipo de distorsiones. Finalmente, cambiando el índice de refracción del núcleo, podemos obtener un tercer tipo de transmisión: el multimodo de índice graduado (Multimode Graded Index). Las características de este tipo están entre las de los anteriores. La refracción variable tiene el efecto de enfocar los rayos más eficientemente que en el tipo multimodo. La tabla 3.3 compara los tres modos de transmisión. Como se puede ver, las capacidades que se

alcanzan con la fibra óptica superan en mucho las del par trenzado y el cable coaxial.

TABLE 3.3 Comparison of Three Types of Optical Fibers

	Step-index Multimode	Graded-index Multimode	Single-mode
Light Source	LED or laser	LED or laser	laser
Bandwidth	wide (up to 200 MHz/km)	very wide (200 MHz to 3 GHz/km)	extremely wide (3 GHz to 50 GHz/km)
Splicing	difficult	difficult	difficult
Typical Application	computer data links	moderate-length telephone lines	telecommunication long lines
Cost	least expensive	more expensive	most expensive
Core Diameter (μm)	50 to 125	50 to 125	2 to 8
Cladding Diameter (μm)	125 to 440	125 to 440	15 to 60
Attenuation (db/km)	10 to 50	7 to 15	0.2 to 2

Dos tipos diferentes de fuentes de luz se usan en sistemas de fibras ópticas: el "Light - Emission - Diode" (LED) y el "Injection - Laser - Diode" (ILD). El LED es un dispositivo de estado sólido que emite luz cuando se le aplica corriente. El ILD es un dispositivo de estado

sólido que trabaja sobre el principio del Laser en el cual los efectos electrónicos son combinados para producir un haz super radiante de ancho de banda estrecho. El LED es menos costoso, opera bajo un gran rango de temperaturas, y tiene una vida más larga. El ILD es más eficiente y puede proporcionar las mayores velocidades de transmisión.

TABLE 3.4 Transmission Losses of Various Types of Optical Fiber

Mode	Material Core/Cladding	Transmission Loss, dB/km		
		850 nm	1300 nm	1500 nm
Single mode	Silica glass/silica glass	2	0.5	0.2
Step-index multimode	Silica glass/silica glass	2	0.5	0.2
	Silica glass/plastic	2.5	High	High
	Multicomponent glass/multicomponent glass	3.4	High	High
Graded-index multimode	Silica glass/silica glass	2	0.5	0.2
	Multicomponent glass/multicomponent glass	3.5	High	High

El detector que se usa en el extremo receptor para convertir la luz en energía eléctrica es un fotodiodo. Tenemos dos dispositivos: el detector PIN y el APD. El fotodiodo PIN tiene un segmento de cilicio intrínseco (I) entre las capas P y N de un diodo. El diodo de avalancha APD, es similar en apariencia pero usa un campo eléctrico más fuerte. Ambos dispositivos son básicamente contadores de fotones. El PIN es menos caro y menos sensible que el APD.

La modulación de la luz, se hace con una forma de ASK llamada "modulación de intensidad". Normalmente, los dos

dígitos binarios se representan por la presencia ó ausencia de luz a la frecuencia dada. Tanto los LED como los ILD pueden ser modulados de esta manera. Los detectores PIN y APD responden directamente a la modulación de intensidad.

En laboratorio se han alcanzado velocidades de hasta unos gigabits por segundo. En la práctica se pueden obtener unos cientos de megabits por segundo en unos pocos kilómetros.

Hay una relación entre la longitud de onda empleada, y el tipo de transmisión, y la velocidad posible. Tanto el modo único como el multimodo pueden soportar luces con diferentes longitudes de onda y pueden emplear Laser o LEDs como fuentes de luz. En una fibra de cristal, la luz se propaga mejor en tres longitudes de onda distintas (Windows), centradas en los 850, 1.300 y 1.500 nano metros (nm). La pérdida es menor con longitudes de onda mayores, permitiendo así velocidades mayores a grandes distancias. Esto se indica en la tabla 3.4. La mayoría de las aplicaciones locales usan LEDs de 850 nm como fuentes de luz. Aunque ésto es relativamente barato, limita la velocidad por debajo de los 100 Mbps y la distancia a unos pocos kilómetros. Para obtener mayor velocidad y distancias más largas, necesitamos como fuente de luz un LED de 1.300 nm ó un Laser. Aunque el LED de 850 nm es atractivo para su uso en LANs, es más apropiado usar el de 1.300 nm para HSLNs. Las mayores capacidades y distancias

posibles hoy en día, requieren el uso del LED de 1500 nm. Esta necesidad de mayor velocidad y distancia requieren a veces la utilización del Laser como fuente de luz, pero es normalmente muy caro para ser utilizado en redes locales.

Normalmente se usa una sola frecuencia portadora en la transmisión por fibra óptica.

Conectividad:

El uso más común de la fibra óptica es en enlaces punto a punto. Se han hecho sistemas multipunto usando topología Bus experimentalmente, pero resulta muy cara, hoy en día, para ser práctica. No obstante, y en principio, un solo segmento de fibra óptica puede soportar más enganches que el par trenzado ó el cable coaxial. Además posee poca pérdida de potencia, menor atenuación y un mayor potencial de ancho de banda.

Alcance geográfico:

La tecnología actual permite enlaces de 6 a 8 Km. de largo sin repetidores. De este modo la fibra óptica es apropiada para conectar redes locales en distintos edificios via enlaces punto a punto.

Inmunidad al ruido:

La fibra óptica no se ve afectada por ruido ó interferencias electromagnéticas. Esta característica permite grandes velocidades y distancias con una gran

velocidad.

Coste:

Es más caro que el par trenzado ó el cable coaxial en términos de coste por metro y necesita receptores y conectores.

LA ATMOSFERA COMO MEDIO:

En esta sección veremos tres técnicas de transmisión de ondas electromagnéticas a través de la atmósfera: microondas, infrarrojos, y Laser. Todas ellas requieren una "línea visual directa" entre el transmisor y el receptor.

Debido a las altas frecuencias a las cuales operan estos dispositivos (microondas, 10^9 a 10^{10} Hz; infrarrojos, 10^{11} a 10^{14} Hz; Laser, 10^{14} a 10^{15} Hz), existe un claro potencial para alcanzar velocidades de transmisión muy altas. En la práctica se han construido sistemas para enlaces cortos con velocidad del orden de varios mega bits por segundo.

Esta técnica de transmisión es primordialmente útil para conectar redes locales situadas en edificios diferentes, ya que es difícil tender un cable entre edificios separados, ya sea por encima ó bajo tierra, especialmente si el espacio intermedio es de propiedad pública. Los sistemas de línea visual directa sólo requieren equipos en cada edificio.

El enlace por infrarrojos consiste en un par de transmisores receptores (tranceptores) que modulan luz infrarroja no coherente. Los tranceptores deben colocarse en los tejados de ambos edificios ó dentro de los edificios con ventanas exteriores adyacentes. Pero siempre dentro de una línea visual directa. El sistema es altamente direccional; es, por tanto, extremadamente difícil de interceptar, meter datos, ó interferir estos sistemas. No es necesario ninguna licencia, por lo que pueden ser instalados en unos días. En la práctica se pueden exigir velocidades de unos mega bits por segundo en distancias de unos pocos kilómetros.

TABLE 3.5 Transmission Media for Local Networks: Point-to-Point Across Public Property

Medium	Ease of Installation	Regulatory Licensing (months)	Data Rate (Mbps)	Ease of Maintenance	Cost
Infrared	1-2 days, easy	None	1-3	Excellent	Low
Laser	1-2 days, easy	2-6	1-3	Excellent	Low
Microwave	1 week, easy	2-3	1-3	Excellent	Low
Underground coax/ optical fiber	1-18 months, moderate to hard	6-18	10+	Fair to good	Moderate to high
Aerial coax/ optical fiber	1-6 months, moderate	6-18	10+	Good	Moderate to high

Un sistema similar puede instalarse con tranceptores de Laser, los cuales hacen una modulación de luz coherente. La mayor diferencia es que en EE.UU, el estado

exige que el Hardware Laser, esté convenientemente protegido. El proceso de licencia lleva de 2 a 6 meses.

Ambos sistemas, el Laser y los infrarrojos pueden verse afectados por las condiciones ambientales, como la lluvia y niebla. Un sistema con menos sensibilidad es el microondas. Como en los sistemas antes mencionados, la instalación de sistemas de microondas es relativamente sencilla; la mayor diferencia es que los trancptores de microondas pueden ser montados sólo en el exterior de los edificios. Este sistema es menos direccional que los anteriores; de ahí que haya un problema de seguridad en lo que se refiere a inserciones, interferencias ó de espionaje de datos. Como todo sistema de radiofrecuencia necesita una licencia. En EE.UU. la Comisión Federal de Comunicaciones tarda de 2 a 3 meses en extender la misma. En este sistema es posible alcanzar velocidades iguales a las obtenidas con Laser ó con infrarrojos.

La tabla 3.5 resume las características principales de estas técnicas e incluye, para comparar, el uso de cable para el enlace entre edificios.

LA ELECCION DEL MEDIO DE TRANSMISION:

La elección del medio de transmisión adecuado está determinada por varios factores, entre ellos la topología de la red local. Hay otros factores que juegan un papel importante:

- * Capacidad: para soportar el tráfico esperado.

- * Seguridad: para encontrar necesidades disponibles.
- * Tipos de datos soportados: ajustados a la aplicación.
- * Alcance ambiental: para proporcionar servicios por encima del rango de ambientes requeridos.

Esta elección es una parte de la tarea global del diseño de una red local, la cual trataremos en profundidad más adelante. De momento sólo vamos a hacer observaciones generales.

El par trenzado es un medio barato y bien conocido. Aunque comparado con el cable coaxial tenga un ancho de banda limitado, el par trenzado es el más barato y efectivo medio de transmisión para una instalación de red local en un sólo edificio y con poco tráfico. Un buen ejemplo de aplicación es un sistema de automatización de una oficina con mayoría de terminales mudos y/o estaciones de trabajo inteligentes, más unos pocos "minis".

El cable coaxial es más caro pero de mayor capacidad. Con la excepción de sistemas de terminales intensivos, es la opción a elegir para las exigencias de una red local. En la mayoría de los casos, una red local con cable coaxial, puede diseñarse para manejar la demanda actual y poder ser ampliada, dentro de unos costes razonables. Los sistemas coaxiales sobresalen cuando se tienen un buen número de dispositivos y un considerable tráfico de datos. Los ejemplos de aplicación incluyen a las instalaciones de

gran procesamiento de datos y a los sistemas sofisticados de automatización de oficinas, los cuales pueden incluir fascimiles, copiadoras inteligentes y dispositivos gráficos a color.

Por ahora, los enlaces de fibra óptica son apropiados para comunicaciones punto a punto. Por lo tanto no pueden competir con el cable coaxial, a excepción de redes con topología en anillo. No obstante, cuando el coste de la fibra óptica "Multidrop" (de muchos enganches) sea competitivo con el del cable coaxial, sus ventajas (baja influencia del ruido, pérdidas bajas, tamaño pequeño y ligereza) hará de ellas un serio competidor en muchas aplicaciones en redes locales.

Los sistemas que necesitan una línea visual directa no son adecuados para las redes locales. No obstante, son buenos para proporcionar enlaces punto a punto entre edificios con sus propias redes locales.

3.3

RELACION ENTRE EL MEDIO DE TRANSMISION Y LAS TOPOLOGIAS.

Combinaciones:

La elección del medio de transmisión y de la topología no son independientes. La tabla 3.6 ilustra los

cambios.

Para la topología Bus, son apropiados tanto el par trenzado como las dos formas de cable coaxial. Actualmente la fibra óptica no es aplicable, ya que no resultaría rentable.

TABLE 3.6 Relationship Between Medium and Topology

Medium	Topology			
	Bus	Tree	Ring	Star
Twisted pair	x		x	x
Baseband coaxial cable	x		x	
Broadband coaxial cable	x	x		
Optical fiber			x	

La topología Arbol es usada con cable coaxial CATV de banda ancha. como veremos más adelante, la naturaleza unidireccional de la transmisión por ancho de banda, permite la construcción de la arquitectura en Arbol. Por otro lado, la naturaleza bidireccional de la transmisión por banda base, la hace inadecuada para esta topología. De nuevo hemos de decir que la fibra óptica no resulta rentable en esta topología.

La topología Anillo exige enlaces punto a punto entre repetidores. Los pares trenzados, el cable coaxial y la fibra óptica pueden ser usados para proporcionar estos enlaces. El cable coaxial de banda ancha no va a funcionar bien en esta topología, pues cada repetidor debería de ser

capaz de recibir y transmitir datos de manera asíncrona a través de muchos canales. El excesivo coste de estos dispositivos hacen que su uso sea difícilmente justificable.

La topología Estrella requiere un enlace único punto a punto entre cada dispositivo y el conmutador central. El par trenzado va muy bien. La altas velocidades de cable coaxial y de la fibra óptica podrían desbordar a los conmutadores de la tecnología actual.

Disposición (Layout):

Para que el concepto de distribución quede claro, debemos antes hacer una distinción entre topología y geometría. Las ilustraciones de la figura 3.2 muestran las distintas topologías de las redes locales; éstas definen el modo en el que los dispositivos están interconectados. Pero, en la práctica, el camino real que siguen los cables depende de las características físicas del edificio ó recinto. El cable puede seguir rutas que se acomoden a los muros y suelos del edificio. Normalmente se usan caminos predefinidos, algunas veces determinado por la existencia de conductos. Así pues, la geometría, ó disposición del cable, puede diferir en mucho con la forma de la topología deseada.

Vamos a analizar las necesidades que dictan el Layout de un cable instalado. La primera, y la más importante, es minimizar el coste cumpliendo con los requisitos de

capacidad. Un elemento determinante del coste es, por supuesto, el medio en sí. Como ya mencionamos, el par trenzado es más barato que el cable coaxial, el cual es a su vez más barato que la fibra óptica. Suele pasar, no obstante, que los costes de instalación excedan el de los materiales. Esto es particularmente grave en edificios ya construídos, los cuales pueden presentar dificultades para encontrar caminos para los nuevos cables. En un edificio nuevo, los costes y los problemas se reducen bastante si el *Layout* del cable para una red local puede diseñarse con antelación a su fabricación. Luego el cable sería instalado durante su construcción.

Un segundo requerimiento muy importante es que el *Layout* esté preparado para una eventual reordenación del equipo y para el crecimiento de la red. La manera más segura de prever estos eventos es instalar una red que llegue a todas las oficinas, ó instalar una pequeña red que pueda ser fácilmente ampliable con un mínimo ó con ningún efecto sobre la red existente. Por último señalar que el *Layout* debe proporcionar una buena gama de servicios y ser de fácil mantenimiento. De tal manera que cuando ocurra un fallo en la red, lo podamos localizar, aislarlo, y repararlo tan pronto como sea posible.

Teniendo en cuenta lo dicho, llegamos a la conclusión de que hay dos estrategias para disponer el medio de transmisión de una red local: de manera lineal ó en estrella.

TABLE 3.7 The Use of Alternative Wiring Strategies

Medium	Topology		
	Star	Ring	Bus
Twisted pair	S	L, S	L, S
Coaxial cable		L	L
Optical fiber		L	L

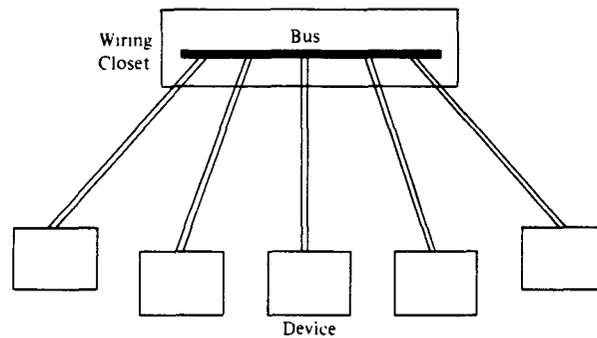
L = linear wiring strategy
S = star wiring strategy

La tabla 3.7 muestra la relación entre la estrategia de *Layout*, en el medio y la topologías en redes locales.

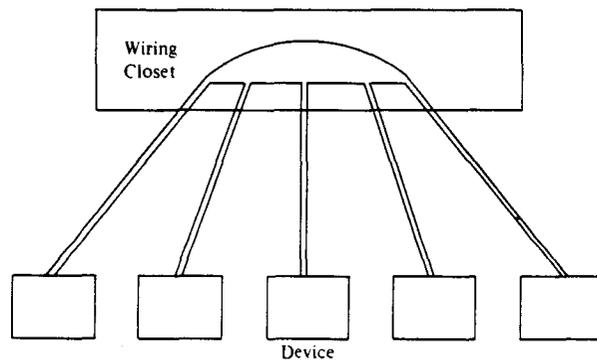
La estrategia lineal trata de proporcionar la topología deseada con el mínimo cableado, dependiendo de las características del edificio. Cualquiera de los medios guiados estudiados pueden utilizarse, y tanto las topologías Bus como Anillo pueden lograrse con esta estrategia.

La estrategia en estrella usa un cable individual desde un punto de concentración hasta cada uno de los puntos requeridos. Este es el método apropiado para la topología Estrella. También puede ser usado en las topologías Bus y Anillo como se muestra en la figura 3.5. En el caso de la topología Bus, el Bus es muy pequeño y reside en el punto de concentración; los cables que se

tienden hasta los dispositivos son relativamente largos.



a. Bus Using Star Wiring



b. Ring Using Star Wiring

FIGURE 3-5. Bus and Ring Topologies Using Star Wiring

En el caso de la topología Anillo, el anillo se deforma de manera que cada enlace del anillo se encorve a través del punto de concentración. Normalmente, este *Layout* es usado por separado en cada piso de un edificio. Al punto de concentración se le denomina "armario de cableado" (Wiring Closet). Las conexiones entre los diferentes pisos

de un edificio se hace enlazando los armarios de conexiones. Este tipo de *Layout* es usado muy a menudo para soportar la instalación de teléfonos en un edificio de oficinas, y cada vez más se usa para redes locales.

TABLE 3.8 Classes of Local Networks

Characteristic	Local Area Network	High Speed Local Network	Circuit-switched Local Network
Transmission medium	Twisted pair, coaxial (both), fiber	CATV coaxial	Twisted pair
Topology	Bus, tree, ring	Bus	Star
Transmission speed	1–20 Mbps	50 Mbps	9.6–64 kbps
Maximum distance	25 km	1 km	1 km
Switching technique	Packet	Packet	Circuit
Number of devices supported	100's–1000's	10's	100's–1000's
Attachment cost	\$500–\$5000	\$40,000–\$50,000	\$250–\$1000

Aunque la estrategia de *Layout* en estrella es muy adecuada para las topologías Estrella, para las de Bus y Anillo no lo es tanto. Su mayor desventaja es que para estas topologías la estrategia en Estrella requiere más cable que la lineal, incrementando así el coste y la aglomeración de cable. Por esta razón esta estrategia es poco usada en redes locales de cable coaxial ó de fibra óptica. No obstante, puede resultar conveniente para redes locales de par trenzado, donde el coste es mucho menor.

Algunas de las ventajas de la estrategia en Estrella son:

- 1.- Se acomodan al cableado existente en el edificio.
- 2.- El sistema puede ser fácilmente expandible. Sólo habría que añadir nuevos cables a la red conectandolos en el armario de cableado.
- 3.- La prestación de servicios y el mantenimiento es más sencillo. El diagnóstico de problemas puede llevarse a cabo desde los puntos centralizados. Los fallos pueden ser fácilmente aislados desconectando cables de la red.

3.4

CLASES DE REDES LOCALES.

Esta sección presenta la clasificación en tres categorías de las redes locales: las redes de área local (LAN), las redes locales de alta velocidad (HSLN) y las redes locales de *Circuit Switching*. La tabla 3.8 resume sus características más representativas. Como en toda clasificación, ésta fué hecha en base a unos criterios de clasificación. Estos fueron tres, y basados en los siguientes campos:

- * Tecnología: La arquitectura y diseño de las tres clases difieren entre sí de forma significativa.

Esto se observa en áreas como el rendimiento, protocolos de comunicación, técnicas de *Switching* (conmutación), interfaces de Hardware /Software, medio de transmisión y topologías.

- * Aplicaciones: Aunque hay un cierto solapamiento, las tres clases de redes locales han sido desarrolladas independientemente para satisfacer una serie de requerimientos.
- * Estandars: Los protocolos de comunicación para LAN y HLSN han sido desarrollados separadamente.

Redes de área local (LAN):

El término red de área local (LAN) es normalmente usado para referirse a una red local de propósito general, la cual sirve a una gran variedad de dispositivos en un área extensa. Las LANs "minis", ordenadores centrales, terminales, y periféricos. En muchos estos casos estas redes no transportan solo datos, también voz, video, y gráficos. Un tipo común de LAN es un Bus ó Arbol usando cable coaxial. Una alternativa podría ser un anillo con cable coaxial, par trenzado ó incluso fibra óptica. La velocidad de transmisión en las LANs (1-20 Mbps) es lo suficientemente alta para satisfacer la mayoría de las necesidades y suministrar capacidad suficiente para permitir que se enganchen a ella un gran número de dispositivos.

Una subcategoría de las LANs son las redes de bajo

coste dirigidas a los microcomputadores y periféricos baratos. Este es el caso de los ordenadores personales. Estas redes tienen una velocidad de 1 Mbps ó menos, y usan normalmente par trenzado. Debido a su bajo coste, el auge de los ordenadores personales, es el tipo de red local predominante hoy en día.

La LAN es probablemente la mejor elección cuando se trata de conectar una gran variedad de dispositivos con tráfico mixto.

Los estándares actuales para LANs han sido desarrollados por un comité del Instituto de Ingenieros Electrónicos y Eléctricos, que es conocido como el comité IEEE 802.

Redes locales de alta velocidad (HSLN):

Las redes locales de alta velocidad (HSLN) han sido diseñadas para proveer una alta transparencia punto a punto entre dispositivos caros de alta velocidad como ordenadores centrales y dispositivos de almacenamiento masivo de datos.

Hasta hace poco los trabajos sobre HSLNs se centraban en la topología Bus con cable coaxial tipo CATV. Se pueden alcanzar velocidades muy altas (del orden de 50 Mbps), pero tanto la distancia como el número de dispositivos es limitado. Un trabajo más reciente ha estudiado los Anillos de fibra óptica, en los cuales se han alcanzado velocidades de 80 a 100 Mbps.

La HSLN es normalmente encontrada en las salas de

ordenadores. Su principal función es proporcionar conexiones de E/S entre un número determinado de dispositivos. Debido al alto coste del sistema de HSLN, no son normalmente rentables para microcomputadoras, minicomputadoras y periféricos baratos.

Los estándares para los HSLNs han sido desarrollados por un comité financiado por el Instituto Americano de Standards (ANSI), conocido como el comité **ANS X3T9.5**.

Redes locales de Circuit - Switching:

En contraste con las LANs y HSLNs, los cuales usan *Packet Switching*, tenemos otra opción de red local que usan *Circuit Switching*. Normalmente este tipo de redes locales tienen una topología en Estrella ó en Estrella jerárquica. En esta última, podemos utilizar enlaces de alta velocidad como son el cable coaxial ó la fibra óptica, para unir interruptores periféricos al Switch central. Las velocidades a las estaciones individuales son bajas (≤ 64 Kbps), pero el ancho de banda está garantizado y no hay retardo en la red una vez la conexión esté hecha.

Una forma de red local de *Circuit Switching* es la *Private Branch Exchange* (PBX). Se trata de un diseño de conmutador para manejar tanto conexiones de datos como de voz. Aunque el poder de estos sistemas es su soporte para teléfonos, son también adecuados para el tráfico de datos entre las terminales y el ordenador principal. Otra forma es el conmutador de datos digitales. En esta modalidad los

dispositivos han sido diseñados para manejar sólo datos, no voz, y son en general menos costosos que sus compatibles en PBX.

La elección del tipo de red:

Como los tipos de redes locales se diferencian, al menos en parte, por el medio de transmisión y la topología, las observaciones previas pueden ser aplicadas aquí. En general, la elección del tipo de red local es una media entre las necesidades y el coste.

Para aplicaciones que necesiten una transparencia alta y frecuente entre dispositivos caros, las HSLNs controlan el mercado. Aunque su coste es alto (\$40.000 a \$50.000), eso sólo supone una porción del coste de los ordenadores centrales conectados con ella. En el futuro (como veremos más adelante), las LANs de banda ancha proporcionarán servicios de alta velocidad, y por tanto serán competidoras directas de las HSLNs.

Para las restantes aplicaciones, la elección está entre las redes locales de *Circuit Switching* y las LANs. Ambas pueden manejar una gran variedad de dispositivos. Normalmente las redes locales de *Circuit Switching* tienen una velocidad limitada de 64 Kbps para cada conexión. No obstante, esta velocidad es típica en los dispositivos que se conectan a las LANs. Sólo requieren velocidades mayores en ciertos casos como el uso de gráficos de alta velocidad ó la necesidad de soportar un gran tráfico entre "minis".

PARTE II

REDES DE AREA LOCAL: TOPOLOGIA Y MEDIOS DE TRANSMISION

Las redes de área local (LANs) son el tipo de red de mayor propósito general de los tres. Su uso se extiende desde los pequeños y baratos sistemas de ordenadores personales, hasta los sistemas de cable coaxial de banda ancha que recorren las pequeñas ciudades soportando una gran gama de dispositivos.

En este capítulo examinaremos en detalle las topologías y medios de transmisión en las LANs. Dejaremos para el capítulo 5 los controles de acceso al medio. No hay que olvidar que estas tres son las principales características de las redes de área local.

TOPOLOGIA BUS/ARBOL.

Características de las LANS de Bus/Arbol:

De las topologías estudiadas en el capítulo anterior, sólo la Bus/Arbol es un medio multipunto. Esto es, hay más de dos dispositivos conectados al medio, capaces de transmitir a través de él.

El funcionamiento de este tipo de LAN puede resumirse brevemente. Como muchos dispositivos comparten un sólo camino de datos, sólo uno puede transmitir cada vez. Una estación normalmente transite paquetes de información con la dirección de destino. El paquete se propaga por el medio llegando a todas las estaciones, y la estación de destino copia los paquetes al pasar.

Existen dos técnicas de transmisión usadas en LANS: banda base (Baseband) y banda ancha (Broadband). La banda base usa señal digital y podemos usar tanto par trenzado como cable coaxial. La banda ancha usa señal analógica de radiofrecuencia (RF) y cable coaxial. Algunas de las diferencias entre ellas se resumen en la tabla 4.1. Hay también otra variedad llamada "banda ancha de canal único", que tiene las características de señal de la banda base y algunas restricciones propias de la banda base.

La naturaleza multipunto de la topología Bus/Arbol provoca problemas considerables. El primero es determinar

que estación transmite en cada momento.

TABLE 4.1 Bus/Tree Transmission Techniques

Baseband	Broadband
Digital signaling	Analog signaling (requires RF modem)
Entire bandwidth consumed by signal— no FDM	FDM possible—multiple data channels, video, audio
Bidirectional	Unidirectional
Bus topology	Bus or tree topology
Distance: up to a few kilometers	Distance: up to tens of kilometers

En enlaces punto a punto (sólo dos dispositivos en el medio), resulta tarea fácil; si la línea es *Full-Duplex*, sólo se necesita un mecanismo que asegure que las dos estaciones se turnen. Históricamente, la modalidad de acceso compartido más común ha sido la línea multienganche (Multidrop), en donde el acceso es determinado mediante "llamadas" (Encuestas) ó "Polling" desde una estación de control. Esta estación puede enviar datos a cualquier otra estación, ó puede realizar una llamada (Poll) a una estación determinada en espera de respuesta. Es método, no obstante, niega algunas de las ventajas de los sistemas distribuidos y es de difícil manejo para comunicaciones entre dos estaciones no controladas. Como ya adelantamos, en el capítulo 5 trataremos una serie de estrategias distribuidas llamadas protocolos de control de acceso al medio para las topologías Bus y Arbol.

El segundo problema tiene que ver con el "balanceo"

(equilibrar) de la señal. Cuando dos dispositivos intercambian datos, la fuerza de la señal debe ser ajustada para que esté dentro de ciertos límites. La señal debe ser lo suficientemente fuerte como para llegar al receptor, después de la atenuación del medio, con una fuerza mínima exigida por éste. También debe ser lo suficientemente fuerte para mantener una relación de ruido adecuada. Por otro lado, no debe ser tan fuerte que sobrecargue los circuitos del transmisor, lo que haría surgir armónicos y falsas señales (parásitas). Aunque muy fácil para enlaces punto a punto, el balanceo de la señal no es tarea fácil en líneas multiacceso. Si cada dispositivo puede comunicarse con cualquier otro dispositivo, el balanceo debe de hacerse para cada permutación de estaciones, tomándolas de dos en dos. Para n estaciones hay $n(n-1)$ permutaciones. Así, para un sistema de 200 estaciones (que no es un sistema particularmente grande), habría que satisfacer 39.800 condiciones de fuerza de señales simultáneamente. Si las distancias entre los dispositivos son del orden de decenas o miles de metros, resulta una tarea imposible excepto para redes pequeñas. El sistema de señales de radiofrecuencia (RF), el problema es compuesto debido a la posibilidad de interferencias en la señal de RF. La solución es dividir el medio en segmentos, en los que es posible un buen balanceo, usando entre ellos amplificadores o repetidores.

Sistemas de banda base:

Las características principales de los sistemas de banda base se listan en la tabla 4.1. Como ya se dijo, las LANs de banda base utilizan señales digitales. (Este es un uso de la palabra "banda base" (Baseband), el cual ha sido aceptado en los círculos de redes locales. En general, el término se refiere a la transmisión de señales analógicas o digitales en su forma original, sin modular). Las señales digitales son insertadas en la línea como pulsos de voltaje (tensión), usando normalmente la codificación Manchester ó Manchester diferencial. se usa todo el espectro de frecuencias del medio; por lo tanto no podemos usar la FDM. La transmisión es bidireccional. Esto quiere decir que cualquier señal insertada en el medio, se propagará en ambas direcciones hasta los extremos en donde es absorbida (figura 4.1a). El uso de señales digitales, exige una topología Bus, pues al contrario que las señales analógicas, las digitales encuentran dificultad en atravesar los divisores y juntas necesarias en una topología Arbol. La distancia en este sistema se limita a un kilómetro como mucho. Esta limitación se debe a la atenuación que sufre la señal, lo cual se acentua a altas frecuencias, causando el deterioro de los pulsos y haciendo que no sea práctico este sistema para grandes distancias.

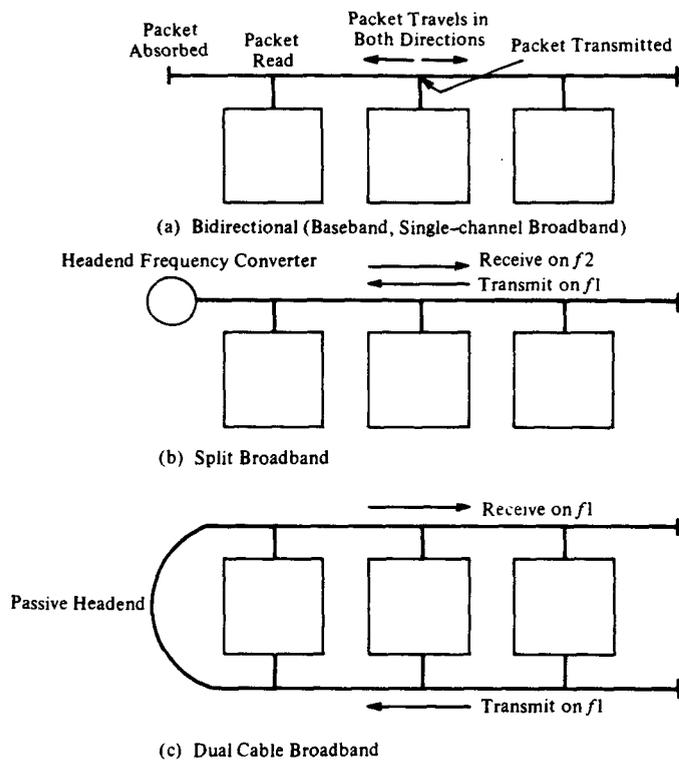


FIGURE 4-1. Baseband and Broadband Transmission Techniques

Banda base coaxial:

La red de área local más conocida con topología Bus, usa cable coaxial. Vamos a centrarnos en estos sistemas. Mientras no se indique lo contrario, estaremos hablando del sistema *Ethernet* y el estandar (casi idéntico a él) de **IEEE**.

La mayoría de los sistemas de banda base, usan cable coaxial de 50 Ohm. en vez del **CATV** de 75 Ohm. Estos valores se refieren a la impedancia del cable. Esta impedancia determina el voltaje que debe ser aplicado al

cable para lograr una señal con una determinada fuerza. Para señales digitales, el cable de 50 Ohm. sufre menos reflexiones al insertarle las capacidades de las derivaciones (Taps), y proporciona la mejor inmunidad al ruido electromagnético a bajas frecuencias. La LAN de Bus con banda base coaxial más simple consiste en un cable coaxial sin ramificar, con resistencias terminales en cada extremo. El valor de estas resistencias es fijado al mismo que el cable; ésto previene la reflexión absorbiendo cualquier señal en el cable.

Como todo sistema de transmisión, existe una serie de consideraciones a nivel de ingeniería, que incluyen la velocidad de datos, la longitud del cable, el número de derivaciones (ó tomas), y las características del transmisor y del receptor. Por ejemplo, cuanto menor sea el rango de velocidades, mayor puede ser la longitud del cable. Esto es debido a lo siguiente: Cuando la señal es transmitida a través de un medio de comunicación, la integridad de la señal sufre atenuación, ruido y otros deterioros. Cuanto mayor es la distancia de propagación, mayores son estos efectos, incrementándose el riesgo de error. A velocidades bajas, un pulso individual de una señal digital dura más (durante más tiempo, más longitud) y puede ser recuperado más fácilmente en presencia de ruidos que a grandes velocidades donde los pulsos son más cortos.

Con lo anterior en mente, vamos a analizar un ejemplo

ilustrativo. La especificación *Ethernet* y el standard original de **IEEE**, especifican el uso del cable coaxial de 50 Ohm. y 0.4 pulgadas de diámetro, y una velocidad de 10Mbps. Con estos parámetros, la longitud máxima del cable es de 500m. Las estaciones se conectan al cable por medio de "tomas" (derivaciones), con una distancia entre ellas múltiplo de 2.5 m; ésto es para asegurar que las reflexiones de tomas adyacentes no se sumen en fase. Se permiten un máximo de 100 estaciones. En la jerga del **IEEE**, este sistema se denomina "10 base 5". Los primeros dos dígitos indican la velocidad en mega bits por segundo; las cuatro letras son la abreviatura del medio usado (Baseband); y el último dígito es la máxima longitud del cable en cientos de metros.

TABLE 4.2 IEEE Specifications for 10-Mbps Baseband Coaxial Bus Local Networks

Parameter	10base5	10base2
Data Rate	10 Mbps	10 Mbps
Maximum Segment Length	500 m	200 m
Network Span	2500 m	1000 m
Nodes per Segment	100	30
Node Spacing	2.5 m	0.5 m
Cable Diameter	0.4 in	0.25 in

Para proporcionar sistemas más económicos para redes locales de ordenadores personales, el **IEEE** desarrolló despues su especificación "10 base 2". La tabla 4.2

compara este sistema, apodado "Cheapernet" (red barata), con la especificación "10 base 5". La diferencia principal es el uso de un cable más delgado (0.25 pulgadas), como el utilizado en las casas particulares. Por otro lado el cable delgado sufre más atenuación y resiste peor el ruido. Por lo tanto es capaz de soportar menos tomas en menos distancia.

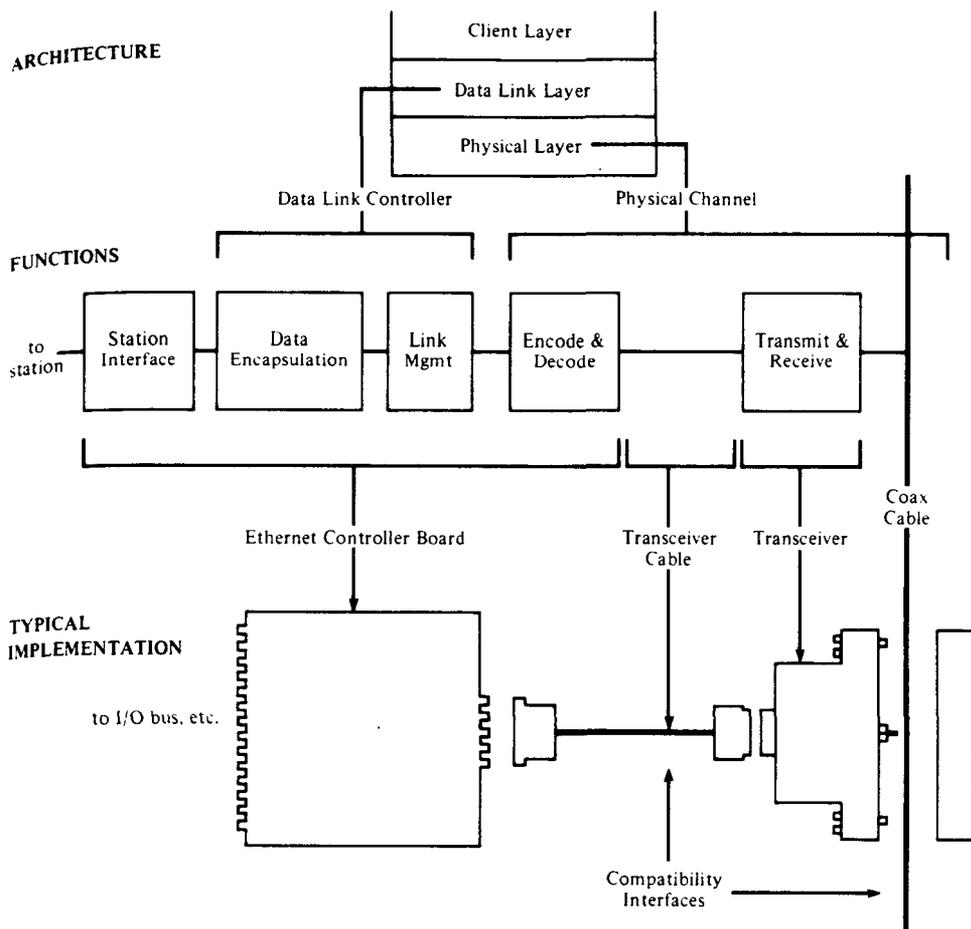


FIGURE 4-2. Ethernet Architecture and Typical Implementation

La figura 4.2, muestra los componentes principales de la especificación *Ethernet* y su función. Los componentes principales son:

- * Transceptor (Transceiver).
- * Cable de transceptor.
- * Controlador (Controller).
- * Cable coaxial de 50 Ohm.
- * Extremos del cable coaxial. (Terminadores).

El transceptor, se conecta (deriva) mediante una toma de cable coaxial. El transmite señales desde la estación al cable y viceversa. Tiene también la electrónica necesaria para reconocer la presencia de una señal en el cable y para reconocer la colisión entre dos señales. Esta última función se hace necesaria en la *Ethernet* y en la 802 debido al protocolo CSMA/CD que usan (lo veremos en el capítulo 5). Cualquier otra LAN con Bus de banda base con otro protocolo no necesitaría esta complejidad. El transceptor proporciona también un aislamiento a masa entre las señales provenientes de la estación y las del cable. Como dos masas locales pueden diferir en varios voltios, la conexión de la misma al cable puede hacer que aparezca una corriente que fluya a través del campo del cable, introduciendo ruido y un riesgo en la seguridad.

El cable de transceptor comprende dos pares trenzados (llamados par gemelo) y conecta al transceptor con el controlador, el cual contiene la mayor parte de la inteligencia requerida para comunicarse a través de la

LAN. Esta partición es arbitraria: toda la electrónica podría estar incluida en el extremo del tranceptor. No obstante esta distribución está justificada en el hecho de que la estación suele estar a alguna distancia del cable y que la toma de la misma en el cable puede estar en un lugar relativamente inaccesible. Por esto, la electrónica en la toma (derivación) suele ser lo más sencillo posible para reducir los costes de mantenimiento. Este cable proporciona la alimentación necesaria al tranceptor y pasa señales de datos entre éste y el controlador así como señales de control. Estas últimas incluyen una "señal de presencia de colisión" desde el transceptor al controlador. También se pueden tener otras señales. Por ejemplo, en el standard 802 se tiene una señal de "Isolate" y "Cease-To-Isolate", los cuales permiten al controlador habilitar y deshabilitar al transceptor.

El controlador es una implementación de todas las funciones (menos las que realiza el transceptor) necesarias para manejar el acceso al cable coaxial, con el fin de hacer posible el intercambio de paquetes entre el cable y la estación a la que está conectado. Profundizaremos más sobre este tema en el capítulo 5.

Finalmente, el sistema de transmisión consiste en un cable coaxial de 50 Ohm. y los terminadores (extremos). Los terminadores absorben las señales, evitando que haya reflexiones desde los extremos del Bus.

Estos cinco tipos de componentes son suficientes para

construir una LAN con Bus de banda base de un kilómetro de larga y unos cien equipos. En muchos casos, esto es suficiente, pero para necesidades mayores hace falta otro componente: el repetidor.

El repetidor se usa para aumentar la longitud de la red. Un repetidor consiste, en esencia, en dos transceptores unidos entre sí y conectados (cada uno) a dos segmentos diferentes de cable coaxial. Los repetidores pasan señales digitales en ambos sentidos, amplificándolas y regenerándolas a medida que van pasando. Es totalmente transparente para el resto del sistema, pues al no almacenar nada en ningún momento, no aísla en ningún modo un segmento de cable coaxial del otro. Así, si por ejemplo dos estaciones en segmentos diferentes requieren transmitir a la vez, los paquetes de cada una se interfieren unos con otros (colisionan). Para evitar interferencias multicaminos, sólo se permite un camino de segmentos y repetidores en cada camino entre dos estaciones, ampliando la longitud efectiva del cable a 2.5 kilómetros. La figura 4.3 es un ejemplo de sistema banda base con tres segmentos y dos repetidores.

Banda base con par trenzado:

Como señalamos en el capítulo 1, existe la necesidad de crear redes locales de bajo coste para conectar entre sí dispositivos baratos como los microcomputadores. Un excelente remedio es la LAN de banda base con par

trenzado. Este tipo de sistema soporta menos estaciones y a menores velocidades que las LAN con Bus de banda base, pero a mucho menor coste.

Los componentes del sistema son pocos y simples:

- * Bus de par trenzado.
- * Terminadores (a los extremos).
- * Interface de controlador.

Este último puede ser un simple interface de E/S estandar de dos cables ó un interface de comunicaciones. Normalmente, el estandar de capa física típica usada como interface es la RS-422. Este es un interface común y barato.

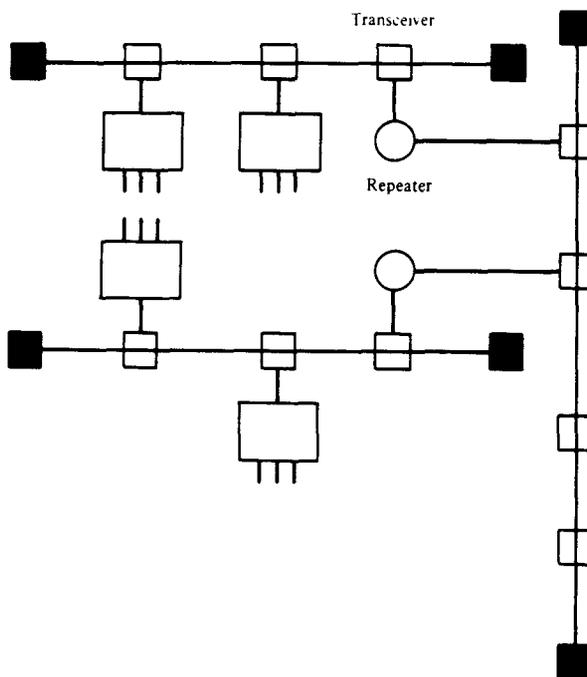


FIGURE 4-3. Baseband Configuration

Con una red de este tipo, podemos obtener unos parámetros del siguiente orden:

- * Longitud: hasta 1 Km.
- * Velocidad: hasta 1 Mbps.
- * Número de dispositivos: Decenas.

El par trenzado es un buen medio por muchas razones. Primero, tiene un coste menor que el cable coaxial, proporcionando casi la misma inmunidad al ruido. Segundo, virtualmente cualquiera puede realizar la instalación, lo cual se resume en tender el cable y conectar los controladores. Esta tarea requiere solamente un destornillador, unos alicates y se asemeja a la conexión de altavoces de alta fidelidad.

Sistemas de banda ancha:

Como el término "banda base" el término "banda ancha" (Broadband) ha sido adaptado por el círculo de las redes locales de el mundo de las telecomunicaciones, con un cambio de significado. En general, banda ancha (Broadband) se refiere a cualquier canal que tenga un ancho de banda mayor al canal de voz (4 KHz). En círculos de redes locales, el término se reserva para los cables coaxiales en los que se usa una señal analógica. También se aplica cuando se puede tener una multiplexación por división en frecuencia (FDM) en el cable. Nosotros nos referiremos a sistemas capaces de FDM cuando usemos el término banda ancha. Los sistemas destinados a transportar sólo una

señal analógica los llamaremos "banda ancha de canal único" (Single Channel Broadband).

Banda ancha con FDM:

En la tabla 4.1 podemos ver las características más importantes de los sistemas de banda ancha. Como antes mencionamos, el término ancho de banda implica el uso de señal analógica. Por lo tanto el FDM es posible: el espectro de frecuencias del cable es dividido en canales ó secciones del ancho de banda. Canales separados pueden soportar tráfico de datos, señales de TV y de radio. Los componentes de banda ancha permiten realizar las operaciones de división (Splitting) y de unión (Joining); por lo que tanto la topología Bus como la de Arbol, son adecuadas. Con este sistema se pueden llegar a distancias del orden de las decenas de kilómetros, debido a que las señales analógicas que transportan datos digitales se propagan a más distancia antes de que el ruido y la atenuación dañen los datos.

La figura 4.4 muestra un típico sistema de banda ancha. Como sucedía en sistemas de banda base, las estaciones se enganchan al cable por medio de una derivación (Tap). A diferencia con los banda base, los sistemas de banda ancha tienen un medio unidireccional; las señales insertadas en el medio (cable) pueden propagarse sólo en una dirección. La principal razón para ello es la impracticabilidad de construir amplificadores

que pasen señales de una frecuencia en ambas direcciones. Esta unidireccionalidad hace que sólo una estación que esté por debajo, en el curso de la corriente de datos, de la estación transmisora puede recibir el mensaje.

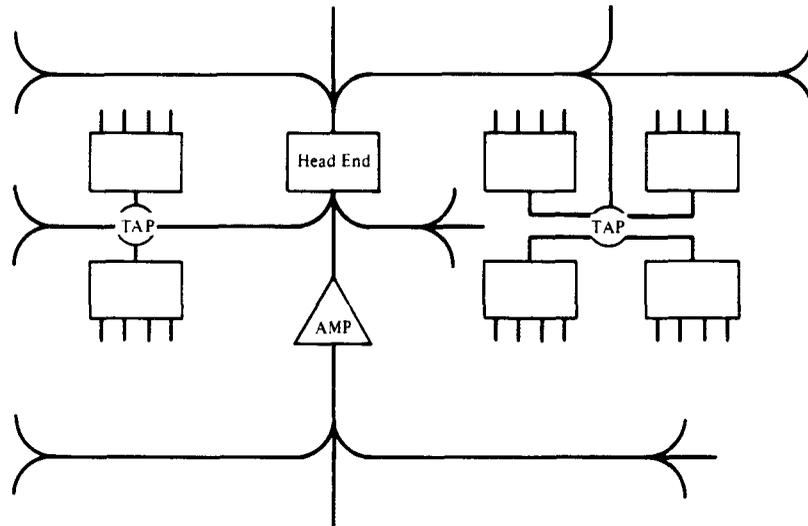


FIGURE 4-4. Broadband Configuration

¿Cómo se logra pues una conectividad total?.

Evidentemente, se necesitan dos caminos para los datos. Estos caminos se unen en un punto de la red conocido como "Head-end". Para la topología Bus, este punto es simplemente uno de los extremos del Bus. Todas las estaciones transmiten por un camino hacia el *Head-end*, al que se denomina "de llegada" (Inbound). Las señales recibidas en el *Head-end* son entonces propagadas a lo largo de un segundo camino desde el *Head-end*, denominado "de salida" (Outbound). Todas las estaciones emiten en el

camino *Inbound* y reciben en el *Outbound*. Físicamente hay dos configuraciones para implementar los caminos de entrada y de salida (figura 4.1b y c). En una configuración de cable dual (dual-cable), estos caminos son cables separados, donde el *Head-end* es un simple conector pasivo entre los dos. Las estaciones transmiten y reciben en la misma frecuencia.

Por el contrario, en la configuración "Split" (división ó dividida) los caminos de entrada y de salida son bandas de diferentes frecuencias en el mismo cable. Los amplificadores "bidireccionales" pasan las bajas frecuencias de los *Inbounds* y las altas de los *Outbounds*. (Téngase en cuenta que éste es un significado diferente de la palabra "bidireccional"). Entre las bandas de entrada y de salida hay una banda de frecuencias de protección. Esta banda no transporta señal alguna y separa las señales de las otras dos bandas de frecuencia. El *Head-end* contiene un dispositivo, conocido como "traductor de frecuencias", para traducir las frecuencias de entrada en frecuencias de salida.

Este dispositivo puede ser analógico ó digital. Sí es analógico, simplemente traduce las señales a una nueva frecuencia y las retransmite. Sí es digital, reconstruye los datos digitales de la señal analógica y entonces retransmite la señal limpia en la nueva frecuencia.

Los sistemas "Split" se caracterizan por la localización en frecuencia de los dos caminos, como se

muestra en la tabla 4.3. El "Subsplit" es normalmente usado por la industria CATV (Antenas comunitarias de televisión) para la distribución de señales de TV en áreas metropolitanas.

TABLE 4.3 Common Cable Frequency Splits

Format	Inbound Frequency Band	Outbound Frequency Band	Maximum Two-way Bandwidth
Subsplit	5 to 30 MHz	54 to 400 MHz	25 MHz
Midsplit	5 to 116 MHz	168 to 400 MHz	111 MHz
Highsplit	5 to 174 MHz	232 to 400 MHz	169 MHz
Dual Cable	40 to 400 MHz	40 to 400 MHz	360 MHz

Proporciona la vía más fácil de convertir (remozar) sistemas de cable unidireccionales en sistemas que operen en ambas direcciones. El *Subsplit* tiene una limitada utilización en **LANS** debido a su pequeño ancho de banda (sólo 25 MHz). El "Midsplit" es más adecuado para las **LANS**, ya que proporciona una distribución más equitativa de su ancho de banda. No obstante, el *Midsplit* fué desarrollado en un momento en el que el espectro práctico del cable CATV era de 300 MHz, mientras que ahora se obtienen espectros superiores a los 400 MHz. Por ello, una especificación "Highsplit" ha sido desarrollada para lograr un ancho de banda de dos direcciones máximo, en sistemas *Split*.

Las diferencias entre los sistemas *Split* y *Dual* son mínimas. El sistema *Midsplit* es especialmente válido para edificios en los que ya exista una instalación de un sólo

cable. Es más, el sistema ya instalado resulta entre un 10% y un 15% más barato que el sistema *Dual* (dos cables). Por otro lado, este último sistema tiene una capacidad casi del doble que el *Midsplit*, no necesita traductores de frecuencia en los *Head-end*.

Los sistemas *Broadband* utilizan componentes estandar CATV, incluyendo el cable coaxia de 75 Ohm. Todos los extremos son acoplados a una resistencia de 75 Ohm. (terminador) para absorber las señales. Estos sistemas pueden llegar a longitudes de decenas de kilómetros de radio desde el *Head-end* y a cientos ó incluso miles de dispositivos. Los componentes principales del sistema son:

- * Cable.
- * Terminadores.
- * Amplificadores.
- * Acopladores (conectores) direccionales.
- * Controladores.

Los cables usados en las redes de *Broadband* son de tres tipos. El "cable tronco" (Trunk cable) suele ser la espina dorsal de las grandes LANs. Tienen un diámetro de 0.5 a 1.0 pulgadas, con una atenuación de 0.7 a 1.2 dB por cada 100 pies de cable a 300 MHz. Normalmente, este cable está encapsulado en una coraza rígida de aluminio, y suele ser de longitudes que oscilan entre unos pocos kilómetros y decenas de kilómetros. Los "cables de distribución" (distribution cables), se usan en distancias menores y para formar las ramificaciones. Su diámetro oscila entre

0.4 y 0.5 pulgadas, con una atenuación de 1.2 a 2.0 dB cada 100 pies de cable, y puede ser semirígido ó rígido. Y por último los "cables a los terminales" (drop cables), son cortos y se usan para conectar las estaciones a la LAN. su diámetro es de 0.25 pulgadas, son flexibles y con una atenuación de 4 a 6 dB por cada 100 pies de cable.

Los amplificadores pueden ser usados en los cables tronco y en los de distribución para compensar la atenuación. Estos amplificadores deben tener un "Slope" (control) que tenga en cuenta las variaciones de la atenuación en función de la frecuencia; en bajas frecuencias se necesita menos amplificación. Para los sistemas tipo *Split*, los amplificadores deben ser bidireccionales, pasando y amplificando señales de frecuencia bajas en una dirección y de altas frecuencias en la otra.

Los acopladores direccionales (ó Taps) facilitan un modo de dividir una entrada en dos salidas y combinar dos entradas en una sólo salida. Los "divisores" (Splitters), usados para ramificar el cable, proporcionan aproximadamente la misma atenuación a lo largo de las ramas. Las tomas ó derivaciones (Taps) usadas para conectar el "cable a los terminales" y por tanto éstas a la LAN, introducen más atenuación en estos cables. La figura 4.5 ilustra estos conceptos.

Finalmente, como en los sistemas *Baseband*, los controladores son necesarios para proporcionar el servicio

básico de la LAN.

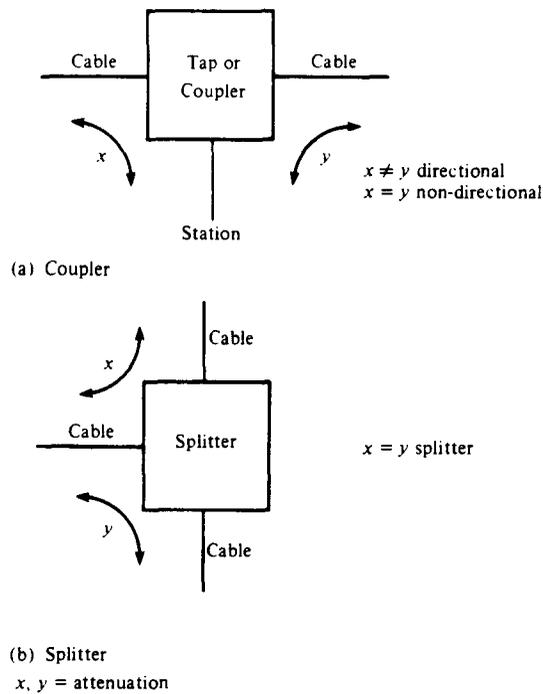


FIGURE 4-5. Directional Couplers and Splitters

Como se mencionó con anterioridad, una LAN de *Broadband* puede ser usada para transportar muchos canales, algunos para señales analógicas, como el video y la voz, y otros digitales. Normalmente, los canales digitales pueden alcanzar velocidades entre los 0.5 y 2 bps/Hz. La figura 4.6 muestra un ejemplo de distribución del espectro de frecuencias de un cable de 350 MHz.

En un cable *Broadband* existen tres tipos de servicio de transferencia de datos: asignado (Dedicated), conmutado, y acceso múltiple (figura 4.7). Para el servicio "Dedicated", una pequeña porción del ancho de

banda del cable es reservado para el uso exclusivo de los dos dispositivos.

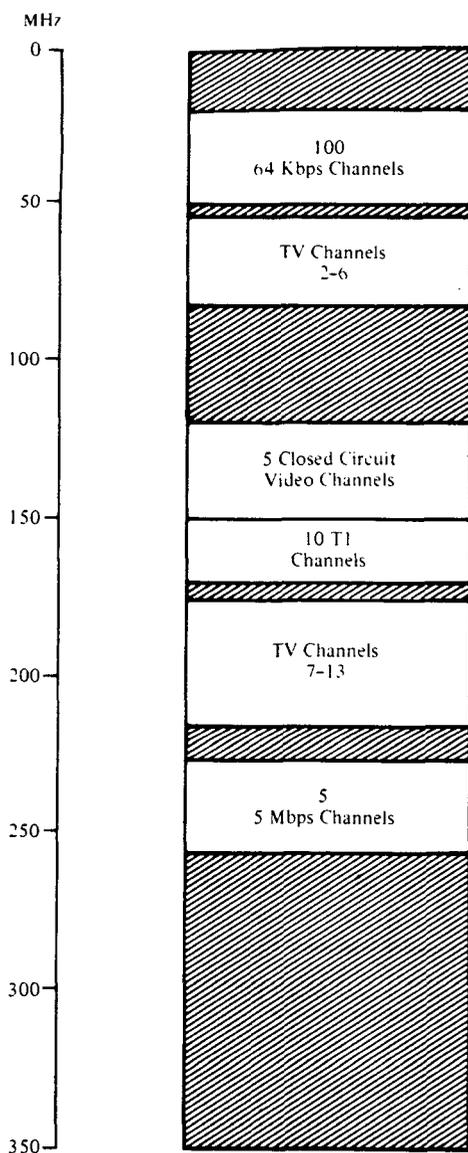


FIGURE 4-6. Dual-Cable Broadband Spectrum Allocation

No se necesitan protocolos especiales. Ambos dispositivos se conectan al cable a través de un modem; ambos modems están sintonizados a la misma frecuencia.

Este servicio podría ser usado cuando se espera un tráfico denso en un determinado diseño. Se pueden alcanzar velocidades de 20 Mbps.

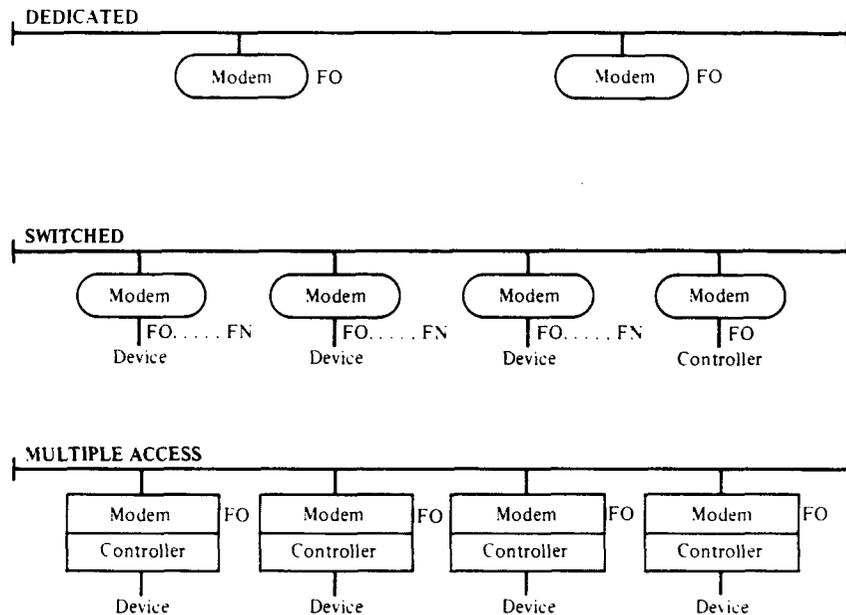


FIGURE 4-7. Broadband Data Transfer Services

La técnica "conmutado" requiere el uso de varias bandas de frecuencias. Los dispositivos son conectados a la red a través de "modems de frecuencia ágil" (Frequency agile modem), capaces de cambiar su frecuencia electrónicamente. Inicialmente, todos los dispositivos, junto a sus controladores, son ajustados a la misma frecuencia. Una estación que desee establecer una conexión, envía una solicitud al controlador, el cual asigna una frecuencia disponible a ambos dispositivos e

indica a sus modems (mediante una señal) que sintonicen a esa frecuencia. Como el coste de modems de frecuencia ágil se dispara con el aumento de la velocidad de transmisión, se usan unas velocidades de 56 Kbps ó menores.

Por último, el servicio de "acceso múltiple", permite que un cierto número de dispositivos enganchados, sean soportados a la misma frecuencia. Esto proporciona una comunicación en igualdad, entre muchos dispositivos, que es el primer objetivo de las redes locales. Como es lógico (y como pasaba en Baseband), es necesario algún protocolo de control de acceso al medio. Estos protocolos los trataremos en el capítulo 5.

Sistemas de banda ancha de canal único:

Una forma abreviada de *Broadband*, conocida como *Broadband de canal único ó banda portadora* (Carrierband), es aquella en la cual el espectro entero del cable se dedica a un sólo camino de transmisión de señales analógicas. Como veremos, esta técnica es especialmente aplicable a redes de alta velocidad (HSLNs). Aunque también ha sido propuesta para su uso en LANs, y es parte del estandar 802 de IEEE.

En general, una LAN de *Broadband* de canal único tiene las siguientes características. Se usa una topología Bus para proporcionar una transmisión bidireccional. Por tanto, no puede haber amplificadores, y no son necesarios los *Head-ends*. Se usa alguna forma de FSK a bajas

frecuencias (unos pocos MHz). Esto constituye una ventaja, pues la atenuación es menor en frecuencias bajas.

Como el cable se dedica por entero a una tarea, no es necesario preocuparse de que el modem se ajuste a un ancho de banda estrecho. La energía puede propagarse sobre el espectro del cable. Como resultado la electrónica a usar es muy simple y barata. Esta modalidad de *Broadband* es comparable a la *Baseband* en prestaciones y coste.

Banda ancha por líneas de potencia:

Un sistema de bajo coste que puede competir con la banda base de par trenzado, es la red basada en la red de distribución de potencia. El medio de transmisión de esta red, es el sistema de distribución de potencia "AC" que se instala en cada hogar y oficina. En consecuencia este sistema no implica instalación de medio alguno.

El interface para el medio es un simple macho de dos ó tres clavijas. Normalmente, los datos son modulados en FSK en una estrecha banda a una frecuencia de 200 a 400 KHz. Esta señal no interfiere con la de 60 Hz (EE.UU.) de la distribución de potencia, y presenta un nivel de RF lo suficientemente bajo como para evitar interferencias con los equipos de oficina. Usando estas técnicas se pueden conseguir de 10 a 20 canales separados, con velocidades de hasta 9.600 bps.

Una de las ventajas principales de éste sistema es su portabilidad. Una estación de trabajo puede ser movida

dentro de la oficina, enchufándola mediante un controlador a la pared, e inmediatamente formará parte de la red.

Banda base versus banda ancha:

Hay espacio suficiente para ambas tecnologías en el campo de las redes locales. Los compradores potenciales, se enfrentan a decisiones más difíciles que ésta. La tabla 4.4 nos muestra los pros y los contras de ambas tecnologías. La *Baseband* tiene la ventaja de la sencillez, y en principio, de menor coste. La disposición de la trama de un cable *Baseband*; sólo hay cinco especificaciones que se refieren a la disposición del cable "tronco" en la especificación *Ethernet*. Un simple electricista es capaz de hacer el trabajo.

Las desventajas potenciales de la *Baseband*, incluyen las limitaciones en capacidad y distancia (desventajas que aparecen sólo si los requerimientos exceden esas limitaciones). También hay que tener en cuenta la masa. Como tenemos componentes de "DC" en el cable, podemos ponerlos todos a masa en un mismo sitio. Pero debemos tomar medidas para evitar shocks de potencia y efectos de antena.

La gran baza de la *Broadband* es su enorme capacidad; puede llevar una amplia gama de tráfico en un gran número de canales. Si usamos amplificadores, podemos alcanzar una cobertura realmente grande. Además, el sistema se basa en la conocida tecnología *CATV*, cuyos componentes son fiables

y fácilmente asequibles.

TABLE 4.4 Baseband versus Broadband

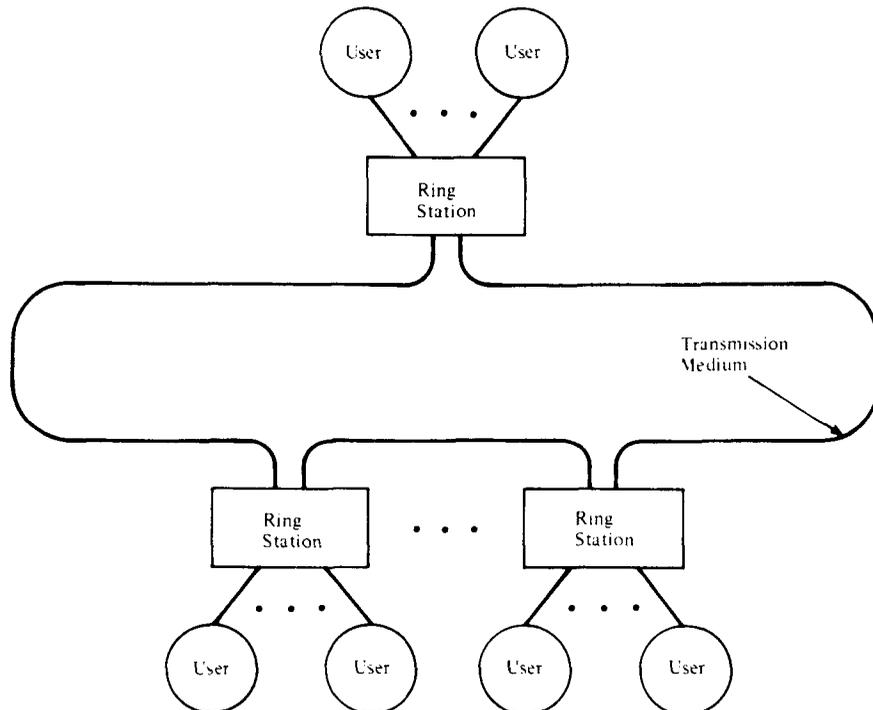
Advantages	Disadvantages
	<i>Baseband</i>
Cheaper—no modem Simpler technology Easy to install	Single channel Limited capacity Limited distance Grounding concerns
	<i>Broadband</i>
High capacity Multiple traffic types More flexible configurations Large area coverage Mature CATV technology	Modem cost Installation and maintenance complexity Doubled propagation delay

No obstante, los sistemas *Broadband* son más complejos de instalar y de mantener. El diseño de la disposición (Layout) debe incluir la selección del tipo de cable y del lugar y fijación de todos los amplificadores y tomas (Taps). El mantenimiento incluye unas revisiones periódicas y el alineamiento de todos los parámetros de la red. Este es un trabajo para ingenieros especializados en RF. Por último, en *Broadband*, el retardo de propagación entre dos estaciones es el doble que en *Baseband*. Reduciéndose así su eficiencia y rendimiento.

Como en cualquier otra elección de red, la selección de uno u otro sistema debe basarse en costos relativos y los beneficios. Así, es posible que algunas instalaciones tengan ambos tipos.

TOPOLOGIA ANILLO.**Descripción:**

El Anillo consiste en un número de repetidores, cada uno conectado a otros dos mediante enlaces de transmisión unidireccionales formando un camino cerrado (figura 4.8). Los datos se transfieren secuencialmente, bit a bit, a lo largo del Anillo de un repetidor al siguiente. Cada repetidor regenera y retransmite cada bit.

**FIGURE 4-8. Ring System**

Para que un Anillo opere como una red de comunicaciones, se necesitan tres funciones: inserción de los datos, recepción de datos, y alineación de datos. Estas funciones son realizadas por los repetidores. Cada repetidor, además de ser un elemento activo del Anillo, sirve como dispositivo de punto de anclaje para la inserción de datos.

Los datos se transmiten en paquetes, cada uno de los cuales contiene un campo de dirección de destino. A medida que un paquete circula por los repetidores, este campo es copiado para la estación conectada a ese repetidor. Si la estación reconoce la dirección, se copia el resto del paquete.

Para determinar como y cuando los paquetes son removidos del anillo ó insertados en él, hay varias estrategias.

Los repetidores realizan las funciones de inserción y recepción de datos de manera similar a las tomas (Taps), las cuales sirven de punto de anclaje en las topologías Bus ó Arbol. La eliminación de datos, no obstante, es más difícil en un anillo. En el Bus ó Arbol, las señales se insertan, se propagan hacia los terminales y son absorbidos por los terminadores (resistencias). Por lo tanto, poco despues de terminar la transmisión, el Bus ó Arbol está sin datos. Pero como el Anillo es un circuito cerrado, los datos circularían indefinidamente a no ser que fuesen eliminados. Un paquete puede ser eliminado por

el repetidor de la estación a la que va dirigido. También, cada paquete puede ser extraído por el repetidor que lo ha emitido, cuando el paquete haya completado un recorrido completo por el circuito. Esta última opción es mejor pues (1) permite una aceptación (reconocimiento) automática, y (2) por que permite el direccionamiento múltiple (compuesto \equiv Multicast): que consiste en enviar un mismo paquete a varias estaciones.

El repetidor pues, tiene dos funciones principales: (1) el contribuir al funcionamiento correcto del Anillo haciendo circular los datos, y (2) el proporcionar puntos de acceso para las estaciones enganchadas, para recibir y transmitir datos. Correspondiendo a estos dos propósitos, hay dos estados (figura 4.9): el estado de escucha y el de transmisión.

En el estado de escucha, cada bit recibido ha retransmitido con un pequeño retardo, necesario para que el repetidor realice las funciones necesarias. Lo ideal sería que el retardo fuese del orden de la duración de un bit. Las funciones que provocan este retardo son:

- * Rastrear (Scan) la cadena de bits mediante las plantillas pertinentes. La más importante es la dirección ó direcciones de los dispositivos. Otra plantilla (patrón), usada en la estrategia "Token" (que veremos más adelante), indica el permiso para transmitir. Por lo que vemos, el repetidor tiene que tener algún conocimiento a

cerca del formato del paquete.

- * Copiar cada bit que le llega y mandarlo a la estación correspondiente, mientras continua retransmitiendo cada bit. Esto se hará para que cada bit de cada paquete destinado a la estación engachada a ese repetidor.
- * Modificar un bit al tiempo que pasa. En ciertas estrategias de control, los bit deben ser modificados para, por ejemplo, indicar que el paquete ha sido copiado. Esto podría servir como señal de reconocimiento.

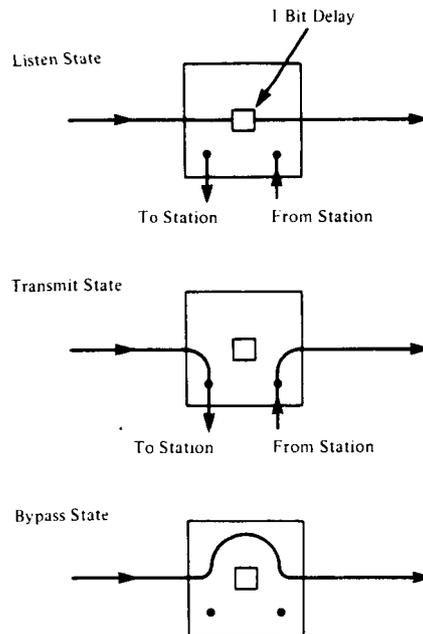


FIGURE 4-9. Ring Repeater States

Cuando la estación de un repetidor tiene datos que enviar y el repetidor, basándose en la estrategia del control, tiene permiso para enviar, el repetidor entra en el estado de transmisión. En él, el repetidor recibe datos de la estación y los retransmite por su línea de salida. Durante los periodos de transmisión, pueden aparecer bits en su línea de entrada. Hay dos posibilidades, en las cuales los bits son tratados de manera diferente:

- * Estos bits pueden formar parte del mismo paquete que todavía está enviando. Esto ocurre si la longitud (en bits) del anillo es menor que la del paquete. En este caso, el repetidor pasa de nuevo los bits a la estación, la cual los comprobará como modo de asentimiento.
- * En algunas estrategias de control, podemos tener más de un paquete circulando a la vez por el anillo. Si el repetidor recibe bits mientras transmite, recibe bits de un paquete que no introdujo él, lo almacenará para retransmitirlos más tarde.

Estos estados, escucha y transmisión, son suficientes para facilitar el funcionamiento correcto del anillo. Pero otro estado, el estado de derivación (desvío), es también útil. En este estado, se activa un relé de derivación, de manera que la señal se propaga a través del repetidor, sin más retardo que el introducido por el medio. Este relé de derivación, aporta dos

beneficios: (1) proporciona una solución parcial al problema de la fiabilidad, y (2) aumenta el rendimiento al eliminar el retardo en los repetidores de aquellas estaciones que no están activadas en la red en ese momento.

Beneficios del anillo:

Después de la publicación de libros y artículos en EE.UU. acerca de las LAN con topología Anillo, tenemos los primeros resultados en el aumento considerable de la producción de productos para este tipo de redes, encabezada en 1.985 por IBM y seguido por una serie de productos compatibles de otros vendedores (marcas).

Como en el Bus y el Arbol, el Anillo es una red multiacceso ó de acceso compartido (incluso el medio es en sí un conjunto de enlaces punto a punto). Sus ventajas van desde la capacidad de extenderse hasta el coste proporcional a su aplicación (crecimiento). Pero hay una serie de ventajas del Anillo que no las tienen otras topologías.

La mayor de estas ventajas es que el Anillo utiliza enlaces de comunicación punto a punto. Hay una serie de consecuencias de esto. Primero, la señal transmitida es regenerada en cada nodo, con lo que se pueden hacer coberturas a mayor distancia que en el bus de banda base. En las redes de banda ancha de Bus/Arbol puede cubrir unas distancias similares, pero la colocación de

amplificadores en cascada, puede provocar la pérdida de integridad de la señal en altas velocidades. Segundo, el Anillo puede utilizar fibra óptica la cual proporciona velocidades muy altas y unas características excelentes frente a las interferencias electromagnéticas (EMI). Por último, la electrónica (componentes) y mantenimiento de líneas punto a punto son más sencillas para las líneas multipunto.

Otro beneficio es que la falta de aislamiento y su remedio es más fácil en el Anillo que en otra topología.

Con el Anillo, el problema de la "dirección duplicada" es resuelto sencillamente. Si en un Bus ó Arbol, hay dos estaciones a las que accidentalmente se les han asignado la misma dirección, no hay una forma sencilla de evitarlo. Debemos incorporar un algoritmo relativamente complejo en el protocolo de la LAN. En un anillo, la primera estación con la dirección duplicada que encuentre el paquete, puede modificar un bit en señal de recibo. Las siguientes estaciones con la misma dirección puede así reconocer fácilmente el problema.

Por último, el Anillo tiene una capacidad de tratamiento potencial, superior a las redes LAN de Bus y Arbol.

Problemas potenciales del Anillo:

Los problemas potenciales del Anillo son, a primera vista, más obvios que los beneficios:

- 1.- Vulnerabilidad del cable: Una ruptura en cualquiera de los enlaces entre repetidores inhabilita la red entera hasta que el problema. El Anillo puede extenderse de manera muy amplia abarcando un edificio, pero es vulnerable en muchos puntos.
- 2.- Fallo de repetidor: Como con los enlaces, el fallo de un sólo repetidor hecha a bajo toda la red. En muchas redes es muy común que muchos nodos no estén operativos durante todo el tiempo, pero todos deben funcionar correctamente.
- 3.- Preambulación: Cuando falla un enlace ó un repetidor, debemos tener acceso a todas las habitaciones que contengan cables y repetidores, para localizar la avería, es decir se requiere la preambulación del Anillo.
- 4.- Problemas de instalación: Para instalar un nuevo repetidor con objeto de soportar nuevos dispositivos, debemos identificar dos repetidores, es decir, topológicamente adyacentes. Debe comprobarse (mediante la documentación de la red), que son verdaderamente adyacentes, y luego conectar los cables del nuevo repetidor uno a cada repetidor adyacente. Esto conlleva una serie de consecuencias no deseadas. La longitud del cable del repetidor

fuente varía, necesitando un reajuste (posiblemente). El cable viejo, si no se elimina se va acumulando. Y además, la geometría del Anillo puede llegar a ser muy irregular, exacerbando el problema de la preambulación.

- 5.- Limitación de tamaño: Existe una limitación práctica en el número de estaciones que podemos enganchar en un Anillo. Este límite está marcado por los problemas de fiabilidad y de mantenimiento citados antes, el "Timing Jitter" del que hablaremos a continuación, y el retardo que se acumula al tener muchos repetidores. Un límite de unos pocos cientos de estaciones es razonable.
- 6.- Inicialización y recuperación: Para evitar que un nodo del Anillo actúe como controlador (perdiéndose así los beneficios del control distribuido), se necesita una estrategia para asegurar la cooperación de todas las estaciones cuando se necesite una inicialización o una recuperación. Esta necesidad se tiene, por ejemplo, cuando un paquete es mutilado por un error de línea transitorio; en ese caso, ningún repetidor asume la responsabilidad de retirar el paquete.
- 7.- Timing Jitter: Este es un problema delicado que tiene que ver con la sincronización de una señal

en una red distribuida. Lo veremos a continuación.

Los problemas 1 y 2 son problemas de fiabilidad. Estos dos problemas junto con el 3, 4 y 5 pueden ser mejorados, refinando la arquitectura del Anillo, como veremos en la siguiente sección. El problema 6, en cambio, es un problema de Software. En cuanto al problema 7, lo trataremos a continuación.

Timing Jitter (inestabilidad de la base de tiempos):

En una LAN en Anillo de cable coaxial ó par trenzado, se usan normalmente señales digitales con codificación bifásica, usualmente **Diferential Manchester**. A la vez que los datos circulan por el Anillo, cada receptor debe recomponer los datos de la señal recibida. Para hacer ésto, el receptor debe saber los tiempos de comienzo y de finalización de cada bit, de modo que pueda muestrear de forma apropiada la señal recibida. Esto requiere que todos los repetidores deben estar sincronizados. Recordando lo dicho en el capítulo 2, los códigos bifásicos son códigos autosincronizados; la señal incluye una transmisión en medio de cada bit. De hay que los repetidores reconstruyan el sincronismo así como los datos de la señal recibida. Esta reconstrucción del reloj, se desvia, de manera ocasional, de la transición central de cada bit por muchas razones, incluyendo la aparición de ruido en la transmisión e imperfecciones en la circuitería del

receptor. La razón primordial, no obstante, es la distorsión por retardo. Esta distorsión por retardo está causada por el hecho de la velocidad de propagación de una señal a través de un medio guiado varía con la frecuencia. El efecto es que algunos de los componentes de la señal, un pulso, puede saltar de su posición y colocarse en la de otro pulso; esto se conoce como "Intersymbol Interference". La desviación de la reconstrucción del reloj de sincronismo, se conoce por "Timing Jitter" (ó inestabilidad de la base del tiempo).

A medida que cada repetidor recibe datos, va reconstruyendo el reloj por dos razones: primero conocer cuando debe muestrear la señal que le llega para reconstruir los datos, y segundo, para usar la sincronización (Clocking) para transmitir la señal con código **Diferential Manchester** al próximo repetidor. El repetidor da pues salida a una señal limpia y sin distorsiones. De todos modos, como el reloj es reconstruido a partir de la señal de entrada, el error de temporización no es eliminado. por lo tanto, la anchura de los bits puede variar de forma ocasional, a medida que la señal viaja por el anillo, y se acumule el "Timing Jitter". Este efecto acumulatorio del "Timing Jitter" es la causa de que varíe la longitud en bits del Anillo (Latency). No obstante, aunque la latencia (Latency) del Anillo permanezca constante, pueden perderse bits (no ser transmitidos) sí la latencia del Anillo disminuye ó

añadirse bits si ésta se incrementa.

Debido a esto, el "Timing Jitter" supone una limitación en el número de repetidores en un Anillo. Aunque esta limitación no puede ser superada por completo, se deben hacer los ajustes y medios necesarios para mejorarla; esto está ilustrado en la figura 4.10. Cada repetidor puede incluir un circuito cerrado de fase bloqueada. Este es un dispositivo que utiliza realimentación para minimizar la desviación (servo autocontrol) entre el tiempo de un bit y el siguiente. Pero, aunque el uso de este sistema reduce el *Timing Jitter*, existe todavía una cierta acumulación en el Anillo. Una medida suplementaria a tomar es incluir un *Buffer* en uno de los repetidores, normalmente designado como el repetidor de control. Los datos son escritos a su entrada usando el reloj reconstruido y son reconstruidos a la salida usando un reloj maestro de cristal de cuarzo. El *Buffer* se inicializa para sostener un cierto número de bits y se expande o se contrae según se necesite. Por ejemplo, el estandar de **IEEE**, especifica un *Buffer* de 6 bits, el cual es inicializado para alojar 3 bits. Esto es, a medida que entran los bits, son colocados en el *Buffer* durante el tiempo de duración de 3 bits antes de ser retransmitidos. Si la señal recibida en el repetidor de control es algo más rápida que el reloj maestro, el *Buffer* se expandirá, según se necesite, a 4, 5 ó 6 bits, para evitar la adición de bits. Así, las señales limpias se

retransmiten sin el problema del *Timing Jitter*. Esta combinación de circuitos cerrados de fase bloqueada y *Buffer*, incrementa al máximo la longitud posible del Anillo. El límite actual dependerá de las características del medio de transmisión, el cual determinará la cuantía de la distorsión por retraso y por tanto la cantidad de *Timing Jitter*. Por ejemplo, el Anillo de IBM especifica un máximo de 72 repetidores en un Anillo de par trenzado con campo de protección.

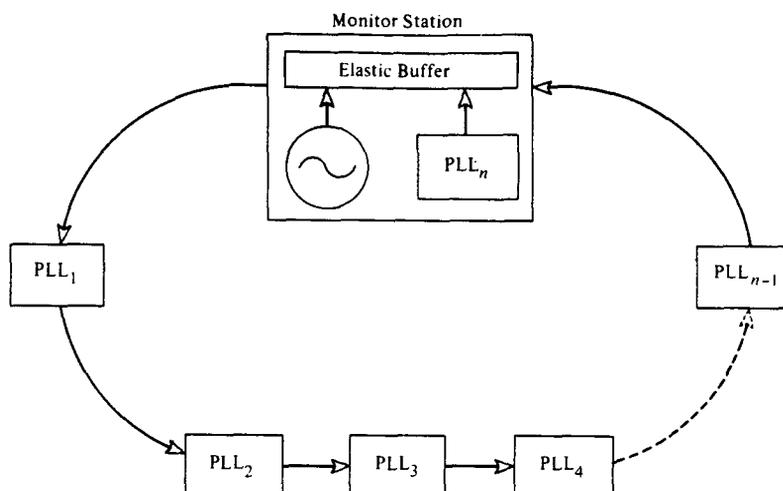


FIGURE 4-10. Ring Synchronization

La arquitectura de Estrella-Anillo:

Podemos hacer las observaciones principales a cerca de la arquitectura descrita a continuación. Primero, hay una limitación práctica en el número de estaciones de un Anillo. Este límite lo fijan los problemas de fiabilidad y mantenimiento ya comentados y el retardo acumulativo que supone un gran numero de repetidores. Este límite se situa

en unos pocos cientos de estaciones. Segundo, los beneficios del Anillo no dependen del *Routing* actual de los cables que enlazan los repetidores.

Estas observaciones han llevado al desarrollo de una arquitectura más refinada, la Estrella-Anillo, la cual acaba con algunos de los problemas del Anillo, y permite la construcción de redes locales grandes. Esta arquitectura usa la estrategia de cableado de la Estrella comentada en el capítulo anterior. Esta es la base de productos como la especificación de IBM para Anillo y similares.

Como primer paso, consideremos la reordenación de un Anillo en una Estrella. Esto se consigue teniendo enlaces inter-repetidor, todos enlazados a través de un sólo sitio (figura 4.11). Este concentrador de cableado del Anillo tiene un buen número de ventajas. Es muy sencillo aislar un fallo, ya que hay acceso a la señal en cada enlace. Un mensaje puede ser introducido en el Anillo y rastreado sin tropiezos para ver hasta donde llega. Un segmento roto puede ser desconectado y reparado más tarde. También podemos añadir nuevos repetidores de manera sencilla: simplemente empalmar dos cables desde el nuevo repetidor al sitio de concentración de cableado del Anillo y unirse a él.

El relé de derivación asociado a cada repetidor, puede ser colocado en el concentrador de cableado del Anillo. El relé puede automáticamente derivar su repetidor

ó dos enlaces si se produce un mal funcionamiento. Debido a ésto, el camino de transmisión entre el repetidor y el siguiente es aproximadamente constante; así, el rango de niveles de la señal al que el sistema debe adaptarse automáticamente es mucho menor.

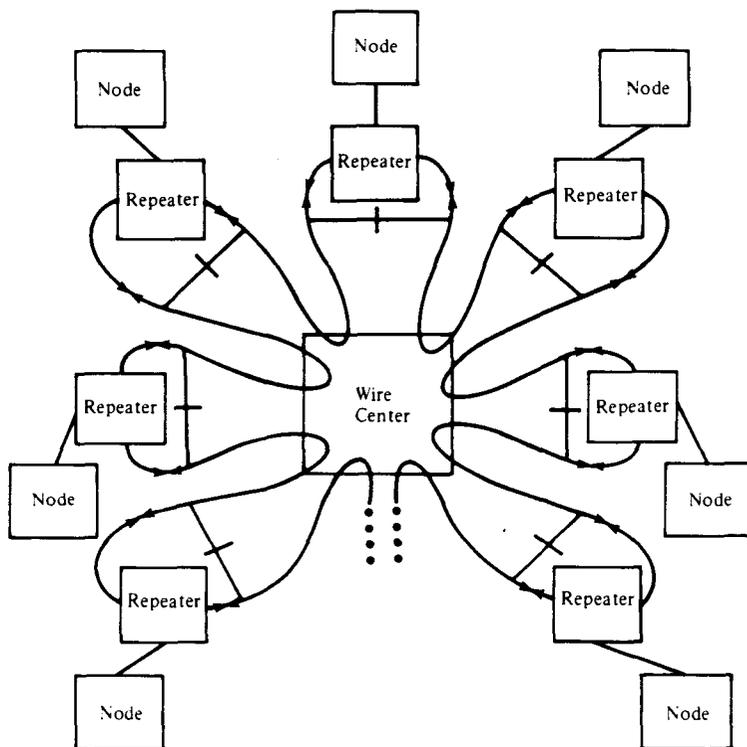


FIGURE 4-11. Ring Wiring Concentrator

El concentrador de cableado del Anillo, alivia en gran medida los problemas de preambulación y de instalación mencionados antes. Y permite una rápida reparación de un fallo de repetidor ó de un cable. No obstante, un fallo sólo, puede deshabilitar, al menos

temporalmente, la red entera. Es más, las consideraciones de transparencia y de *Timing Jitter*, todavía suponen un límite práctico en el número de estaciones en el Anillo. Por último, debemos señalar que en una red de gran difusión, un solo concentrador de cableado emplea una gran cantidad de cable.

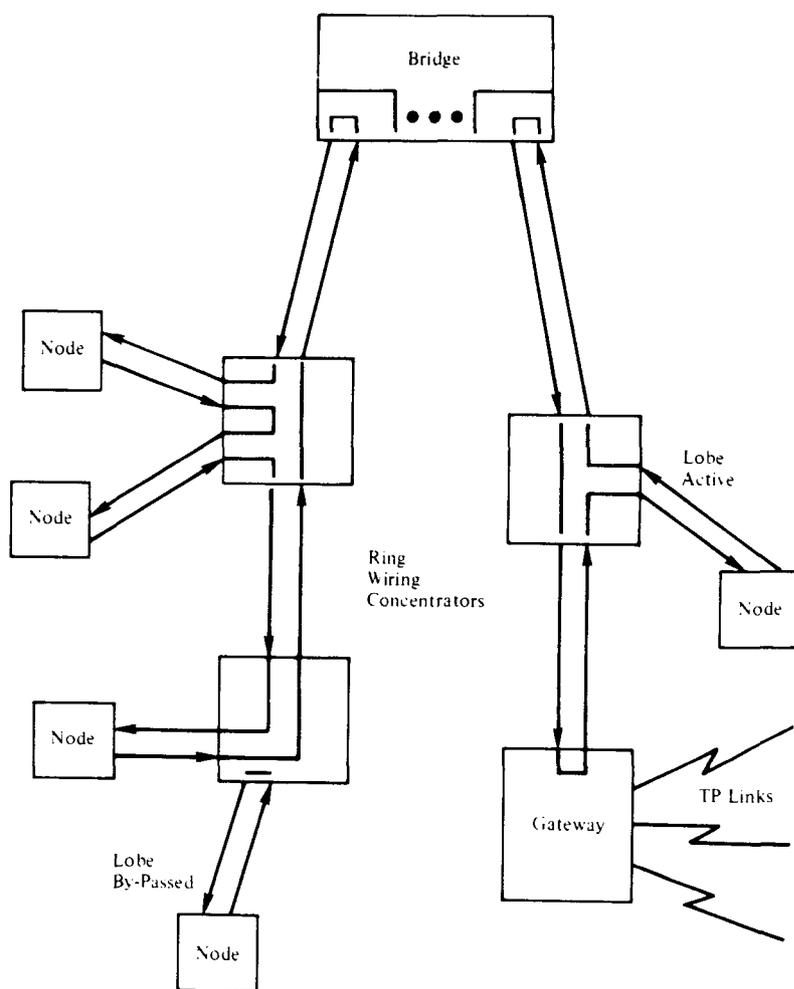


FIGURE 4-12. Ring Bridge

Para atajar estos problemas remanentes, vamos a considerar una red formada de varios anillos. Cada Anillo consiste en una secuencia de concentradores de cableado y el conjunto de anillos conectados por un "puente" (Bridge) tal y como se muestra en la figura 4.12. El puente encamina paquetes de datos desde una subred a otra (anillos) de acuerdo con la información de dirección que lleve cada paquete. Desde un punto de vista físico, cada Anillo opera de forma independiente a los demás Anillos unidos al puente. Desde un punto de vista lógico, el puente provee de encaminamiento transparente entre los anillos.

El puente debe realizar cinco funciones:

- * **Filtrado de entrada:** Para cada Anillo, el puente maneja el tráfico en el Anillo y copia todos los paquetes destinados a otros anillos del puente. Esta función puede ser desempeñada por un repetidor programado para reconocer una familia de direcciones en vez de una sólo.
- * **Buffering de entrada:** Los paquetes pueden necesitar un almacenamiento temporal a su entrada ya sea porque el tráfico inter-anillo es máximo, ó porque el *Buffer* de salida está lleno.
- * **Switching:** Cada paquete debe ser encaminado a través del puente a su apropiado anillo de destino.
- * **Buffering de salida:** Un paquete puede necesitar

ser almacenado temporalmente al salir hacia el Anillo de destino, debido a la espera de una oportunidad de ser instalado en el sistema.

- * Transmisión de salida: Es una función que la puede realizar un repetidor ordinario.

Para un número corto de anillos, el puente es un dispositivo razonablemente sencillo. A medida que el número de anillos en un puente aumenta, la complejidad del *Switching* y la carga del puente también aumentan. Para instalaciones muy grandes, se necesitan varios puentes interconectados por medio de enlaces de alta velocidad (figura 4.13).

Del uso de puentes se derivan tres ventajas principales. Primero, el *Timing Jitter*, que se hacía más patente con el aumento de repetidores en un Anillo, se elimina al reducir el tamaño del Anillo. Segundo, el fallo de un anillo, por cualquier razón, afectará solamente a una porción de la red; un fallo en el puente no impide el tráfico inter-anillo. Por último, se pueden usar varios anillos para aumentar el rendimiento de un Anillo, cuando la capacidad de transparencia del mismo ha sido desbordada.

Hay también algunos peligros. Primero, el asentimiento automático del Anillo se pierde; se necesitan protocolos de mayor nivel para proporcionarlo. Segundo, el rendimiento no mejorará si el tráfico interno en los anillos es muy alto. Luego debemos tratar de reducir este

tráfico colocando de manera apropiada los dispositivos más ocupados en anillos diferentes.

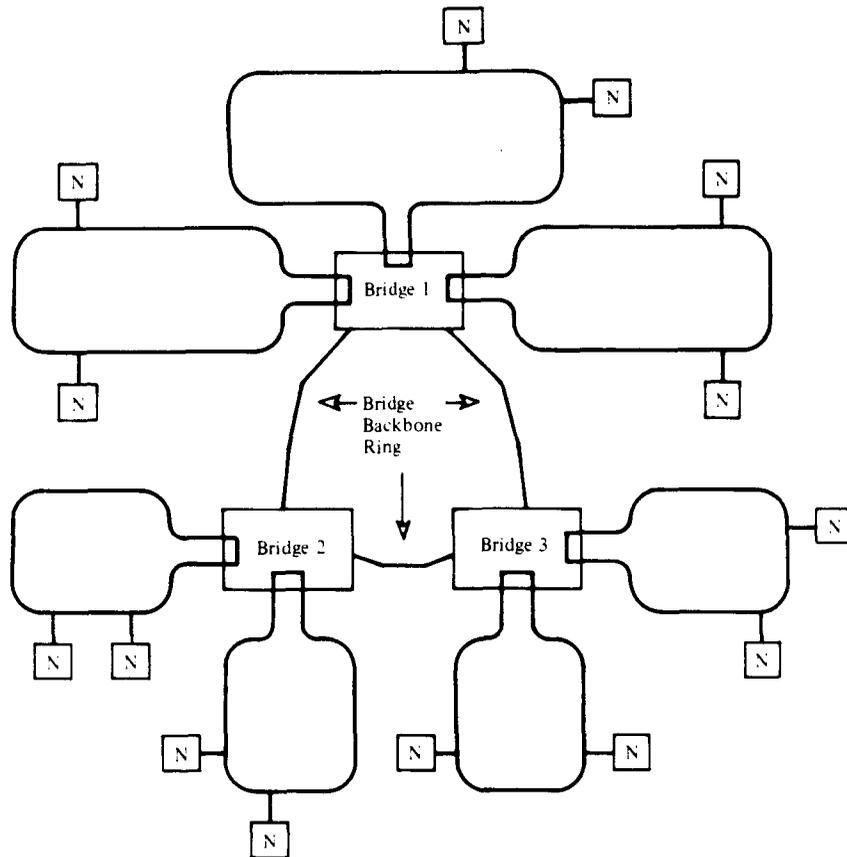


FIGURE 4-13. Multiple Bridges

4.3

LANS DE FIBRA OPTICA.

Hasta ahora, los medios más usados en las LANs y HSLNs son el par trenzado y el cable coaxial. El uso de

fibra óptica se ha rezagado debido a su coste y a las dificultades derivadas de su utilización. No obstante, debido al gran avance de este medio, en los últimos años se ha incrementado el interés por su aplicación en LANs.

En esta sección examinaremos los beneficios de la fibra óptica, y daremos un vistazo a las aproximaciones que se han hecho en el campo de su arquitectura. Más adelante, en el capítulo 6, volveremos a ver este tema al hablar de las redes de área local de alta velocidad.

Beneficios:

Uno de los mayores avances tecnológicos en la transmisión de datos ha sido el desarrollo de los sistemas prácticos de comunicación por fibra óptica. La fibra óptica tiene ya considerable uso en el campo de las comunicaciones de larga distancia, y su utilización en el campo militar va en aumento. Las continuas mejoras en su rendimiento y precio, junto al avance inherente de la fibra óptica, confluirán en la aparición de nuevos campos de aplicación, como son las redes locales y la distribución de señales de video en áreas cortas. Las características que distinguen a la fibra óptica del par trenzado y del cable coaxial se pueden resumir así:

- * Mayor ancho de banda: El ancho de banda potencial, y por tanto, la velocidad del medio crece con la frecuencia. Se pueden conseguir velocidades de 2 Gbps a lo largo de decenas de

kilómetros para frecuencias muy altas. No hay comparación con el límite máximo, en la práctica, de unos cientos Mbps a lo largo de 1 Km para el cable coaxial ó con los pocos Mbps en 1 Km del par trenzado.

- * Menor tamaño y peso: La fibra óptica es considerablemente más pequeña que el cable coaxial ó los manojos de pares trenzados, al menos en orden de magnitud es menor en diámetro para una misma capacidad de transmisión. Tanto su menor peso como su ligereza, reduce los apoyos estructurales necesarios.
- * Menor atenuación: La atenuación es sensiblemente inferior para las fibras ópticas que para el par trenzado y el cable coaxial y es constante para su amplio rango.
- * Aislamiento electromagnético: Los sistemas de fibra óptica no se ven afectados por campos electromagnéticos externos. Por tanto, no son vulnerables a las interferencias y el ruido. Por este mismo rasgo, las fibras ópticas no irradian energía, provocando unas interferencias mínimas con otros equipos y proporciona un alto grado de seguridad frente a las escuchas; además, la fibra óptica es inherentemente difícil de "pinchar" (derivar).
- * Mayor espaciado entre repetidores: Menos

repetidores significa menor coste y menos fuentes de error. Los laboratorios de la Bell Company han probado con éxito un enlace de 68 Km sin repetidores a 8Gbps, con un rango de error de 3×10^{-10} . Los sistemas de par trenzado y cable coaxial necesitan repetidores cada pocos kilómetros.

Hay, por supuesto, algunas desventajas. Una de ellas es el manejo e instalación de los cables de fibra. Los técnicos y herramientas para la instalación de conectores, los empalmes, y el trazado del cable, difieren de aquellos usados en sistemas de par trenzado y cable coaxial, y son en general mas complicados. Un segundo inconveniente ha sido el coste. El equipo de fibra óptica opera en dos campos: el óptico y el de la electrónica. El circuito para la conversión de señales ópticas en electrónicas y viceversa es complejo y caro. Además, hay costes y asuntos técnicos específicos de la arquitectura empleada, como veremos a continuación.

Debido a los innegables beneficios e la fibra óptica, ha habido un gran esfuerzo de investigación para solucionar estos problemas. Así han empezado a surgir LANs basadas en fibra óptica. Sin embargo, habrá que progresar mucho hasta que la fibra óptica sea realmente competitiva con los demás medios de transmisión. El área más prometedora es la de la óptica integrada, la cual es análoga a la integración de circuitos en el campo de la

electrónica. En los próximos años podemos esperar avances en este campo, para mejorar significativamente las características de rendimiento de las fibras ópticas y su coste.

Estrella Pasiva:

Uno de los primeros diseños comerciales disponibles para las LANs de fibra óptica fué el "acoplador en estrella pasiva". El acoplador en estrella pasiva se fabrica fusionando un número determinado de fibras ópticas.

Cualquier luz de entrada de una de las fibras en un extremo del acoplador será dividida en partes iguales entre todas las fibras de salida en el otro extremo del acoplador. Para formar una red, cada dispositivo (estación) es conectado al acoplador mediante dos fibras, una para transmitir y otra para recibir (figura 4.14). Todas las fibras de transmisión entran por un extremo del acoplador, y todas las de recepción salen por el otro extremo. Por lo tanto, aunque la disposición es típicamente en Estrella, actúa como un Bus: una transmisión desde uno cualquiera de los demás dispositivos, es recibida por todos los demás dispositivos, y si dos dispositivos transmiten a la vez, se producirá una colisión.

Los dispositivos comercializados en la actualidad soportan unas decenas de estaciones en un radio de más ó

menos 1 Km. Las limitaciones en el número de dispositivos y en las distancias vienen dadas por las pérdidas en la red.

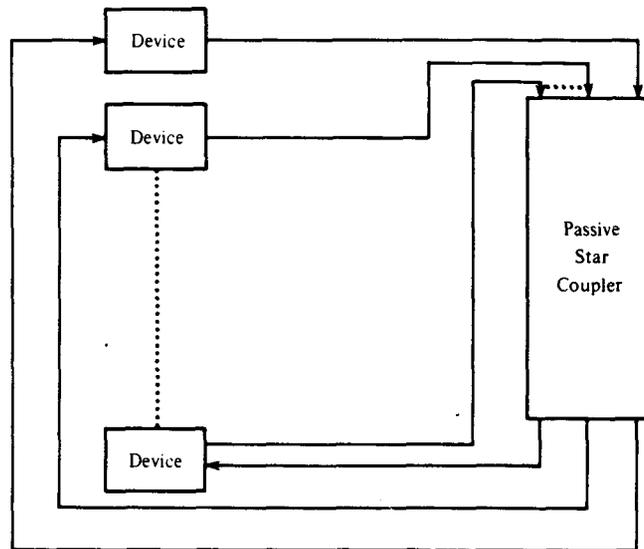


FIGURE 4-14. Optical Fiber Passive Star Configuration

Con el equipo existente hoy en día, las pérdidas toleradas en potencia óptica entre transmisor y receptor son del orden de 25 a 28 dB. La atenuación dependerá de los siguientes componentes:

- * Pérdidas en los conectores ópticos: Los conectores se usan para unir segmentos de cable para aumentar la longitud de los mismos. Normalmente, las pérdidas en los conectores son de 1.0 a 1.5 dB por conector. Una red en estrella pasiva típica lleva de 0 a 4 conectores

en cada enlace emisor-receptor. Esto supone una atenuación máxima de 4 a 6 dB.

- * Atenuación del cable óptico: La atenuación típica de los cables usados en este tipo de sistemas es del orden de los 3 a 6 dB por kilómetro.
- * División de la potencia óptica en el acoplador: El acoplador divide la potencia óptica de un camino de transmisión, en partes iguales entre los caminos de recepción. Expresadas en dB, las pérdidas vistas por cada nodo son $10\text{Log}(N^{\circ}\text{nodos})$. Por ejemplo, las pérdidas efectivas en un acoplador de 16 puertos es de 12dB. Usando este tipo de números, surge la figura 4.15. En ella podemos apreciar la relación entre distancias y el número de dispositivos.

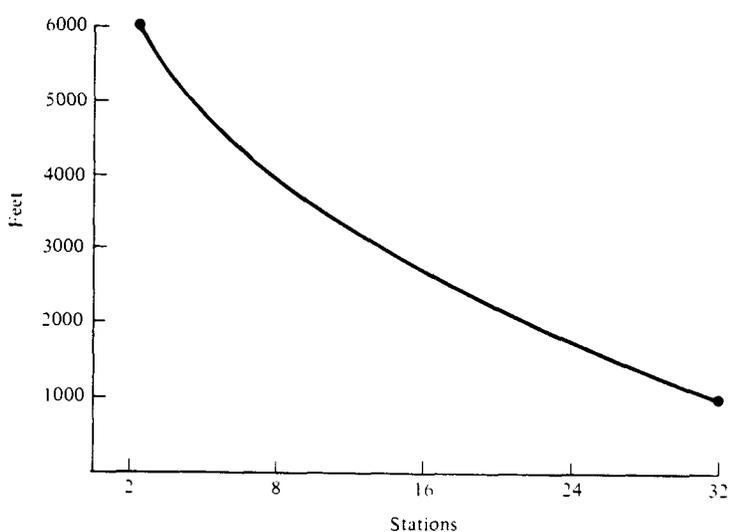


FIGURE 4-15. Passive Star Performance

Como indica la figura, el acoplador de la estrella pasiva es bastante limitado, pues los acopladores con un número de puertos > 100 sólo son realizables a un alto coste. Es por ésto que las investigaciones han derivado hacia otros diseños.

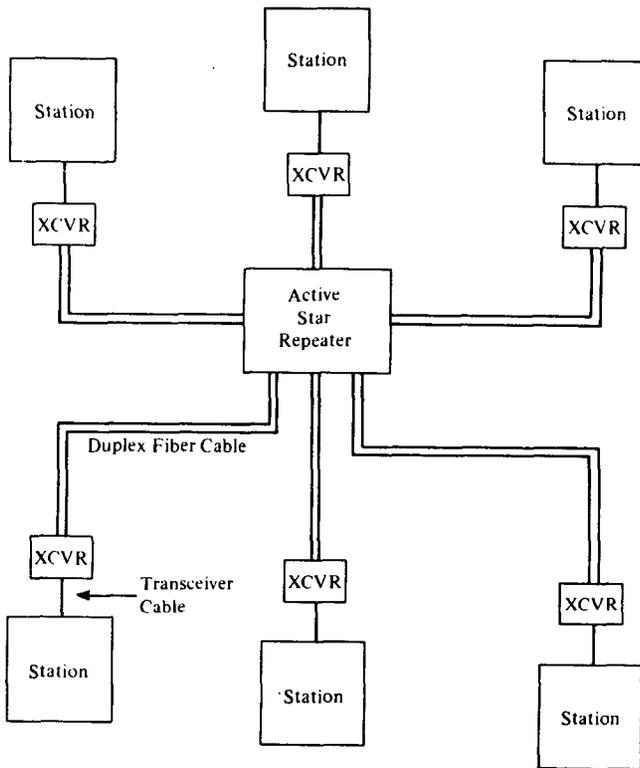
Estrella activa:

Durante unos años, el trabajo realizado en el centro de investigaciones de Xerox en Palo Alto, se centraba en conseguir una versión mejorada de las LANs de fibra óptica con topología Estrella. El resultado es Fibernet II, que se diferencia de la estrella pasiva solo en que el acoplador central es un repetidor activo en vez de un dispositivo pasivo.

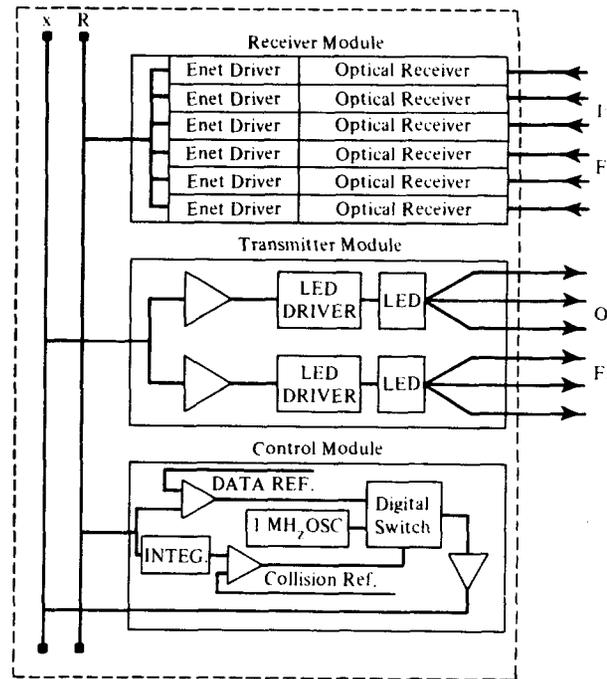
No obstante, la estrella activa (como la pasiva) aparece como un Bus para los dispositivos conectados a ella: la transmisión de uno de ellos es recibida por el resto, y sólo puede transmitir uno y luego otro, nunca dos a la vez.

La figura 4.16 es un diagrama esquemático de Fibernet II. Como comentamos antes, cada dispositivo (estación) se conecta al nodo central mediante dos cables de fibra óptica, uno para transmitir y otro para recibir. En la misma figura 4.16 tenemos la organización interna del nodo. Cuando una estación transmite, el módulo de recepción detecta la señal óptica en las fibras de entrada y la retransmite por un Bus denominado R. El Bus es en

realidad un diminuto cable coaxial de 50 Ohm.



a. Overall Diagram



b. Active Star Organization

FIGURE 4-16. Fibernet II Active Star Configuration

La señal del Bus R es recibida por el módulo de control, el cual la retransmite por otro Bus coaxial de 50 Ohm. Llamado X. El propósito de este módulo intermedio es detectar las colisiones. Este tema lo veremos en el siguiente capítulo. Finalmente, el módulo de transmisión toma la señal del Bus X y la retransmite en forma óptica a través de todas las fibras de salida. El retardo de este proceso es del orden del tiempo de unos pocos bits. Este sistema es un ejemplo típico de topología Bus usando cableado en Estrella, como vimos en la figura 3.5a.

La estrella activa tiene varias ventajas frente a la pasiva. En esta última, la señal de entrada es dividida en partes iguales entre todas las fibras de salida, así cuanto mayor es el número de fibras, mayores son las pérdidas en cualquier camino. Con la estrella activa no tenemos estas pérdidas. Por lo tanto la estrella activa puede soportar más estaciones a más distancias. La Fibernet II está diseñada para soportar por encima de los cientos de dispositivos en un radio máximo de 2.5 Km. La desventaja de la estrella activa es que es más cara debido a los componentes activos de su nodo central.

Anillo de fibra:

Es el más prometedor de los modelos para redes locales de fibra óptica. El Anillo consiste en una serie de conexiones punto a punto, y la tecnología para retransmisiones punto a punto con fibra óptica es bien

conocida y disponible. Además, la fibra tiene menos retardo que el cable coaxial y que el par trenzado, por lo cual sufre menos de *Timing Jitter*. Esto significa que se pueden construir Anillos mayores.

Dadas las altas velocidades alcanzables con la fibra óptica, el Anillo de fibra es una elección natural para las redes locales de alta velocidad (HSLN), como veremos en el capítulo 6. En esta sección veremos algunas consideraciones para las LANs de fibra y en Anillo. Como ya mencionamos, el coste es menor para una HSLN que para una simple LAN, debido al valor de los dispositivos enganchados en uno y otro. Por tanto, en esta sección trataremos de determinar cual es el coste razonable para un Anillo de fibra óptica de baja velocidad (5 - 10 Mbps). Como ejemplo, veremos las especificaciones dadas por IBM para su Anillo. Estas son representativas de lo que es comercialmente factible.

TABLE 4.5 IBM Optical Fiber Ring Specification

Core Diameter	100 μm
Cladding Diameter	143 μm
Wavelength	850 nm
Attenuation	<6 dB/km
Bandwidth	>150 MHz
Data Rate	up to 20 Mbps
Distance	1.5 to 2.0 km

La especificación de IBM para su Anillo de fibra fué escrita para satisfacer una transmisión corriente usando una luz de 850 nanómetros (nm) de longitud de onda. La especificación también incluye un posible incremento de la longitud de onda hasta 1300 nm para redes de mayor rendimiento.

La tabla 4.5 muestra los parámetros principales de la especificación. Con una longitud de onda de 850 nm, se usan LEDs y detectores PIN de coste relativamente bajo. se consiguen velocidades de más de 20 Mbps a una distancia de 1.5 a 2.0 Km (en cada enlace sencillo). El sistema es capaz de soportar al menos tantos repetidores en un Anillo sencillo como uno de par trenzado con campo, esto es, alrededor de 250.

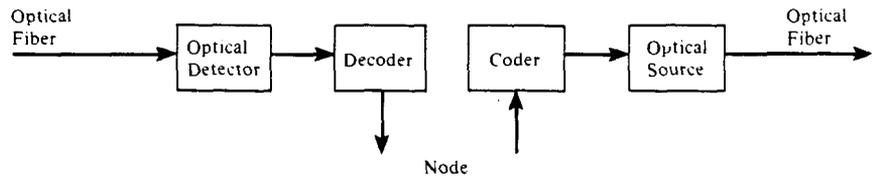
Bus de fibra:

Se pueden hacer dos enfoques en el diseño de una LAN ó HSLN con topología Bus. Las diferencias tienen que ver con el hecho de introducir en el Bus tomas (Taps) activas ó pasivas. En el caso de poner tomas activas (figura 4.17a), se suceden los siguientes pasos:

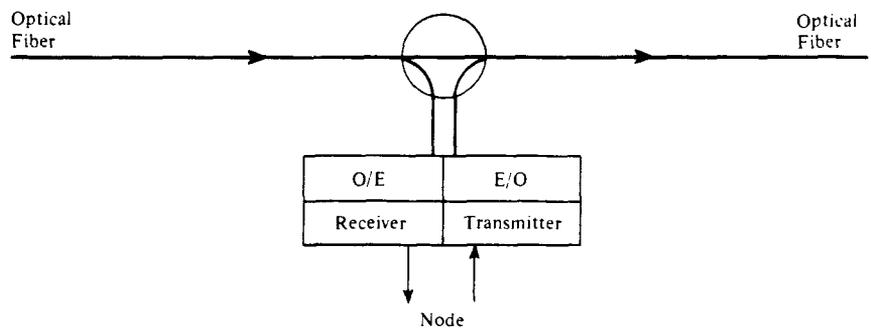
- 1.- La energía de la señal óptica entra en la toma desde el Bus.
- 2.- La información sincronizada es recuperada de la señal y la señal se convierte en una señal eléctrica.
- 3.- La señal convertida es presentada al nodo y

quizás modificada por este último.

- 4.- La señal óptica (un haz de luz) se modula de acuerdo con una señal eléctrica y lanzada dentro del BUS.



a. Active Tap



b. Passive Tap

FIGURE 4-17. Optical Fiber Bus Taps

En el caso de poner tomas pasivas (figura 4.17b), la toma extrae una porción de la energía óptica del Bus para la recepción e inyecta energía óptica directamente en el medio para la transmisión. En efecto, el medio no se rompe. Este enfoque con tomas pasivas es equivalente al tipo de tomas usadas para pares trenzados y cable coaxial.

Las configuraciones activa y pasiva se ven en la

figura 4.18. para la configuración activa se necesitan dos fibras ópticas y cada toma consiste en dos acopladores activos como los descritos anteriormente.

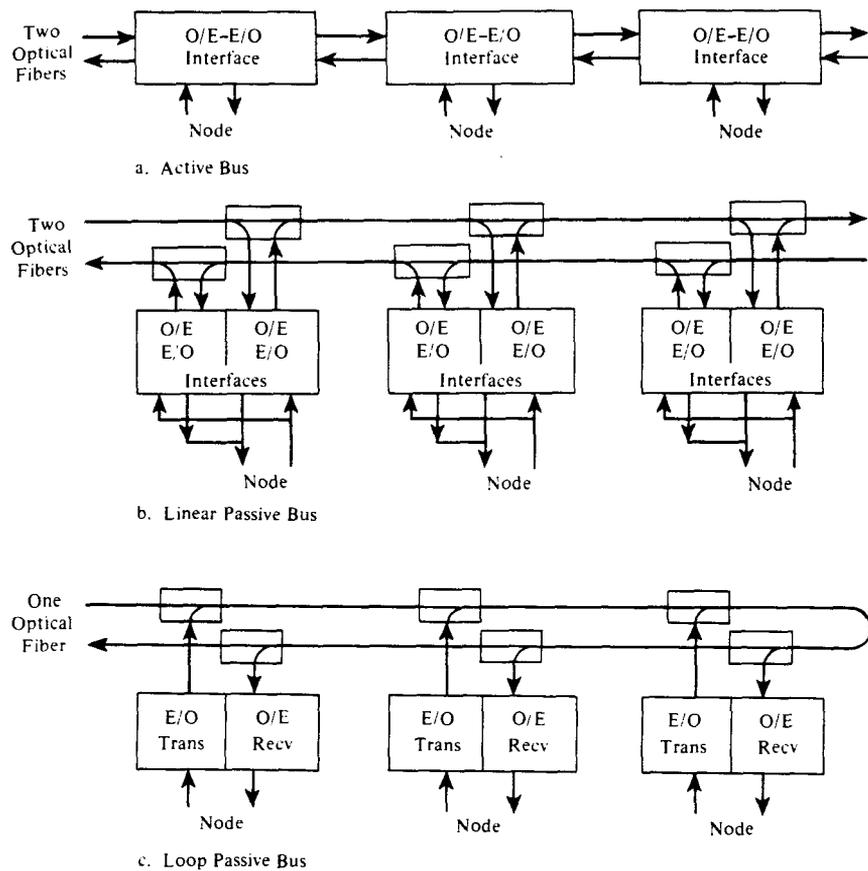


FIGURE 4-18. Optical Fiber Bus Configurations

Esto es debido a la inherente naturaleza unidireccional del dispositivo de la figura 4.17a. Para la configuración pasiva, cada toma debe conectarse al Bus mediante dos cables, debido a que las tomas ópticas son unidireccionales. La figura 4.18b muestra una

configuración en la que se utilizan dos fibras. Cada toma consiste en dos transmisores-redeptores de tal modo que las señales puedan ser insertadas y extraídas de las fibras unidireccionales. Un enfoque mejor, ilustrado en la figura 4.18c, usa un solo cable de fibra óptica en el cual uno de los extremos del Bus está cerrado. Las estaciones transmiten en una pierna y reciben en la otra pierna de la fibra, del mismo modo que un Bus *Broadband* de doble cable. Esta última configuración reduce el número necesario de transmisores y de receptores en la red a la mitad.

La complejidad electrónica y el coste del interface son inconvenientes a tener en cuenta a la hora de implementar un Bus activo. Incluso cada toma introducirá un aumento en el retardo al igual que pasaba en el caso del Anillo. En los buses pasivos, resulta un inconveniente la naturaleza tendente a pérdidas de las tomas púrmanete ópticas (no teniendo conversiones opto-eléctricas y viceversa). Tomas de pocas pérdidas no están disponibles comercialmente en la actualidad. Con tomas de altas pérdidas, sólo podemos utilizar muy pocas tomas antes de que la señal se vuelva demasiado débil para detectarla. No obstante se sigue investigando. La Bell Communications Research estudia una toma con pérdidas bajas que creen pueda aplicarse en un número superior a los 80 en un Bus de fibra.

REDES DE AREA LOCAL: PROTOCOLOS

En el capítulo anterior examinamos algunos de los puntos más importantes referentes a la arquitectura y propiedades físicas de las LANs. Debido a su alcance e importancia, el tema de la arquitectura de las comunicaciones ó protocolos merece un capítulo propio.

Este capítulo comienza con una discusión global sobre los protocolos de LAN, y profundiza hasta determinar qué capas de funcionalidad se requieren. Luego se estudiarán las áreas específicas del control de enlace y de control de acceso al medio. A lo largo de todo el tema se harán referencia al estándar de IEEE 802. Esto se debe a dos razones:

- * Este estándar es bien conocido, proporcionando

un marco de trabajo para la exposición y clarificación de puntos referentes a la arquitectura de comunicaciones de las LANS.

- * Este estándar ha tenido una influencia notable en los productos para LANS.

5.1

PROTOCOLOS PARA LAN.

Modelo de referencia:

En el capítulo 2 se resume una arquitectura para comunicaciones, el modelo de referencia de OSI, basado en siete capas de protocolos. Como vimos se requieren las capas 1,2 y 3 para el correcto funcionamiento de una red *Packet-Switched*. Recordando, estas capas fueron descritas como sigue:

- 1.- Capa física: Relativa a la transmisión de una cadena no estructurada de bits a través de un enlace físico. Comprende parámetros como la oscilación del voltaje de la señal y la duración de los bits. Se ocupa de las características mecánicas, eléctricas y de procedimiento para establecer, mantener o desactivar el enlace físico.
- 2.- Capa de enlace de datos: proporciona una transferencia de datos fiable a través del

enlace físico; envía bloques de datos (frames) con la sincronización necesaria, control de error y control de flujo.

3.- Capa de red: aporta capas superiores con independencia de la tecnología de *Switching* y de transmisión de datos usadas para conectar sistemas; responsable de establecer, mantener y determinar las conexiones.

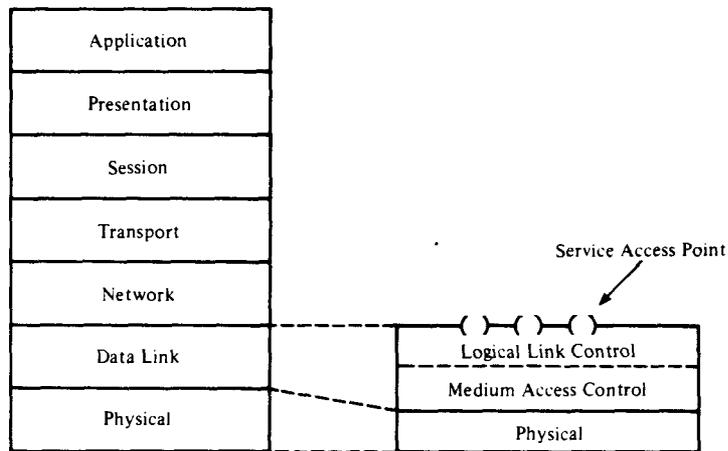


FIGURE 5-1. LAN Protocol Layers Compared to OSI

Una vez recordado el objetivo de cada una de estas capas, volvemos a la pregunta de cuales son las capas necesarias para la correcta operación de la LAN. Por motivos de claridad, examinaremos la cuestión en el contexto del modelo de referencia de OSI. En el contexto adoptado hay dos características de las LANs importantes.

Primero, los datos se transmiten en *Frames* (bloques o marcos) direccionados. Segundo, no hay *Switching* intermedio, por lo tanto no es necesario el *Routing* (encaminamiento) (usamos repetidores en los anillos y en los buses de *Baseband*, pero no incluyen el *Switching* ó *Routing* a excepción del anillo con puente).

Estas dos características determinan la respuesta a la pregunta ¿Qué capas del modelo OSI son necesarias?. La capa 1, ciertamente, pues se requiere una conexión física. La capa 2, también, ya que los datos transmitidos a través de la LAN deben ser organizados en *Frames* y controlados. Pero ... ¿Y la capa 3?. La respuesta es sí y no. Sí nos fijamos en las funciones desempeñadas por la capa 3, la respuesta sería no, ya que hay *Routing* y con un enlace directo disponible entre cada dos puntos, éste no es necesario. El resto de las funciones de la capa 3: direccionamiento, secuenciamiento, control de flujo y de error, etc... Son realizados, como hemos visto, por la capa 2. La diferencia estriba en que la capa 2 realiza estas funciones a lo largo de un enlace único, mientras que la capa 3 puede realizarlas a través de la secuencia de enlaces necesarios para recorrer la red. Pero desde el momento en que se necesite sólo un enlace para recorrer la LAN, estas funciones de la capa 3 se vuelven superfluas y redundantes.

Desde el punto de vista de un sistema enganchado, la respuesta a la necesidad de que la LAN proporcionara la

capa 3 sería sí. El dispositivo se ve a sí mismo enganchado a un punto de acceso de una red que soporta comunicaciones con muchos dispositivos. La función que asegura que un mensaje enviado a través de un punto de acceso llegue a uno de los puntos finales parece que debiera ser una función de la capa 3. Así que se puede decir que aunque la red proporcione servicios hasta la capa 3, las características de la red permiten que estos servicios sean implementados en dos capas del modelo OSI. Estudiaremos más a fondo éste particular en el capítulo 8. Por ahora es suficiente el tener claro que las funciones de comunicación mínimas que debe proporcionar una LAN, corresponden a las capas 1 y 2 del modelo OSI.

Con lo dicho en mente, pensemos en los requerimientos funcionales para controlar una red local y examinémoslos de arriba a bajo. Seguiremos el razonamiento utilizado por el comité IEEE 802, ilustrado en la figura 5.1.

En el nivel superior están las funciones asociadas a la aceptación de transmisiones desde otra estación enganchada y facilitar las recepciones a las estaciones de la red. Estas funciones incluyen:

- * Proporciona uno ó más SAP. Un SAP (como se recordará) es un interface lógico entre dos capas adyacentes.
- * En la transmisión, ensambla datos formando *Frames* con los campos de dirección y de CRC (Cyclic Redundancy Check).

* Manejo de la comunicación a lo largo del enlace.

Estas son las funciones típicamente asociadas a la capa 2, la capa de enlace de datos (Data Link). Las tres primeras funciones descritas, están agrupadas en la llamada *Logical Link Control Layer* (LLC) en el estándar de IEEE 802. La última función es tratada por este comité como una capa separada, llamada *Medium Acces Control* (MAC). Esta disposición obedece a dos razones:

* La lógica necesaria para administrar el acceso a un enlace multi-fuente, multi-destino, no se encuentra en una capa 2 tradicional.

* Para el mismo LLC, es posible tener varias opciones MAC.

Por último, en la capa inferior hay funciones típicamente asociadas a la capa física. Estas incluyen:

* Codificación/decodificación de señales.

* Generación eliminación de preámbulos para la sincronización.

* Recepción/transmisión de bits.

Como ocurre en el modelo de OSI, estas funciones son asignadas a una capa física en el estándar de IEEE 802.

Control de acceso al medio (MAC) para redes locales:

Todas las redes locales (LAN, HSLN, Circuit-Switched) consisten en una colección de dispositivos que deben compartir la capacidad de transmisión de la red, por lo que es necesario algún tipo de control de acceso al medio

de transmisión, para que, cuando lo requieran, dos dispositivos particulares intercambien datos.

Los parámetros clave en cualquier técnica de control de acceso al medio son el dónde y el cómo. El "dónde" se refiere a dónde se va a ejercer el control, en un sistema centralizado ó distribuido. En un diseño centralizado, se designa un controlador. En una red descentralizada, las estaciones realizan colectivamente una función de control de acceso al medio para determinar de forma dinámica el orden en el cual van a transmitir las estaciones. Un diseño centralizado tiene ventajas como:

- * Puede afrontar mayor control sobre el acceso, proporcionando cosas como prioridades, y ancho de banda garantizado.
- * Permite que la lógica en cada estación sea lo más simple posible.
- * Evita el problema de la coordinación.

Sus principales inconvenientes son:

- * Tiene un punto clave de posible fallo.
- * Puede actuar como un cuello de botella, reduciendo así la eficiencia.

Los pros y contras del diseño distribuido son los contrarios que los dichos anteriormente.

El segundo parámetro "cómo" está limitado por la topología y es un compendio de factores de competitividad, coste, rendimiento y complejidad. En general, podemos clasificar las técnicas de control de acceso en síncronas

y asíncronas. Con las técnicas síncronas, se dedica una capacidad específica a cada conexión (esto se hace en las redes locales de Circuit Switching). Estas técnicas no son óptimas en LANs y HSLN debido a que las necesidades de las estaciones son generalmente impredecibles. Es preferible poder colocar la capacidad necesaria de una manera asíncrona (dinámica), más ó menos en respuesta a las necesidades inmediatas. Las técnicas asíncronas pueden ser divididas en tres categorías: *Round Robin* (mesa redonda o turnos), *Reservation* (reserva) y *Contention* (contención).

Round Robin:

Las técnicas *Round Robin* son conceptualmente simples, y se basan en la filosofía de "dar a todo el mundo un turno" A cada estación (por turnos) se le da la oportunidad de transmitir. Durante esa oportunidad, la estación puede declinar el transmitir ó puede hacerlo, supeditada a un límite superior, normalmente dado por la máxima cantidad de datos ó tiempo que tiene para esta oportunidad. En cualquier caso, la estación, cuando ha acabado, debe ceder su turno, de manera que el derecho a transmitir pasa a la siguiente estación de la secuencia lógica. El control de los turnos puede estar centralizado ó distribuido. Un ejemplo de técnica centralizada es el *Polling* (encuesta) en una línea multipunto.

Cuando muchas estaciones tienen datos que transmitir a lo largo de períodos largos de tiempo, la técnica de

Round Robin puede ser muy eficiente. Si sólo unas pocas estaciones tienen datos a transmitir en cualquier momento, es preferible la utilización de otras técnicas, máxime si el tráfico es "Stream" (cadena de bits) ó "Bursty" (ráfagas). El tráfico tipo *Stream* se caracteriza por ser transmisiones largas y continuas. Como ejemplos podemos citar las comunicaciones de voz, la telemetría y la transferencia total de ficheros. En cambio la transmisión tipo *Bursty* se caracteriza por que son transmisiones cortas y esporádicas. Un ejemplo de este tráfico es el tráfico interactivo entre el terminal y su ordenador nodriza (ó principal).

Reserva:

Son técnicas que van muy bien con el tráfico tipo *Stream*. En general en estas técnicas el tiempo en el medio es dividido en porciones (Slots). Una estación que desee transmitir, reserva porciones futuras por un período extenso ó indefinido. Estas técnicas pueden hacerse de un modo centralizado o distribuido.

Contención:

Las técnicas de contención son muy apropiadas para el tráfico tipo *Bursty*. En éstas, no se hace ningún control para determinar de quien es el turno; todas las estaciones compiten por tiempo (para acceder al medio) en un nodo que, como veremos, puede ser brusco y desordenado. Estas

técnicas son distribuidas por naturaleza. Su principal ventaja es que son simples a la hora de implementar y eficientes para una carga ligera ó mediana. Para una gran carga estas técnicas tienden a colapsarse.

TABLE 5.1 Medium Access Control Techniques

	Centralized	Distributed
Round-robin	Polling	Token bus Token ring Delay schedule Implicit token
Reservation	Centralized reservation	Distributed reservation
Contention		CSMA/CD Slotted ring Register insertion

Aunque las técnicas de reserva centralizadas y distribuidas se han implementado en algunos productos LAN, las técnicas usadas más comunmente son las *Round Robin* y las de contención.

En la tabla 5.1 podemos ver la clasificación de técnicas de control de acceso al medio, dependiendo de su cualidad de centralizadas ó distribuidas.

El formato de Frames de la IEEE 802:

Esta sección muestra los formatos usados como *Frames* (bloques de datos) en el estándar de IEEE 802. Estos formatos son similares a los utilizados por la mayoría de los propietarios de redes. Estos son la base para el LLC,

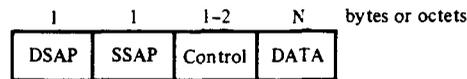
MAC, y la funcionalidad de la capa física.

Los requerimientos de un *Frame* para una red local son muy similares a los del formato HDLC visto en el capítulo 2. Debe haber por supuesto, un campo de datos o de información. Se necesita un campo de control para pasar los bits de control e identificar el tipo de marco (*Frame*). También se suelen utilizar unas plantillas (patrones de bits) al comienzo y al final, que sirvan de delimitadores. Se requiere también un direccionamiento. Aquí surge la mayor diferencia con respecto al formato del HDLC. Dado que los enlaces de las LANs son multifuente y multidestino, se necesitan tanto la dirección de la fuente (origen) como la del destino. Es más, a diferencia del HDLC y virtualmente de todos los protocolos de la capa 2, los protocolos para LAN de IEEE 802 soportan una forma de multiplexación común en protocolos de capa 3. Como veremos, esto es realizado en la IEEE 802 identificando puntos de acceso a servicios (SAP) en cada estación.

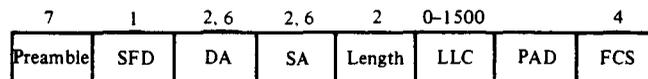
La figura 5.2 nos muestra los formatos de la IEEE 802. Como se puede ver, se usa un formato separado en el nivel de LLC, y éste es entonces incrustado en el apropiado marco (*Frame*) del MAC. La IEEE 802 soporta tres alternativas de MAC: CSMA/CD, Token Bus, y Token Ring.

Cada campo será descrito en la sección correspondiente, pero hay un aspecto que merece la pena ser comentado ahora: La información de la dirección ha sido dividida entre el *Frame* del LLC y el del MAC.

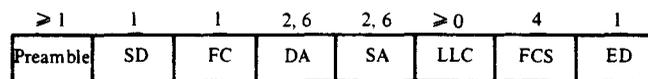
Logical Link Control (LLC)



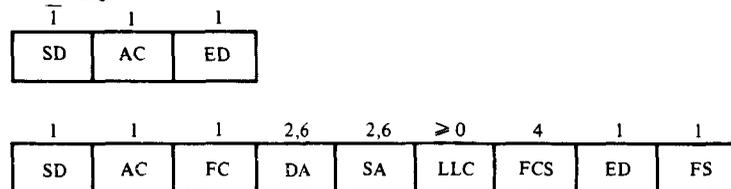
CSMA/CD



Token Bus



Token Ring



- AC = Access Control
- DA = Destination Address
- DSAP = Destination Service Access Point
- ED = Ending Delimiter
- FC = Frame Control
- FCS = Frame Check Sequence
- FS = Frame Status
- SA = Source Address
- SD = Starting Delimiter
- SFD = Start Frame Delimiter
- SSAP = Source Service Access Point

FIGURE 5-2. IEEE 802 Frame Formats

Esto es debido a que los SAP de origen y destino deben ser conocidos solamente a nivel de LLC, para lograr la transferencia de datos entre estaciones enganchadas a la red. No obstante, como veremos, las direcciones de origen y de destino son parte crítica de la función del

MAC.

5.2

PROTOCOLOS DE CAPA DE ENLACE EN LANs.

En esta sección examinaremos los requerimientos generales del nivel de enlace para una red de área local y luego estudiaremos la especificación del IEEE 802.

Principios:

Las capas de enlaces para LANs tienen algún parecido con las capas de enlaces más comunes ya existentes. Estas capas tienen que ver con la transferencia de un *Frame* de datos entre dos estaciones, sin que pase por nodos de conmutación (Switching Nodes).

Las capas de enlaces para LANs se diferencian en tres aspectos de las tradicionales:

- * Debe soportar la naturaleza multiacceso del enlace (se diferencia del multipunto en que no hay nodo primario).
- * Es relevada de algunos detalles del acceso al enlace por la capa del MAC.
- * Debe facilitar algunas funciones de capa 3.

La figura 5.3 nos ayudará a comprender los requerimientos para la capa de enlaces. En ella se consideran dos estaciones que se comunican vía LAN (Bus ó

Anillo). Las capas superiores (correspondientes al transporte y demás) proporcionan servicios punto a punto entre las estaciones. Por debajo de la capa de enlaces, una capa de Control de Acceso al Medio (MAC) proporciona la lógica necesaria para obtener acceso al medio para la transmisión y recepción de *Frames*.

Como mínimo, la capa de enlaces debería realizar las siguientes funciones:

- * Control de error: La capa de enlaces debe asegurar una transmisión sin errores a través de la LAN.
- * Control de flujo.

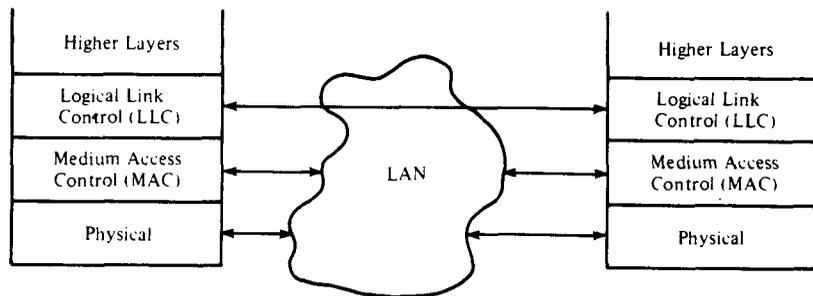


FIGURE 5-3. LAN Communication Architecture

Como ya mencionamos, al no haber nodos intermedios de distribución, una LAN no necesita una capa 3 diferenciada; las tres funciones esenciales de la capa 3 pueden ser incorporadas a la 2:

- * *Connectionless*: Este servicio es necesario para aumentar su eficiencia para un gran tráfico

interactivo. Se refiere a la necesidad de no conectar todos y cada uno de los puntos entre sí.

- * *Connection-Oriented*: Surge de la necesidad de contar con un servicio de orientación de las *Frames* que se transmiten a lo largo de la conexión deseada.
- * Multiplexado: Normalmente, una estación se engancha a una LAN por medio de un sólo enlace físico; debería ser posible el facilitar la transferencia de datos a muchos puntos diferentes de destino, a través de ese único enlace físico.

Como no hay necesidad de un encaminamiento (Routing), las funciones mencionadas se pueden facilitar de una manera sencilla.

La primera de ellas sólo requiere el uso de campos de dirección de origen y destino. La estación emisora del *Frame* debe especificar la dirección de destino, de tal manera que el *Frame* sea tratado correctamente. Por su parte, la dirección de origen debe también estar indicada para que la estación receptora sepa de donde viene el *Frame* recibido.

Las otras dos funciones pueden ser soportadas utilizando el concepto de *SAP*, que ya vimos en el capítulo 2. En la figura 5.4 tenemos una situación que nos puede ayudar a ver más claramente el campo de estas dos

funciones.

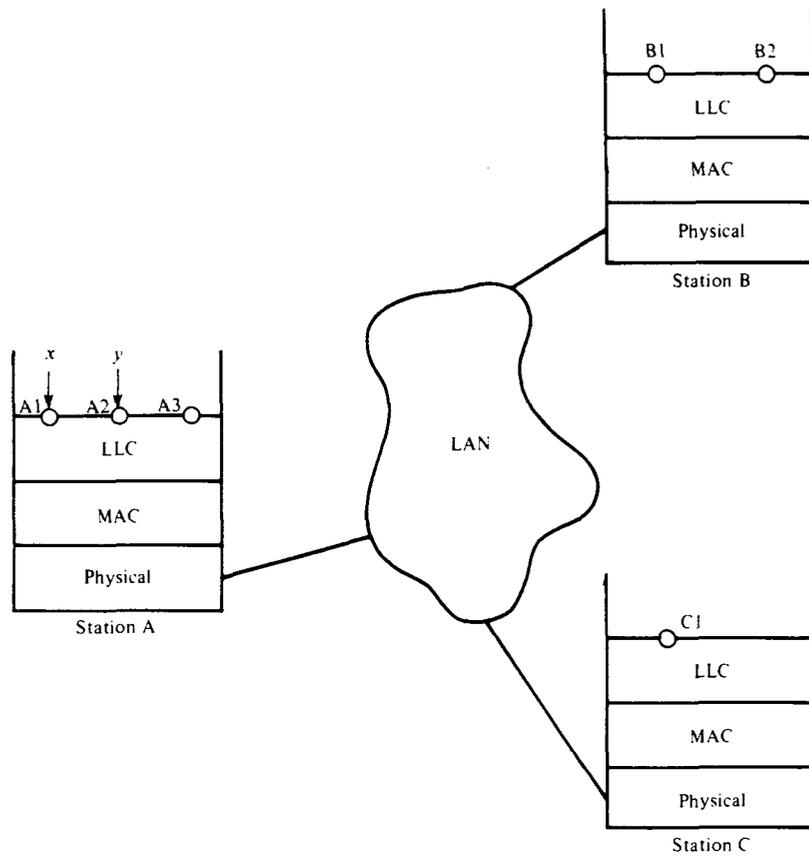


FIGURE 5-4. LAN Link Control Scenario

Cada estación tiene una dirección, y además la capa de enlace tiene varios SAPs cada uno de los cuales tiene su propia dirección. La capa de enlaces facilita la comunicación entre SAPs. Supongamos que un proceso o aplicación X en la estación A quiere mandar un mensaje a un proceso en la estación C. X puede ser un generador de informes en el miniordenador A, y C puede ser una impresora con un sólo Driver. X se engancha al SAP1 y

solicita una conexión con el **SAP1** de la estación C (si C es una impresora de un sólo Driver, sólo tendrá un SAP). La capa de enlaces de la estación A envía entonces un *Frame* de petición de conexión que incluye la dirección fuente (A,1), y la dirección de destino (C,1), y algunos bits de control indicando que se trata de una petición de conexión. La LAN entrega este *Frame* a C, la cual, si está libre, devuelve un *Frame* de aceptación de conexión. Desde ese momento, todos los datos de X serán ensamblados en *Frames* por la LLC de la estación A, incluyendo la dirección de origen (A,1) y la de destino (C,1). Todos los *Frames* que lleguen a A serán rechazados a no ser que vengan de (C,1). De igual modo la estación C sólo aceptará *Frames* provenientes de (A,1).

Como vemos, así se facilita un servicio de conexión orientada. Al mismo tiempo, un proceso Y puede engancharse al SAP (A,2) e intercambiar datos con (B,1). Esto es un ejemplo de multiplexado. Otros procesos en A pueden usar (A,3) para enviar datagramas a otros destinos.

Por último, la capa de enlaces debe incluir una función para asumir la naturaleza multiacceso de la LAN:

- * *Multicast, Broadcast* (multireparto): La capa de enlace debe proporcionar un servicio que facilite la posibilidad de mandar un mensaje a múltiples destinos ó a todos los posibles.

Control Lógico de Enlaces de IEEE 802:

El estándar de IEEE 802 referente al Control Lógico de Enlaces (LLC) es un buen ejemplo de capa de enlaces para LAN. En este apartado veremos sus rasgos principales.

La figura 5.2 muestra el formato del *Frame* del LLC. Como se puede ver, en él se especifican los SAPs de origen (SSAP) y de destino (DSAP) (permitiendo el multiplexado del enlace), un campo de control de 1 ó 2 bits, y un campo de datos. Los campos de origen y de destino los necesita el LLC, pero son usados también por el MAC, y están incluidos en el *Frame* exterior del MAC. El LLC puede ser especificado en tres partes:

- * El interface con la estación, especificando los servicios que el LLC (y por tanto la LAN) facilitan al abonado de la red.
- * El protocolo del LLC, especificando las funciones del LLC.
- * El interface con el MAC, especificando los servicios que el LLC requiere para realizar su función.

No todas las funciones mencionadas en el apartado anterior se necesitan en todos los entornos de aplicación. Por ello, el estándar de IEEE 802 define dos categorías generales de operación de control de enlace de datos. La primera es una operación tipo "Connectionless" que proporciona un servicio mínimo con la mínima complejidad en el protocolo. Esto es aplicable y eficiente si las

capas superiores (capa de red, de transporte) proporcionan control de error, de flujo y funciones de secuenciamiento. También es provechoso cuando no se requiere garantía de buena entrega de los datos. La segunda categoría es una operación de conexión orientada, la cual proporciona las funciones mencionadas arriba usando un protocolo similar al HDLC. Estos dos tipos de operación están reflejados en las especificaciones tanto de los servicios del LLC como de su protocolo.

Servicios del LLC:

El LLC proporciona 3 servicios:

- * Servicio *Connectionless* sin confirmación (ACK):
Es un servicio de datagramas que simplemente permite la transmisión y recepción de *Frames*. Soporta conexiones punto a punto, multipunto y multidestino (Broadcast).
- * Servicio de conexiones orientadas: Proporciona una conexión lógica entre **SAPs**. Facilita control de flujo, secuenciamiento, y restablecimiento de errores.
- * Servicio *Connectionless* con confirmación (ACK):
Este es un servicio tipo *Connectionless* pero dotado de confirmación (acuse de recibo), aliviando a las capas superiores de esta carga. Este servicio soporta transferencias punto a punto.

TABLE 5.2 Logical Link Control Primitives

Unacknowledged Connectionless Service

L_DATA.request (local_address,remote_address,l_sdu,service_class)
L_DATA.indication (local_address,remote_address,l_sdu,service_class)

Connection-oriented Service

L_DATA_CONNECT.request (local_address,remote_address,l_sdu)
L_DATA_CONNECT.indication (local_address,remote_address,l_sdu)
L_DATA_CONNECT.confirm (local_address,remote_address,status)

L_CONNECT.request (local_address,remote_address,service_class)
L_CONNECT.indication (local_address,remote_address,status,service_class)
L_CONNECT.confirm (local_address,remote_address,status,service_class)

L_DISCONNECT.request (local_address,remote_address)
L_DISCONNECT.indication (local_address,remote_address, reason)
L_DISCONNECT.confirm (local_address,remote_address,status)

L_RESET.request (local_address,remote_address)
L_RESET.indication (local_address,remote_address,reason)
L_RESET.confirm (local_address,remote_address,status)

L_CONNECTION_FLOWCONTROL.request (local_address,remote_address,amount)
L_CONNECTION_FLOWCONTROL.indication (local_address,remote_address,amount)

Acknowledged Connectionless Service

L_DATA_ACK.request (local_address,remote_address,l_sdu,service_class)
L_DATA_ACK.indication (local_address,remote_address,l_sdu,service_class)
L_DATA_ACK_STATUS.indication (local_address,remote_address,service_class,status)

L_REPLY.request (local_address,remote_address,l_sdu,service_class)
L_REPLY.indication (local_address,remote_address,l_sdu,service_class)
L_REPLY_STATUS.indication (local_address,remote_address,l_sdu,service_class,status)

L_REPLY_UPDATE.request (local_address,l_sdu)
L_REPLY_UPDATE_STATUS.indication (local_address,status)

Estos servicios están especificados en términos de "primitivas", que pueden ser vistas como comandos ó llamadas a procedimientos con parámetros (tabla 5.2).

El servicio *Connectionless* sin confirmación es un servicio al estilo datagrama que permite simplemente el envío y recepción de *Frames LLC*, sin ningún tipo de

confirmación que asegure la entrega. En él se pueden realizar direccionamientos punto a punto, multipunto, y **Broadcast**, así como el multiplexado.

Este servicio proporciona a través de sólo dos primitivas, el interface entre la LLC y la capa inmediatamente superior (sin incluir las primitivas de servicio de manejo-dirección). **L-DATA Request** se utiliza para pasar un *Frame* hacia abajo, hacia la LLC para su transmisión. **L-DATA Indication** se usa para elevar un *Frame* a la LLC para su recepción. Los parámetros "Local Address" y "Remote Address" especifican los usuarios local y remoto respectivamente. Cada uno de ellos es equivalente a la combinación de los **SAPs** de la LLC y la dirección del **MAC**. Volveremos más adelante sobre este punto. El parámetro **l-sdu** especifica la unidad de dato de servicio de la LLC; esto es, el bloque de datos intercambiado entre la LLC y su usuario. El parámetro **Service Class** especifica la prioridad deseada. Este parámetro es pasado a través de la entidad LLC hacia la entidad **MAC**, la cual tiene la responsabilidad de implementar un mecanismo de prioridad. Las especificaciones **Token Bus** y **Token Ring** son capaces de realizar esto, pero no la **802.3 CSMA/CD**.

El servicio de conexiones orientadas proporciona conexiones entre **SAPs** del tipo circuito virtual. Este servicio facilita un medio por el cual un usuario puede solicitar ó ser notificado a cerca del establecimiento o terminación de una conexión lógica. También proporciona

control de flujo, secuenciamiento, y corrección de errores. Se puede realizar direccionamiento punto a punto y multiplexado.

El servicio de conexiones orientadas incluye las primitivas `L-DATA-CONNECT.Request` y `L-DATA-CONNECT.Indication`, cuyo significado es análogo al de las descritas anteriormente, más `L-DATA-CONNECT.Confirm`, la cual da idea del resultado (sí se ha confirmado `-ACK-`, sí ha habido un fallo) de su asociado `L-DATA-CONNECT.Request`, a través del parámetro de `Status`. Sí la transferencia fué bien, esta primitiva nos indica que la entidad LLC remota recibió el `1-sdu` y lo confirmó positivamente a través del protocolo de la LLC.

Las siguientes seis primitivas que están listadas en la tabla 5.2 se usan para establecer y desconectar una conexión lógica entre SAPs. El parámetro `Status` indica sí la solicitud (`Request`) ha tenido éxito, y sí no es así, la razón del fallo. El parámetro `Reason`, nos indica la razón de la desconexión de una petición LLC. Las primitivas `L-RESET` se usan para rastrear una conexión lógica a su estado inicial.

Las dos primitivas de control de flujo regulan el flujo de datos a través de los SAPs entre la LLC y sus usuarios. El flujo puede ser controlado en cualquiera de las direcciones. Este es un mecanismo de control de flujo local que especifica la cantidad de datos que pueden ser pasados por el SAP.

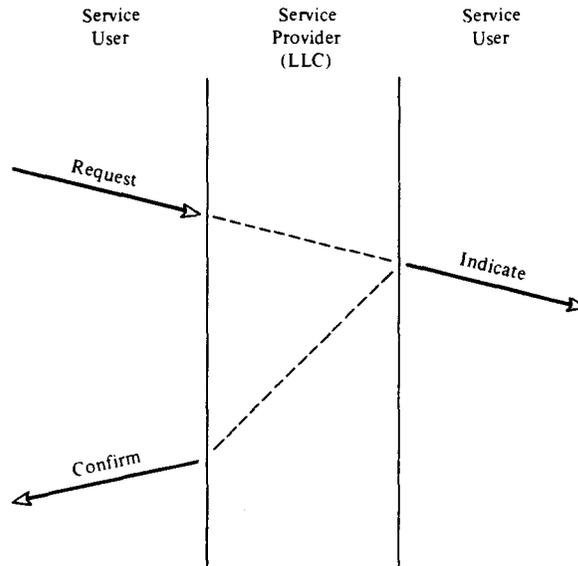


FIGURE 5-5. Relationship Among LLC Primitives

El diagrama de la figura 5.5 puede ayudar a clarificar la relación entre varias primitivas. Una primitiva de solicitud (*Request*) es pasada hacia abajo desde un usuario de LLC hacia la entidad LLC en una estación, para solicitar que la LLC inicie un servicio. La entidad LLC responde mandando un *Frame* a través de la LAN a la otra entidad LLC en otra estación, usando el protocolo que explicamos en el siguiente apartado. Cuando este *Frame* llega, la entidad LLC receptora usa una primitiva de indicación (*Indicate*) para pasar hacia arriba los datos ó el *Status* a uno de sus usuarios. En un servicio de conexiones orientadas, la entidad LLC receptora también envía un *Frame* a través de la LAN que

sirve de confirmación de que el *Frame* ha sido recibido. Cuando esta confirmación es recibida, la entidad LLC original pasa una confirmación hacia arriba a su usuario.

El servicio *Connectionless* con confirmación proporciona un mecanismo por el cual un usuario puede enviar una unidad de dato y recibir una confirmación de que dicha unidad ha sido entregada, sin la necesidad de fijar conexión.

En este servicio se incluyen la *L-DATA-ACK.Request* y la *L-DATA-ACK.Indication*, cuyo significado es análogo al del servicio sin confirmación, más la *L-DATA-ACK-STATUS.Indication* para proveer al usuario de acuse de recibo. Las primitivas *L-REPLY* facilitan un servicio de intercambio de datos. Este servicio permite al usuario el solicitar que el dato sea devuelto de la estación remota ó que se realice un intercambio de unidades de datos con una estación remota. Asociadas a éstas tenemos las primitivas *L-REPLY-UPDATE*, las cuales permiten al usuario pasar datos al LLC para ser mantenidos y enviados posteriormente al recibir una petición de otra estación en este sentido.

El hecho de especificar tres tipos de servicios atiende al deseo de permitir que el LLC se use para soportar una gran variedad de requerimientos del usuario, para facilitar la implementación del LLC para lograr dar solución a las necesidades específicas y para optimizar la implementación de esas necesidades. El servicio sin confirmación es el más simple y el que requiere menor

implementación. En los casos en los que las capas superiores (normalmente la de transporte) nos den control de error y de flujo (End-To-End), se puede usar un servicio mínimo. Por otro lado, el servicio con confirmación, puede ser útil en algunos entornos de tiempo real, como en una LAN de una factoría. Por ejemplo algunas señales de control ó de alarma pueden ser muy importantes, así como críticas con el tiempo. Debido a esta importancia se necesita una confirmación para que el que la envía sepa que la señal ha llegado a su destino.

Protocolo LLC:

El protocolo LLC se modela después del modo balanceado HDLC, y tiene formatos y funciones similares. A lo largo de esta sección, veremos como este protocolo soporta las servicios de LLC definidos con anterioridad.

Primero están los campos de dirección. Tanto el DSAP como el SSAP son campos con direcciones de 7 bits. El bit menos significativo del DSAP nos indica si se trata de una dirección individual o de un grupo. El bit menos significativo del SSAP nos indica si es un *Frame* de comando o de respuesta.

La figura 5.6 muestra el formato para el campo de control del LLC, el cual es idéntico al del HDLC y su funcionamiento el mismo, con cuatro excepciones:

- 1.- El LLC hace uso sólo de un modo de operación asíncrona balanceada, y no emplea el modo de

respuesta normal del HDLC ni el modo de respuesta asíncrono. Este modo es usado para soportar servicios de conexión orientada. El comando **SABM**, se usa para establecer una conexión, y el comando **DISC** sirve para terminar la conexión.

- 2.- El LLC soporta un servicio *Connectionless* usando un *Frame* de información no numerado.
- 3.- El LLC permite la multiplexación por el uso de **SAPs**.
- 4.- El LLC soporta un servicio *Connectionless* con confirmación usando dos nuevos *Frames* no numerados.

	1	2	3	4	5	6	7	8	9	10-16
Information Transfer Command/Response (I-Format PDU)	0	N(S)							P/F	N(R)
Supervisory Commands/Responses (S-Format PDUs)	1	0	S	S	X	X	X	X	P/F	N(R)
Unnumbered Commands/Response (U-Format PDUs)	1	1	M	M	P/F	M	M	M		

Where

- N(S)-Transmitter Send Sequence Number (Bit 2-Low-order Bit)
- N(R)-Transmitter Receive Sequence Number (Bit 10-Low-order Bit)
- S-Supervisory Function Bit
- M-Modifier Function Bit
- X-Reserved and Set to Zero
- P/F-Poll Bit-Command LLC PDU Transmissions
Final Bit-Response LLC PDU Transmissions
(1-Poll/Final)

FIGURE 5-6. IEEE 802 LLC Control Field Format

Como en HDLC; se definen tres formas de *Frame* para LLC: Transferencia de información, supervisión y no numerado. Su uso depende del tipo de operación empleada. Los tipos son:

- Tipo 1 *Connectionless*.
- Tipo 2 Conexión orientada.
- Tipo 3 *Connectionless* con confirmación.

Con la operación tipo 1, las unidades de datos del protocolo (PDUs) son intercambiadas entre entidades LLC sin la necesidad de establecer una conexión lógica. No hay confirmación, control de error, ni de flujo. Este tipo de operación soporta el servicio *Connectionless* sin confirmación.

Se usan tres formatos no numerados de *Frame*. El UI (Unnumbered Information) es usado para enviar un *Frame* de datos *Connectionless* que contiene datos del usuario de una LLC. El XID (Exchange Identification) se usa para dar idea de la "clase" de la estación, es decir, de los tipos de operación que soporta. El TEST se usa para solicitar un *Frame* de prueba (Test) en respuesta, para comprobar el camino entre LLCs.

Con la operación tipo 2, un enlace de datos (Conexión) es establecido entre dos entidades LLC antes del intercambio de datos. Este tipo de operación soporta servicio de conexión orientada y utiliza los tres formatos de *Frame*. Los *Frame* de transferencia de información se usan para enviar datos. N(s) y N(r) son números de

secuencia del *Frame* que tienen control de error y flujo. Una estación que envía una secuencia de *Frames* los numerará, módulo 128, y colocará el número en N(s). El N(r) es una confirmación. El permite a la estación emisora indicar el número del siguiente *Frame* que se espera recibir. Estos números soportan control de flujo ya que, después de enviar siete *Frames* sin una confirmación, una estación no puede enviar más. También soportan control de error como veremos más adelante. El campo P/F se pone a 1 sólo en el último *Frame* de una serie, para indicar que la transmisión se ha acabado.

El *Frame* de supervisión se usa para el control de flujo y para la confirmación. El campo de dos bits SS es usado para indicar uno de tres comandos posibles: Receive Ready (RR), Receive Not Ready (RNR), y Reject (REJ). RR se usa para confirmar el último *Frame* recibido indicando en N(r) el *Frame* esperado a continuación. Este *Frame* se usa cuando no hay tráfico de vuelta para transportar una confirmación *Piggybacked* (remolcado). RNR confirma un *Frame* como RR, pero también le pide a la estación emisora que suspenda la transmisión. Cuando la estación receptora está de nuevo lista envía un *Frame* RR. REJ se usa para indicar que el *Frame* con número N(r) es rechazado y que él y los transmitidos posteriormente deben ser enviados de nuevo.

Los *Frames* no numerados se utilizan para propósitos de control en el nodo de operación tipo 2. El campo de 5

bits **MMMMM** especifica una orden particular ó respuesta.

Estas ordenes comandos son:

- * **SABME** (fija el modo balanceado asíncrono extendido): es usado por una entidad LLC para pedir una conexión lógica con otra entidad LLC.
- * **DISC** (desconexión): usado para terminar una conexión lógica; la estación emisora anuncia con este comando que está suspendiendo las operaciones (el funcionamiento).

Las respuestas son:

- * **UA** (confirmación no numerada): se usa para confirmar los comandos **SABME** y **DISC**.
- * **DM** (modo desconectado): se usa para indicar que la entidad LLC de la estación está lógicamente desconectada.
- * **FRMR** (rechazo de Frame): se usa para indicar que ha llegado un *Frame* incorrecto -un protocolo que de algún modo ha violado el protocolo-.

El bit **P/F** se usa para indicar que se solicita una respuesta a un *Frame* de comando (de orden).

En el tipo 3 de operación, cada *Frame* transmitido es confirmado. Se define un nuevo *Frame* no numerado llamado (AC), (Acknowledged Connectionless Information Frame) el *Frame* de información con confirmación sin conexión. Al contrario de los otros *Frames* usados en la LLC, este *Frame* no está definido en HDLC. Los datos del usuario son enviados en un *Frame* AC de comando y debe ser confirmado

por medio de un *Frame AC* de respuesta. Para la pérdida de *Frames* se utiliza un número de 1 bit. El emisor alterna el uso de 0 y 1 en sus *Frames* de comando, y el receptor responde con un *Frame AC* con el número correspondiente.

Interface LLC-MAC:

La LLC de la IEEE 802 está hecha para operar (funcionar) con cualquiera de los tres protocolos MAC:

- CSMA/CD.
- Token Bus.
- Token Ring.

Está definido un interface lógico simple para cualquiera de las capas del MAC. El estándar 802 no define un interface explícito, pero proporciona un "modelo". Las primitivas básicas son:

- * **MA-DATA.Request:** para solicitar la transferencia de un *Frame LLC* local hasta la LLC de destino. Esto incluye *Frames* de transferencia de información, de revisión y no numerados.
- * **MA-DATA.Confirm:** respuesta desde una capa MAC local a una **MA-DATA.Request** de una capa LLC. Indica el éxito ó fracaso de la petición, pero tiene sólo significado local (no se trata de una confirmación End To End).
- * **MA-DATA.Indicate:** se usa para transferir un *Frame* de LLC entrante (que llega), desde la MAC local a la LLC local.

5.3

CONTROL DE ACCESO AL MEDIO: BUS/ARBOL.

De todas las topologías, las Bus/Arbol presenta los mayores desafíos y las mayores opciones para el control de acceso al medio. Nosotros nos basaremos en dos técnicas que actualmente dominan el mercado:

- CSMA/CD.
- Token Bus.

Los estandars para estas técnicas han sido desarrollados por el comité IEEE 802.

Comentaremos brevemente una tercera técnica, la llamada (Centralized Reservation) "reserva centralizada", que junto a las dos antes mencionadas abarcan totalmente el campo de técnicas de control de acceso al medio para Bus y Arbol.

TABLE 5.3 Bus/Tree Access Methods

	CSMA/CD	Token Bus	Centralized Reservation
Access determination	Contention	Token	Reservation
Packet length restriction	Greater than twofold propagation delay	None	No greater than slot size
Principal advantage	Simplicity	Regulated/fair access	Regulated/fair access
Principal disadvantage	Performance under heavy load	Complexity	Required central controller

La Tabla 5.3 hace una comparación de las tres técnicas.

CSMA/CD:

El control de acceso al medio (MAC) para Bus/Arbol es el "Carrier Sense Multiple Access With Collision Detection" (CSMA/CD) (Acceso múltiple por portadora guiada con detección de colisión). La versión original en banda base de esta técnica fué desarrollada y patentada por Xerox como una parte de su Ethernet LAN. La versión original en banda ancha fué desarrollada y patentada por la casa MITRE como parte de su red local MITREnet. Una versión en banda base inspirada en la Ethernet ha sido publicada como estándar de IEEE 802.

Antes de entrar en el análisis de estas técnicas, veamos de donde provienen.

Precursores:

Todas las técnicas discutidas en esta sección, incluyendo CSMA/CD, pueden englobarse en las llamadas "Random Access Tecnicas" (acceso fortuito ó al azar) ó "Contention Access Tecnicas" (acceso disputado). Estas técnicas están diseñadas para solucionar el problema de como compartir un medio de transmisión común, el problema de ¿quién es el que sigue?. Las técnicas son de acceso fortuito en el sentido de que no existe una predicción ni programación del tiempo de transmisión de cada estación. Y

son de acceso disputado en el sentido de que no se ejerce ningún control que determine de quien es el turno; todas las estaciones deben "luchar" por tiempo en la red.

La primera de estas técnicas, conocida como **ALOHA**, es una verdadera técnica de libertad para todas las estaciones. Cuando quiera que una estación tiene un *Frame* para enviar, lo hace. Entonces la estación permanece a la "escucha" durante un tiempo igual al tiempo máximo de propagación en la red en trayecto de ida y vuelta, (es decir dos veces el tiempo que se tarda en mandar un *Frame* entre las dos estaciones más alejadas de la red). Si la estación "escucha" una confirmación en este tiempo, bien, si no, manda de nuevo el *Frame*. Después de varios fracasos, le llegará la confirmación. Una estación receptora determina la corrección de un *Frame* entrante, examinando la "Check Sum" (Suma de control). Si el *Frame* es correcto, lo confirma inmediatamente. Si no es válido, es debido a ruido en el canal ó por que otra estación transmite otro *Frame* en el mismo tiempo. Si es por esto último, los dos *Frames* van interferir uno con otro y ninguno llega a destino; esto se conoce como "colisión". En este caso, la estación receptora, simplemente ignora el *Frame*. Dada la simplicidad de **ALOHA** se presentan problemas. Dado que el incremento de colisiones aumenta rápidamente con el aumento de carga, la utilización máxima del canal es sólo del 18%.

Para ganar eficiencia se modificó el ALOHA de tal

manera que el tiempo en el canal está organizado en pistas (Slot) uniformes de longitud igual al tiempo de transmisión del *Frame*. Luego es evidente que hace falta un reloj central u otra técnica para sincronizar todas las estaciones. Una transmisión es permitida sólo para empezar en un límite de una pista, de manera que los *Frames* que se solapan lo hacen totalmente. Esto incrementa la utilización máxima del sistema hasta un 37%. Esta modificación se denomina (Slotted ALOHA).

Tanto el ALOHA como el "Slotted ALOHA" son de poca utilización. Ambas técnicas fallan a la hora de aventajar a los LANs en una de sus propiedades principales, ésta es, que el retardo de propagación entre estaciones es usualmente menor que el tiempo de transmisión de un *Frame*. Sí el tiempo de propagación entre estaciones es grande en comparación con el tiempo de transmisión de un *Frame*, entonces, después de que una estación lanza un *Frame*, habrá un tiempo grande antes de que las demás estaciones lo sepan. Durante este tiempo, otra estación puede transmitir un *Frame*; los dos *Frames* pueden interferir uno con el otro y ninguno llegar a destino. Por tanto, si las distancias son lo suficientemente grandes, muchas estaciones pueden empezar a transmitir una tras otra, y ninguno de los *Frames* llegará "ilesos". Supongamos ahora que el tiempo de propagación es extremadamente pequeño comparado con el tiempo de transmisión de un *Frame*. En este caso, cuando una estación lanza un *Frame*, las demás

lo saben casi inmediatamente. Así, si las estaciones tienen algo de inteligencia, no intentarán transmitir hasta que lo haya hecho la primera estación. las colisiones serían mucho menos frecuentes. Sólo ocurrirán cuando dos estaciones empiecen a transmitir simultáneamente.

Lo anteriormente expuesto puede servir para aumentar la eficiencia.

Las observaciones anteriores nos llevan al descubrimiento de una técnica llamada **CSMA** ó **LBT** (Listen Before Talk) que significa "oir antes de hablar". En ella, una estación que desea transmitir, escucha primero el medio para saber si hay otra transmisión en curso. Si el medio se esta usando, la estación espera un tiempo y lo intenta de nuevo, usando los algoritmos que a continuación detallaremos. Si el medio está desocupado, la estación puede transmitir. Pero puede que dos ó más estaciones intenten transmitir aproximadamente a la vez. si esto ocurre, habrá una colisión. Para justificar ésto una estación espera una confirmación durante un tiempo razonable después de la transmisión, teniendo en cuenta el retardo máximo de ida y vuelta entre las estaciones más lejanas, y el hecho de que la estación que confirma puede estar "luchando" por el canal para responder. Si no hay una confirmación, la estación emisora asume que ha habido una colisión y retransmite.

La utilización máxima obtenible con **CSMA** es muy

superior a las de las técnicas ALOHA. Esta va a depender de la longitud del *Frame* y del tiempo de propagación. Cuanto mayor sea el *Frame* ó más corto el tiempo de propagación, mayor es la utilización. Esto será tratado en el capítulo 9.

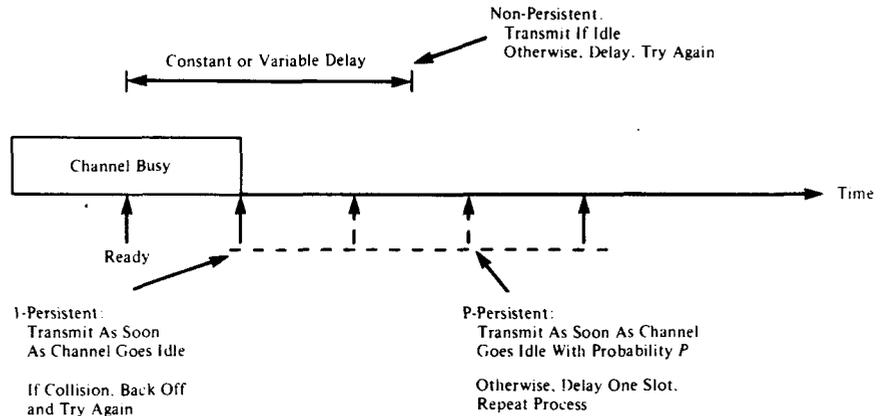


FIGURE 5-7. CSMA Persistence and Back-off

Con la CSMA necesitamos un algoritmo que especifique lo que debe hacer una estación si el medio esta ocupado. En la figura 5.7 tenemos tres de ellos. Un algoritmo es conocido como "Nonpersistent CSMA", en el cual una estación que desee transmitir, escucha el medio y obedece las siguientes reglas:

- 1.- Sí el medio esta desocupado, transmite.
- 2.- Sí el medio esta ocupado, espera un tiempo igual al retardo de transmisión y repite el paso 1.

El uso de tiempos fortuitos (aleatorios) de retransmisión reduce la probabilidad de colisiones. El

inconveniente es que aún teniendo varias estaciones con *Frames* para enviar, habrá probablemente un tiempo perdido de medio desocupado a continuación de una transmisión.

Para evitar ésto, se usa el protocolo denominado "1.Persistent CSMA", en el cual una estación que desee transmitir, escucha el medio y obedece a las siguientes reglas:

- 1º Sí el medio está desocupado, transmite.
- 2º Sí el medio está ocupado, continua escuchando hasta que el medio esté desocupado, entonces transmite inmediatamente.
- 3º Sí hay una colisión (debido a una falta de confirmación), espera un tiempo aleatorio y repite el paso 1.

Mientras las estaciones "Nonpersistent" son deferentes, las "1-Persistent" son "egoístas". Si dos ó más estaciones esperan para transmitir, la colisión está garantizada. Con el algoritmo "P-Persistent" se reducen las colisiones y el tiempo perdido de medio desocupado. Sus reglas son:

- 1º Sí el medio está vacío, transmite con probabilidad P , y espera una unidad de tiempo con probabilidad $(1-P)$. la unidad de tiempo es normalmente igual al retardo máximo de propagación.
- 2º Sí el medio está ocupado, continua a la escucha hasta que el canal está desocupado y repite el

paso 1.

3º Sí la transmisión se retrasa en una unidad de tiempo, repite el paso 1.

La pregunta que surge es ¿cual ha de ser el valor eficiente de p ?. El problema principal es la inestabilidad a grandes cargas . consideremos el caso de " n " estaciones queriendo transmitir *Frames*, mientras se está produciendo una transmisión. al terminar esta transmisión, el número estimado de estaciones que intentarán transmitir es " np ". Sí " np " es mayor que 1, muchas estaciones intentarán transmitir, y se producirá una colisión. Es más, tan pronto como esas estaciones se den cuenta que no han sido cursados sus *Frames* (debido a las colisiones) volverán de nuevo a transmitir, garantizando más colisiones. Peor aún, estos reintentos van a competir con nuevas transmisiones de otras estaciones, incrementando así la probabilidad de colisión. Finalmente, todas las estaciones estarán intentando transmitir causando colisiones continuas. Para evitar ésto, " np " debe ser menor que 1 para los picos de " n " estimados. A medida que " p " se hace menor, las estaciones deben de esperar más tiempo para intentar transmitir pero se reducen las colisiones. A bajas cargas, no obstante, las estaciones sufren retardos innecesariamente largos.

Descripción del CSMA/CD:

La CSMA/CD es apropiada para topologías Bus/Arbol y

es también llamada **LWT** (Listen While Talk) ó lo que es lo mismo: "escucha mientras habla". Esta técnica puede usarse tanto en sistemas de banda ancha como de banda base. Como existen detalles que diferencian una de otra, usaremos la **IEEE 802** y la **MITREnet** como ejemplos a comparar.

La **CSMA**, aunque más eficiente que la **ALOHA**, y **Sloted ALOHA**, tiene un notorio problema; cuando dos *Frames* colisionan, el medio permanece inutilizable durante el tiempo de transmisión de dos *Frames* dañados. Para *Frames* largos, comparados con el tiempo de propagación, la cantidad de ancho de banda perdida puede ser considerable. Esta pérdida puede ser reducida si una estación continua escuchando el medio mientras transmite. En ese caso, a las reglas del **CSMA** hay que añadir las siguientes:

- 1.- Si se detecta una colisión durante la transmisión, inmediatamente se cesa la transmisión del *Frame* y se transmite una señal de "Jamming" (atasco) para asegurar que todas las estaciones sepan que ha habido una colisión.
- 2.- Después de transmitir esta señal del *Jamming*, espera un tiempo aleatorio e intenta transmitir de nuevo usando el **CSMA**.

Ahora, la cantidad de ancho de banda perdida se reduce al tiempo que trata de detectarse una colisión. La figura 5.8 ilustra el tiempo que se tarda en detectar una colisión en un sistema de banda base. Consideremos el caso más desfavorable, es decir cuando las estaciones están lo

más alejadas posible. Como puede verse, el tiempo que se tarda en detectar una colisión es el doble del retardo de propagación (2a). Para un Bus de banda ancha es incluso mayor. La figura 5.9 representa un sistema dual de cables. Esta vez, el caso peor es el de dos estaciones cercanas entre sí y lo más alejadas posible de la cabecera final. En este caso, el tiempo necesario para detectar una colisión es de cuatro veces (4a) el retardo de propagación desde la estación hasta la cabecera final.

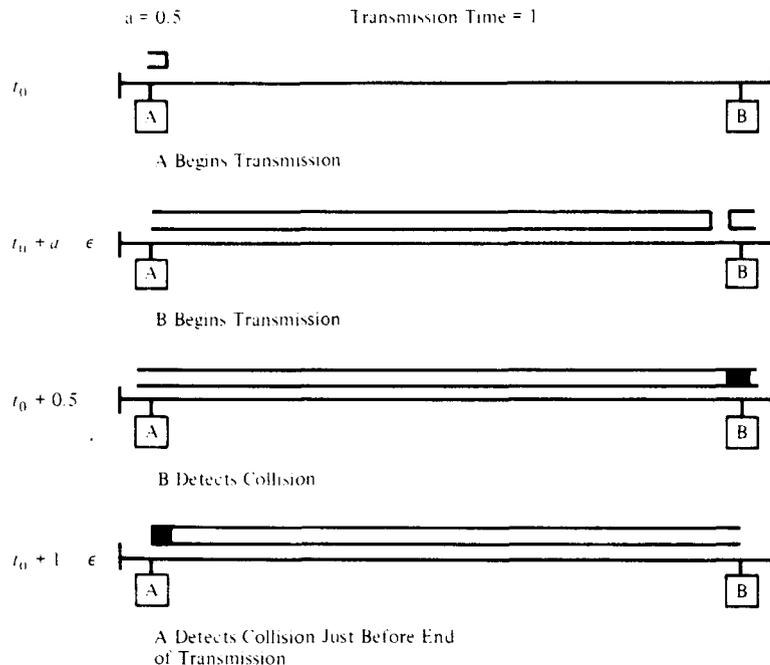


FIGURE 5-8. Baseband Collision Detection Timing

En ambas figuras se indica el uso de *Frames* lo suficientemente largos para permitir una prioridad de la detección de colisiones (CD) frente al final de

transmisión. En la mayoría de los sistemas que usan CSMA/CD, se requiere que todos los Frames tengan al menos esta longitud. De otra manera el rendimiento del sistema es el mismo que el menos eficiente de los protocolos CSMA, en donde las colisiones se detectan sólo después de acabar la transmisión.

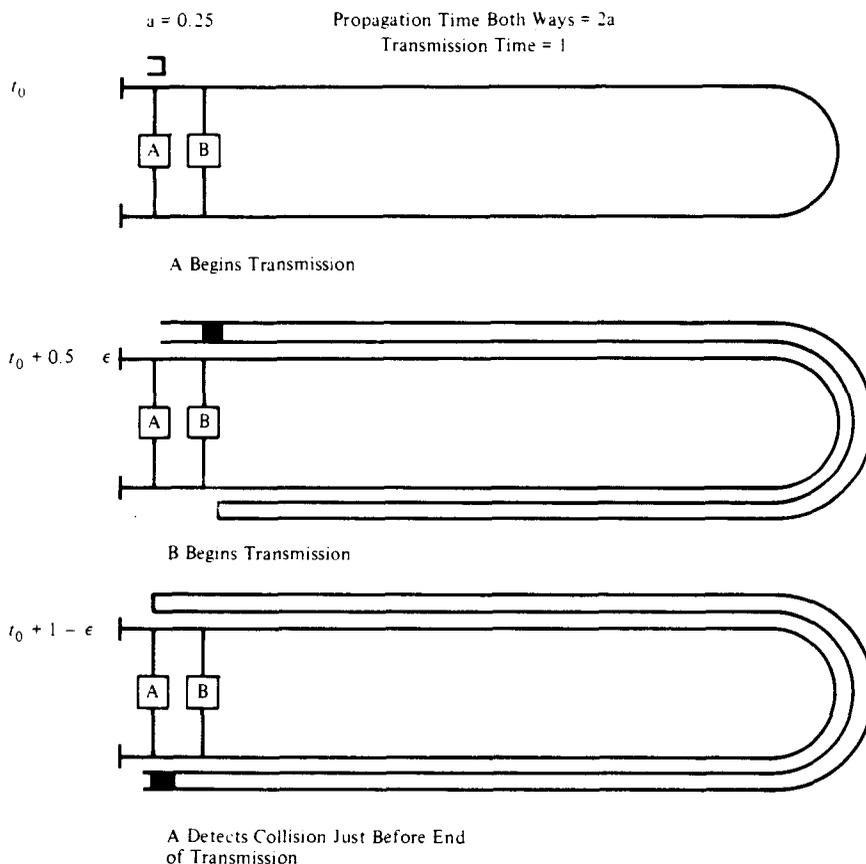


FIGURE 5-9. Broadband Collision Detection Timing

Ahora veamos una serie de detalles del CSMA/CD. Primero veamos qué algoritmo de persistencia se usa. El más usado es 1-Persistent; éste es utilizado tanto en la Ethernet como en la MITREnet y en el estándar de IEEE

802. Tenemos que tener en cuenta que tanto el **Nonpersistent** como el **P-Persistent** tienen problemas de rendimiento. En el caso del primero, se pierde capacidad debido a que el medio permanecerá desocupado después del final de una transmisión, incluso si hay estaciones esperando para transmitir. En el caso del segundo, "p" debe ser lo suficientemente bajo como para evitar la inestabilidad, con el resultado de tener retrasos enormes a baja carga (bajo tráfico). El algoritmo **1-Persistent** (que después de todo significa $p=1$), puede parecer más inestable que el **P-Persistent** en función de la avidez de las estaciones. Lo que lo salva es que el tiempo perdido junto de las colisiones es bastante corto (siempre que los Frames sean largos en relación al retardo de propagación), y retiradas (Backoff) aleatorias, es poco probable que colisionen en los próximos intentos. Para asegurar que estas retiradas aleatorias mantienen la estabilidad, la **IEEE 802** y **Ethernet** usa una técnica llamada retirada binaria exponencial. Una estación intentará transmitir repetidamente a la vista de colisiones que se suceden, pero después de cada colisión, el valor medio de cada retardo aleatorio es doblado. Después de 16 intentos frustrados, la estación lo deja e informa de un error.

Lo bueno del algoritmo **1-Persistent** con retirada binaria exponencial es que resulta eficiente en una gran variedad de cargas. A bajas cargas garantiza que una estación puede apoderarse del canal tan pronto esté vacío.

Al contrario que los otros dos algoritmos. Con altas cargas es al menos tan estable como las otras técnicas. No obstante, un desafortunado efecto del algoritmo de retirada es el de LIFO (Last-In, First-Out); estaciones con pocas o ninguna colisión tendrán antes la oportunidad de transmitir que otras que llevan más tiempo esperando.

Aunque la implementación de la CSMA/CD para banda base y banda ancha es substancialmente la misma, hay diferencias. Una de ellas es el significado de la portadora guiada. Para los sistemas banda base con codificación Manchester, la portadora es convenientemente guiada detectando la presencia de transiciones en el canal. Hablando estrictamente, no hay portadora para guiar la señal digital; el término está sacado del léxico de radio. En banda ancha si se lleva a cabo. La estación receptora escucha en busca de la presencia de una portadora en el canal de salida.

La detección de colisiones también difieren en uno y otro sistema. En un sistema banda base, una colisión podría producir impulsos de voltaje sustancialmente superior a los producidos por un sólo transmisor. En concordancia, Ethernet y la IEEE 802 indican que un transceptor que transmite detectará una colisión si la señal en el cable (en el transceptor) excede el máximo que podría ser producido por el transceptor por sí sólo. Como una señal transmitida se va atenuando a medida que se propaga, hay un problema potencial con la detección de

colisión. Si dos estaciones alejadas están transmitiendo, cada estación recibirá una señal muy atenuada de la otra. La fuerza de la señal puede ser tan pequeña, que cuando es añadida a la de la señal transmitida en el transceptor, la señal resultante no supera el nivel de disparo del CD. Debido a ésto, la **IEEE 802** reduce la longitud máxima del cable a 500 metros. Ya que los Frames pueden atravesar los límites de los repetidores, las colisiones también pueden. Luego, si un repetidor detecta una colisión en cualquier cable, debe transmitir una señal de *Jamming* al otro lado. Como la colisión puede no suponer una transmisión desde el repetidor, el disparo del CD es diferente para un transceptor que no transmite: una colisión es detectada si la fuerza de la señal excede a aquella que puede ser producida por dos salidas de transceptores en el peor caso.

La dificultad de la detección de colisiones en sistemas banda base con par trenzado en estrella cableada (figura 3.5a) es menor. El Bus en el armario de cableado (Wiring Closet) es tan corto que no hay atenuación apreciable en la señal entre los diferentes puntos de conexión sobre él. Por tanto, se puede usar un método de detección basado en la lógica en vez de en la magnitud del voltaje. Si se utiliza una codificación **Manchester**, debería haber una transición en medio de cada bit, de tal manera que siempre haya un cruce a cero en mitad de cada bit. Una colisión hará que este cruce se desplace, a la

vez que la cancelación y adición de voltajes.

El método más común usado en sistemas de banda ancha consiste en realizar una comparación bit a bit entre los datos transmitidos y los recibidos. Cuando una estación transmite a través del canal envío transmisión (Inbound) comienza a oír su propia transmisión en el canal de recepción (Outbound) después de un cierto retardo de propagación hacia la cabecera final y vuelta. En el sistema MITRE, los 16 primeros bits de las señales transmitidas y recibidas son comparados. Si hay diferencias se asume la colisión. El mayor problema de este método es que diferencias en el nivel de la señal entre señales que colisionan haga que el receptor trate a la señal débil como ruido y no detecte la colisión. Debemos ajustar bien todo el sistema; cables, tomas, divisores y amplificadores, para que este problema no se produzca. Otro problema para sistemas de cable dual, es que una estación puede transmitir y recibir a la vez en la misma frecuencia. Sus dos modems de RF (radio frecuencia) deben ser protegidos cuidadosamente para evitar cruces.

El estándar CSMA/CD de IEEE 802:

El estándar CSMA/CD de IEEE 802 es muy similar a la Ethernet. En la figura 5.2 se muestra la estructura de los *Frames* del MAC CSMA/CD. Los campos son los siguientes:

- * Preámbulo (Preamble): Consta de 7 bits y es utilizado por el receptor para establecer la

sincronización de los bits y por tanto localizar el primer bit de un *Frame*.

- * Delimitador de comienzo de *Frame* (SFD) (Start Frame Delimiter): Indica el comienzo de un *Frame*.
- * Dirección de destino (Destination Address) (DA): Especifica la(s) estación(es) a la(s) que va dirigido. Puede ser una dirección física única (sólo una estación como destino), una dirección de grupo (varias estaciones destinatarias), ó una dirección global (todas las estaciones de la red local). La elección de una dirección de 16 ó 48 bits es una decisión de implementación, y debe ser la misma para todas las estaciones en una determinada LAN.
- * Dirección fuente (Source Address) (SA): Especifica la estación que envía el *Frame*. La talla de la SA debe ser la misma que la DA.
- * Longitud (Length): Indica el número de bytes de LLC que siguen.
- * LLC: Es un campo preparado en el nivel LLC.
- * Relleno (Pad): Secuencia de bytes añadidos para asegurar que el *Frame* es lo suficientemente largo para el correcto funcionamiento de la CD (detección de colisión).
- * Secuencia de comprobación de *Frame* (Frame Check Sequence) (FCS): Un valor de 32 bits de Checking

cíclico redundante. Se basa en todos los campos, comenzando por la dirección de destino.

Token Bus:

Se trata de una técnica relativamente nueva para controlar el acceso a un medio de difusión multipunto (Broadcast), inspirado por la técnica "Token Ring" que veremos más adelante. Veremos primero una visión general, y luego estudiaremos algunos detalles de la especificación de la IEEE 802.

Descripción:

La técnica **Token Bus** es mas compleja que la **CSMA/CD**. Para esta técnica, las estaciones del Bus ó Arbol forman un Anillo lógico: es decir, a las estaciones se les asignan unas posiciones lógicas en una secuencia ordenada, con lo que el último miembro de la secuencia sigue siguiendo al primero. Cada estación conoce la identidad de las estaciones precedente y siguiente a ella. El ordenamiento físico de las estaciones en el Bus es irrelevante e independiente de la ordenación lógica. En la figura 5.10 se ve ésto (a trazos el orden lógico).

Un *Frame* de control denominado "Token" (contraseña, señal) regula el derecho del acceso. El **Token Frame** contiene una dirección de destino. A la estación que recibe el *Token* se le asegura el control del medio durante un tiempo especificado. La estación puede transmitir uno ó

más *Frames* y puede hacer un *Polling* (Encuesta) a las demás estaciones y recibir respuestas. Cuando la estación acaba, ó se termina su tiempo, ésta pasa el *Token* a la siguiente estación en orden lógico. Esta otra estación tiene permiso ahora para transmitir. En el Bus pueden haber estaciones que no usen *Token*. Estas estaciones sólo pueden responder a encuestas y hacer confirmaciones.

Este diseño implica un mantenimiento considerable. Las siguientes funciones deben ser realizadas por una ó más estaciones en el Bus:

- * Inicialización del Anillo: Cuando se pone en marcha la red, ó después de descomponer el Anillo, éste debe ser inicializado. Se necesita pues un algoritmo cooperativo, descentralizado para ordenar quien va primero, quien en segundo lugar, y así sucesivamente.
- * Adiciones al Anillo: Periódicamente, estaciones no participantes en el sistema deben tener la oportunidad de integrarse en el Anillo.
- * Exclusión del Anillo: Una estación debe ser capaz de excluirse del Anillo uniéndose a su estación predecesora y sucesora.
- * Recuperación: Pueden ocurrir errores, incluyendo direcciones duplicadas (dos estaciones piensan que es su turno) y rotura del Anillo (ninguna estación piensa que es su turno).

El Token Bus de la IEEE 802:

El protocolo Token Bus de la IEEE 802 sigue los principios generales anteriormente descritos. En la figura 5.2 se puede observar la estructura de *Frame* para MAC en un Token Bus. Los campos se numeran como sigue:

- * **Preámbulo:** Un conjunto de uno ó más bytes usados por el receptor para establecer la sincronización de bits para localizar el primer bit del *Frame*.
- * **Delimitador de comienzo (Start Delimiter) (SD):** Indica el comienzo de un *Frame*.
- * **Formato del *Frame* (FC):** Indica sí éste es un *Frame* de datos de LLC. Sí no, los bits de este campo controlan el funcionamiento del protocolo MAC del Token Bus. Un ejemplo de ésto es el *Frame* de Token (de contraseña).

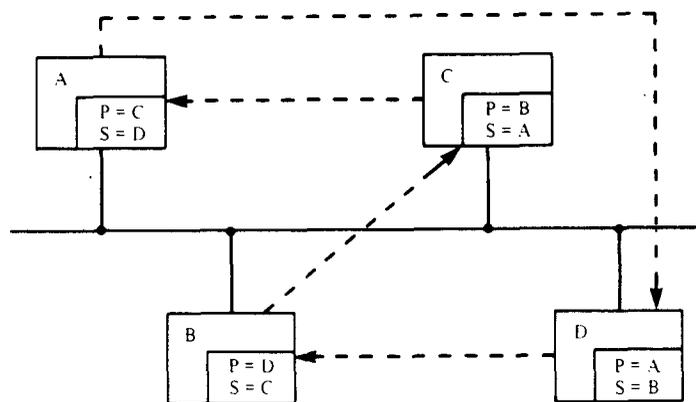


FIGURE 5-10. Token Bus

- * **Dirección de destino (DA):** Igual que en CSMA/CD.

- * Dirección fuente (SA): Igual que en CSMA/CD.
- * LLC: En un campo preparado por LLC.
- * Secuencia de comprobación de *Frame* (SGF):
Igualmente que en CSMA/CD.
- * Delimitador de fin (End Delimiter) (ED): Indica
el final del *Frame*.

Los pormenores del protocolo pueden agruparse en las siguientes categorías:

- * Adición de un nodo.
- * Extracción (eliminación) de un nodo.
- * Fallo en la gestión del poseedor del *Token*.
- * Inicialización del Anillo.
- * Clases de servicios.

Primero, vamos a ver como se realiza la adición de un nodo usando un proceso de contención controlado llamado "ventana de respuesta". Cada nodo en el Anillo tiene la responsabilidad de dar, cada cierto tiempo, la oportunidad de que unos pocos nodos entren en el Anillo. Mientras tiene el *Token*, el nodo envía un *Frame* de solicitud de sucesor (Solicit-Successor), invitando a los nodos con dirección lógica entre sí y el siguiente nodo a pedir entrada. Entonces, el nodo transmisor espera durante una ventana de respuesta o porción (Slot) de tiempo (igual a dos veces el retardo máximo de propagación punto a punto del medio). Pueden darse cuatro situaciones diferentes:

- 1.- No hay respuesta: Nadie quiere entrar. El poseedor del *Token* lo pasa a su sucesor como

siempre.

- 2.- Una respuesta: Un nodo envía un *Frame* de establecimiento de sucesor (*Set-Successor*). El poseedor del *Token* fija su nodo sucesor para que sea el nodo peticionario y le envía el *Token* a él. Este último fija sus eslabonamientos de forma correcta y prosigue.
- 3.- Respuesta múltiple: El poseedor del *Token* detectará una respuesta alternada si más de un nodo quiere entrar. El conflicto se resuelve mediante un esquema de contención basado en las direcciones. El poseedor del *Token* envía un *Frame* de resolución de contención (*Resolve-Contention*), y espera cuatro ventanas de respuesta. Cada demandante puede contestar en una de estas ventanas basado en los dos primeros bits de sus direcciones. Si un demandante oye algo antes de que su ventana aparezca, se abstiene de pedirlo más. Si el tenedor del *Token* recibe un *Frame* válido de establecimiento de sucesor, este nodo entra. Si no es así, lo intenta de nuevo, y sólo aquellos nodos que han respondido la primera vez pueden hacerlo ahora, basados en el segundo par de bits de sus direcciones. Este proceso continua hasta que se recibe un *Frame* válido de establecimiento de sucesor, no se reciba respuesta alguna, ó hasta

que se llegue a un número máximo de reintentos. En los últimos dos casos, el tenedor del *Token* abandona y pasa el *Token*.

4.- Respuesta inválida: Sí el tenedor oye otro *Frame* que no sea el de establecimiento de sucesor, asume que otra estación piensa que ella tiene el *Token*. Para evitar conflictos, la estación se pone en un estado de escucha ó de desocupado.

TABLE 5.4 Token Bus Error Handling

Condition	Action
Multiple token	Defer/drop to 1 or 0
Unaccepted token	Retry
Failed station	“Who follows” process
Failed receiver	Drop out of ring
No token	Initialize after time-out

La eliminación de un nodo es mucho más simple. Sí un nodo desea salir del Anillo lógico, espera a recibir el *Token*, y entonces envía un *Frame* de fijación de sucesor a su predecesor (la estación que le ha transmitido el *Token*) incluyendo la dirección de su sucesor. Luego la estación que desea salir envía el *Token* a su sucesor como siempre. En la próxima vuelta el que fuera predecesor del nodo saliente enviará el *Token* al que fuera sucesor del nodo

saliente. Cada vez que una estación recibe un *Token*, automáticamente fija la dirección de su predecesor a la misma que la dirección de fuente del *Frame* de *Token*. De este modo la estación queda fuera del Anillo lógico.

El fallo en la gestión del tenedor del *Token* incluye una serie de contingencias listadas en la tabla 5.4. En primer lugar, teniendo el *Token*, una estación puede oír un *Frame* indicando que otro nodo tiene el *Token*. Si es así, inmediatamente deja el *Token*, pasando a un estado de escucha. De este modo, el número de tenedores de *Tokens* bajará a 1 ó 0, solventando así el problema de multi-*Token* (que puede estar causado por dos nodos con la misma dirección). Los tres sucesos siguientes de la tabla se producen en la transmisión del *Token*. Al acabar su turno, el tenedor del *Token* envía un *Frame* de *Token* a su sucesor. Este podría enviar inmediatamente un *Frame* de datos ó de *Token*. No obstante, después de enviar un *Token*, el nodo emisor escuchará durante una porción (*Slot*) de tiempo para asegurar que su sucesor está activo. Esto precipita una serie de acontecimientos:

- 1.- Sí el nodo sucesor está activo, el nodo emisor del *Token* oirá un *Frame* válido y pasará a modo de escucha.
- 2.- Sí el emisor del *Token* oye una transmisión alterada, espera cuatro porciones de tiempo. Sí oye un *Frame* válido, asume que su *Token* ha llegado a destino. Sí no oye nada, supone que el

Token ha sido alterado y lo retransmite.

- 3.- Sí el emisor no oyó un *Frame* válido, envía de nuevo el *Token* al mismo sucesor una vez más.
- 4.- Después de dos fracasos, el emisor supone que su sucesor ha fallado y envía un *Frame* de ¿quien sigue? (*Hho-Follows-Frame*), preguntando la identidad (dirección) del nodo que sigue al nodo fallido. El emisor debería recibir un *Frame* de establecimiento de sucesor desde el segundo nodo línea abajo. Sí es así, el emisor ajusta su eslabonamiento y envía un *Token* (se vuelve al paso 1.).
- 5.- Sí el nodo emisor no obtiene respuesta a su *frame* de ¿quien sigue?, lo intenta de nuevo.
- 6.- Sí la táctica de ¿quien sigue? falla, el nodo envía un *Frame* de "solicitud de sucesor" invitando a todos los nodos a responder. Sí funciona, se forma un Anillo de dos nodos y se sigue trabajando.
- 7.- Sí la técnica de la solicitud de sucesor falla, el nodo asume que ha ocurrido un fallo mayor; todas las estaciones han fallado todas han dejado el Anillo, se ha roto el medio, ó el receptor de la estación tenedora falla. En este punto, sí la estación tiene datos para enviar los envía y trata de pasar de nuevo el *Token*. Luego cesa la transmisión y escucha el medio.

La inicialización lógica de un Anillo se produce si una ó más estaciones detectan una carencia de actividad en el Bus por un espacio de tiempo mayor que un cierto *Time-Out* (tiempo de espera): el *Token* se ha perdido. Esto puede deberse a varios motivos como el que la red se acabe de conectar, ó que una estación tenedora del *Token* falle. Una vez que expire el *Time-Out*, un nodo envía un *Frame* de "reclamación de *Token*". La prioridad de las reclamaciones se resuelve de un modo similar al proceso de las ventanas de respuesta. Cada reclamante envía un *Frame* de reclamación de *Token* relleno por 0,2,4, ó 6 porciones basadas en los dos primeros bits de su dirección. Después de la transmisión, un reclamante oye el medio, y si oye algo abandona su reclamación. De otro modo, lo intenta de nuevo con el segundo par de bits de su dirección. El proceso se repite. Solo aquellas estaciones que han transmitido más en el intento previo lo hacen de nuevo, usando pares sucesivos de sus direcciones. Cuando se acaben todos los bits de dirección, el nodo que haya vencido en la última iteración se considera en posesión del *Token*. Ahora el Anillo puede ser reconstruido mediante el proceso de ventanas de respuesta.

Un *Token Bus* puede incluir como opción un mecanismo de establecer acceso priorizado al Bus llamado "clases de servicio". Están descritas cuatro clases de servicios en orden descendente:

- * Síncrono (6).

- * Asíncrono Urgente (4).
- * Asíncrono Normal (2).
- * Asíncrono tiempo-disponible (0).

Toda estación debe tener datos en una ó varias de estas clases para enviar. El objetivo es asignar a los *Frames* de mayor prioridad el ancho de banda de la red y sólo enviar *Frames* de prioridad baja cuando hay suficiente ancho de banda. Para explicarlo definimos las siguientes variables:

- * *THT Token Holding Time*: es el tiempo máximo que una estación puede mantener el *Token* en su poder para enviar datos de la clase 6 (síncrono).
- * *TRT4 Token Rotation Time* para la clase 4: Es el tiempo máximo que un *Token* puede tomar para circular y permitir todavía la transmisión de datos de clase 4.
- * *TRT2 Token Rotation Time* para la clase 2.
- * *TRT0 Token Rotation Time* para la clase 0.

Cuando una estación recibe un *Token*, puede transmitir clases de datos de acuerdo con las siguientes reglas (figura 5.11):

- 1.- Puede transmitir durante un tiempo *THT* datos de clase 6. Por lo tanto, para un Anillo con 'n' estaciones, por cada circulación completa del *Token*, el tiempo disponible para transmisiones de datos de la clase 6 es $n \times THT$.
- 2.- Después de transmitir los datos de clase 6, ó sí

no hubiesen datos de la clase 6 para enviar, puede transmitir datos de clase 4 sólo si el tiempo que ha tardado el *Token* en dar la última circulación completa (incluyendo cualquier dato de clase 6 enviado) es menor que $TRT4$.

3.- La estación a continuación puede enviar datos de clase 2 sólo si el tiempo empleado por el *Token* en la última circulación (incluyendo cualquier dato de clase 6 y clase 4 enviados) es menor que $TRT2$.

4.- La estación puede enviar ahora datos de la clase 0 sólo si el tiempo empleado por el *Token* en la última circulación (incluyendo cualquier dato de las clases 6, 4, y 2 enviados) es menor que $TRT0$.

Este diseño dá preferencia a *Frames* de mayor prioridad. Garantiza, al menos, que los datos clase 6 puedan tener una cierta porción del ancho de banda. Hay dos casos posibles. Si $n \times THT$ es mayor que $\text{MAX}[TRT4, TRT2, TRT0]$, el tiempo máximo posible de circulación del *Token* es $n \times THT$, y los datos de clase 6 ocuparán el ciclo con la exclusión de las otras clases. Si $n \times THT$ es menor que $\text{MAX}[TRT4, TRT2, TRT0]$ el tiempo máximo de circulación es $\text{MAX}[TRT4, TRT2, TRT0]$, y los datos de clase 6 tienen garantizado un tiempo $n \times THT$ de ese tiempo máximo.

La figura 5.12 es un ejemplo simplificado de Anillo

de 4 estaciones con un $THT = 610$ y un $TRT_4 = TRT_2 = TRT_0 = 1600$ octetos.

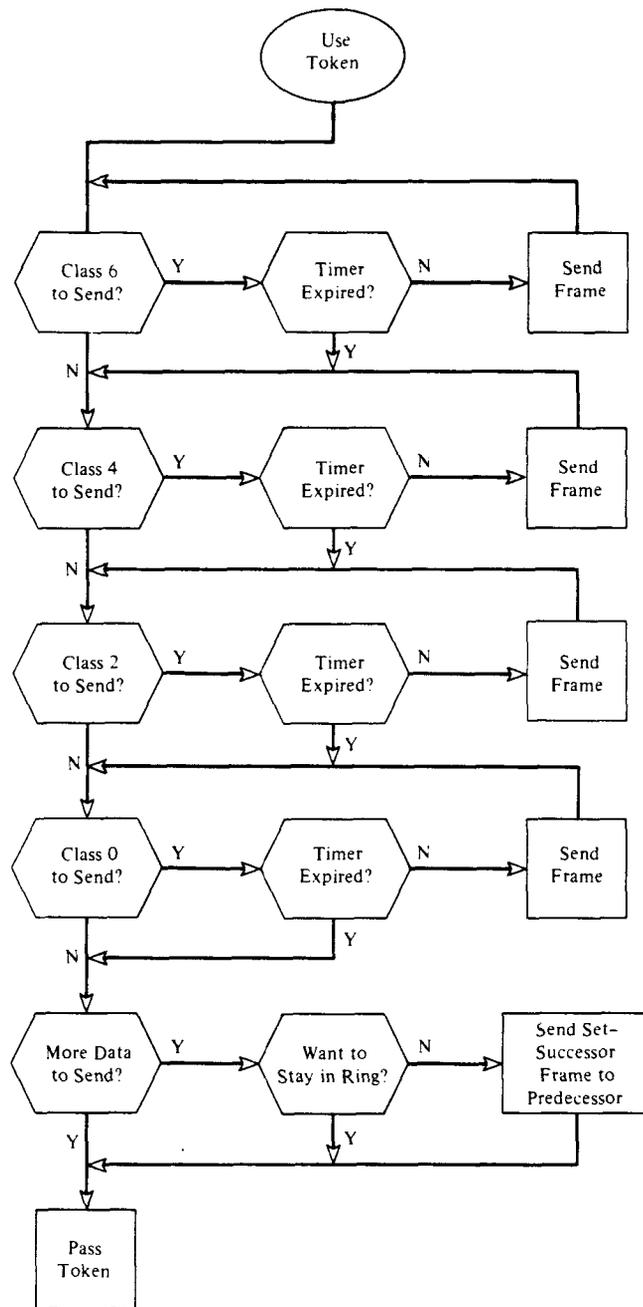


FIGURE 5-11. Token Bus Priority Scheme

La estación 9 siempre transmite tres *Frames* clase 6 de 128 octetos cada uno. Las estaciones 7 y 5 envían

tantos *Frames* de baja prioridad como pueden, con longitud de 400 y 356 octetos respectivamente. La estación 1 transmite *Frames* de clase 6 de 305 octetos cada uno. Inicialmente la estación 1 tiene dos *Frames* para enviar cada vez que tenga el *Token*, y después tiene sólo 1 *Frame* para enviar por cada posesión de *Token* (ver la columna *XMIT*. Suponemos que el tiempo para pasar el *Token* es de 19 octetos. En la figura podemos ver dos columnas de números debajo de cada estación. Los valores en la de la izquierda es el tiempo de circulación del *Token* observado por esa estación en la rotación anterior. Los valores de la columna de la derecha es el número de *Frames* que transmite la estación. Cada fila representa una rotación del *Token*.

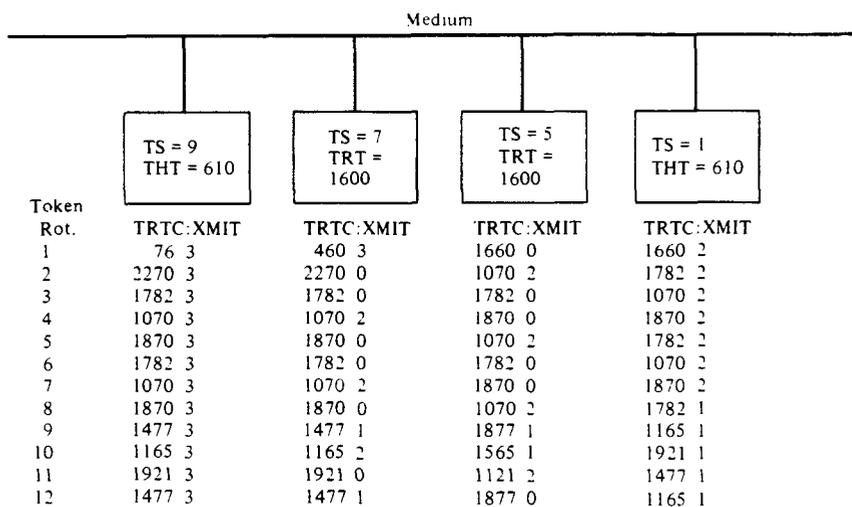


FIGURE 5-12. Operation of a Multiclass Token Bus Protocol

El ejemplo comienza después de un período en el que no se han enviado *Frames* de datos, así que el *Token* ha estado rotando lo más deprisa posible; por lo tanto cada estación mide un tiempo de circulación del *Token* de 76 ($n \times 19 = 4 \times 19 = 76$). En la primera rotación, la estación 9 transmite todos sus *Frames* de clase 6. Cuando la estación 7 recibe el *Token*, estima un tiempo de rotación de 460 desde la última vez que recibió el *Token* ($3 \times 128 + 4 \times 19$). Por lo tanto puede enviar tres de sus *Frames* antes de que se agote su TRT. La estación cinco estima un tiempo de rotación de 1160 ($3 \times 400 + 3 \times 128 + 4 \times 19$) y por lo tanto no puede enviar ningún dato ya que su TRT es igual a 1600. Finalmente, la estación 1 envía dos *Frames* clase 6.

Obsérvese que las rotaciones de la 5ª a la 7ª son una repetición de las rotaciones 2ª a 4ª, mostrando así una localización estable del ancho de banda: Las estaciones 1 y 9 utilizan un 69% del ancho de banda para datos de clase 6 y las estaciones 5 y 7 comparten por igual el ancho de banda restante para datos de menor prioridad. Empezando en la 8ª rotación, la estación 1 reduce su uso de la LAN. Esto hace que el ancho de banda usado para datos de clase 6 disminuya hasta un 52%, de manera que los datos de menor prioridad pueden llenar el ancho de banda no usado.

CSMA/CD Versus Token Bus:

Actualmente estas dos técnicas son las más usadas y

extendidas para topologías Bus/Arbol. En la tabla 5.5 se listan los pros y los contras de ambas técnicas.

Analicemos primero el CSMA/CD. Su algoritmo es simple; esto es conveniente para procesos de VLSI y conveniente también para el usuario en términos de coste y confiabilidad. Este protocolo ha sido usado ampliamente durante mucho tiempo, lo que incide en su costo y fiabilidad. Proporciona un acceso equitativo ya que todas las estaciones tienen las mismas oportunidades en el ancho de banda. Como veremos más adelante, el CSMA/CD tiene un buen retardo y rendimiento de transmisión, al menos para cargas hasta 5 Mbps.

TABLE 5.5 CSMA/CD versus Token Bus

Advantages	Disadvantages
<i>CSMA/CD</i>	
Simple algorithm	Collision detection requirement
Widely used	Fault diagnosis problems
Fair access	Minimum packet size
Good performance at low to medium load	Poor performance under very heavy load
	Biased to long transmissions
<i>Token Bus</i>	
Excellent throughput performance	Complex algorithm
Tolerates large dynamic range	Unproven technology
Regulated access	

Los contras del CSMA/CD son pocos. Desde el punto de vista de la ingeniería, el problema crucial es el requerimiento de la detección de colisión. Para ello la diferencia de fuerza entre señales de diferentes

estaciones debe ser pequeña; ésta no es una tarea fácil. Por otro lado, al permitirse colisiones, el equipo de diagnóstico tiene dificultades para distinguir los errores esperados de los provocados por fallos ó ruido. Este requerimiento (CD) incluso impone un tamaño mínimo al *Frame*, lo que provoca un desaprovechamiento de ancho de banda en situaciones donde hay muchos mensajes cortos.

También tiene problemas de rendimiento para ciertas velocidades y tamaños de *Frame*, el rendimiento del CSMA/CD disminuye a medida que aumenta la carga.

Para el **Token Bus**, hay que señalar como mejor cualidad su excelente rendimiento de transmisión. La transmisión aumenta con la velocidad y con la disminución de los niveles pero no disminuye al saturarse el medio. Es más, este rendimiento no disminuye con el aumento de longitud del cable. Una segunda cualidad positiva es que, debido a que las estaciones necesitan detectar las colisiones, es posible un rango dinámico bastante largo. El único requerimiento es que la fuerza de las señales de cada estación sea la suficiente para que puedan ser oídas en todos los puntos del cable.

Otra virtud del **Token Bus** es que el acceso al medio puede ser regulado. Si se desea un acceso igualitario, el **Token Bus** puede proporcionarlo como el CSMA/CD. Si se necesitan prioridades, también puede proporcionarlas. El **Token Bus** puede incluso garantizar un cierto ancho de banda; ésto es necesario para ciertos tipos de datos tales

como voz, video digital y telemetría.

Otra ventaja ya mencionada es su carácter determinístico; ésto es, hay un límite superior para el tiempo que cualquier estación debe esperar antes de transmitir. Este límite superior es conocido ya que cada estación puede tener el *Token* durante un tiempo especificado. En contraste, el retardo CSMA/CD debe ser expresado estadísticamente. Es más, como cada transmisión en CSMA/CD puede en principio causar una colisión, hay una posibilidad de que una estación pueda ser excluida indefinidamente. Para procesos de control ó de tiempo real, esta conducta "no determinística" es indeseable.

El principal inconveniente del *Token Bus* es la complejidad de su algoritmo como ya vimos. Una desventaja más es que para cargas bajas, una estación puede tener que esperar muchos pases de *Token* infructuosos para tomar turno.

¿Cual elegir?. Hay que tener en cuenta los requerimientos y los costos relativos, así como la elección de un sistema banda ancha ó banda base.

Reserva centralizada:

En esta sección estudiaremos una técnica que requiere control centralizado. Esta es una candidata muy apropiada para un sistema de ancho de banda, donde la función de control está ejercida en las cabeceras.

El diseño centralizado que estudiamos en esta sección

fué desarrollado por AMDAX para su LAN de banda ancha. Fijó un tamaño de *Frame* de 512 bits. El tiempo está organizado en ciclos, cada ciclo está formado por un conjunto de particiones de tiempo idénticas, y cada una de estas particiones es suficiente para transmitir un *Frame*. Los ciclos se suceden uno tras otro. El controlador central en la cabecera puede asignar posiciones de *Frame* o particiones, dentro de ciclos venideros, a estaciones particulares. Las posiciones de *Frame* no asignadas a ninguna estación se denominan "Frames no asignados". Todas las estaciones deben permanecer informadas de cuales son los *Frames* asignados a ella y cuales son los no asignados.

Desde el punto de vista de la estación, la comunicación es como sigue. Si una estación tiene un *Frame* pequeño que enviar, uno que quepa en un sólo *Frame*, lo envía en el próximo *Frame* no asignado disponible, a través del canal de transmisión. Este *Frame* contendrá el mensaje, la dirección fuente y de destino, así como información de control indicando que es un *Frame* de datos. Dado que la posición del *Frame* usado no está asignada, podría ser utilizado por otra estación, causando una colisión. Por tanto la estación emisora debe oír el canal de recepción para su transmisión. Si la estación no ve su *Frame* transcurrido un tiempo corto y definido, continua mandando el *Frame* esporádicamente hasta que se curse su envío.

Para mandar mensajes demasiado grandes como para caber en un sólo *Frame*, la estación puede reservar tiempo

en el Bus. Esto lo realiza enviando una petición de reserva al controlador central por el canal de emisión. La petición usa un *Frame* no asignado conteniendo una indicación especificando su naturaleza, las direcciones fuente y de destino, y el número de *Frames* a enviar. La estación luego escucha el canal de recepción durante un tiempo corto definido, esperando recibir un *Frame* de confirmación de reserva conteniendo su dirección y el número y el orden de los *Frames* que le han sido asignados en ciclos futuros (si la línea está altamente cargada, no obtendrá todo el ancho de banda pedido). Cuando se recibe la confirmación, la estación puede transmitir sus datos en los *Frames* asignados a ella. Si no se recibe la confirmación, la estación supone que su petición de reserva ha sufrido una colisión y lo intenta de nuevo.

Desde el punto de vista del controlador central, la comunicación es como sigue. Los *Frames* son recibidos uno a uno en el canal de recepción. Los *Frames* asignados son repetidos por el canal de transmisión sin más procesamiento. Los no asignados deben ser examinados. Si el *Frame* está mutilado ó contiene un error, es ignorado. Si se trata de *Frame* de datos válido, es repetido por el canal de emisión. Si es un *Frame* de petición de reserva, el controlador llena la reserva dentro de los límites de sus *Frames* disponibles en los ciclos futuros y envía una confirmación.

Debe observarse que esta técnica tiene la fuerza de

ambas técnicas CSMA/CD y Token Bus. Su principal desventaja es que necesita un controlador central bastante complejo, con los consecuentes problemas de confiabilidad.

5.4

CONTROL DEL ACCESO AL MEDIO: ANILLO.

Las tres técnicas más comunes son: inserción de registro (Register Insertion), Anillo particionado (Slotted Ring), y Token Ring. Las dos primeras las trataremos brevemente, mientras que el Token Ring lo estudiaremos en detalle así como el estándar de IEEE 802.

TABLE 5.6 Ring Access Methods

Characteristic	Register Insertion	Slotted Ring	Token Ring
Transmit opportunity	Idle state plus empty buffer	Empty slot	Token
Packet purge responsibility	Receiver or transmitter	Transmitter	Transmitter
Number of packets on ring	Multiple	Multiple	One
Principal advantage	Maximum ring utilization	Simplicity	Regulated/fair access
Principal disadvantage	Purge mechanism	Bandwidth waste	Token maintenance

La tabla 5.6 compara estos tres métodos en una serie de puntos:

* Oportunidad de transmisión. ¿Cuándo puede un

repetidor insertar un paquete en el Anillo?.

- * Responsabilidad de eliminación de paquetes: ¿Quién retira un paquete del Anillo evitando su circulación indefinida?.
- * Número de paquetes en el Anillo: Esto no sólo depende de la longitud en bits del Anillo en relación con la longitud de los paquetes, sino también del método de acceso.
- * Principal ventaja.
- * Principales inconvenientes.

El significado de la tabla se hará mas claro a medida que avancemos en el estudio de estas tres técnicas.

Inserción en registro:

Esta técnica fué desarrollada por investigadores de la Universidad del Estado de Ohio en 1.974. Es una técnica usada por los productos de la serie 1 de IBM y por un producto suizo llamado SILK. El nombre de esta técnica viene del registro de desplazamiento asociado a cada nodo del Anillo. Este registro de desplazamiento, igual el tamaño a la máxima longitud de *Frame*, se usa para retener temporalmente *Frames* que circulan por el nodo. Además, el nodo tiene un Buffer para almacenar *Frames* producidos localmente.

El funcionamiento del Anillo controlado por inserción en registro, puede ser explicado atendiendo a la figura 5.13, la cual muestra el registro de desplazamiento y el

Buffer en un nodo. Primero consideremos el caso en el que la estación no tiene datos para enviar, y sólo está reteniendo *Frames* de datos que circulan por su posición. Cuando el Anillo está desocupado, el puntero de entrada apunta a la primera posición (hacia la derecha) del registro de desplazamiento que está libre. Cuando llegan datos desde el Anillo son insertados bit a bit en el registro de desplazamiento, con el puntero de entrada desplazándose a la izquierda por cada bit. El *Frame* comienza con un campo de dirección. Tan pronto como todo el campo de dirección está en el registro, la estación puede determinar si es la destinataria. Si no, el *Frame* es desplazado bit a bit a medida que entran los bits del Anillo y sacándolos al Anillo. Después de que llegue el último bit del *Frame*, la estación sigue desplazando bits a la derecha hasta que el *Frame* se haya ido. Si, durante este tiempo, no llegan otros *Frames*, el puntero de entrada volverá a su posición inicial. De otro modo, un segundo *Frame* empezará a acumularse en el registro a medida que el primero es expulsado.

Con lo dicho anteriormente, se puede dar que haya más de un *Frame* en el Anillo a la vez. Además tendríamos una serie de *Frames*, con huecos entre ellos, pasando por una estación.

Si un *Frame* entrante está dirigido a la estación en cuestión, la estación tiene dos posibilidades. Uno, puede desviar el resto del *Frame* hacia sí misma y borrar los

bits de dirección del registro, con lo que eliminarían el *Frame* del Anillo. Este es el procedimiento seguido por IBM. Un segundo pensamiento revela que esta estrategia puede suponer la utilización total del ancho de banda que ha veces excede la velocidad actual de transmisión. No obstante se trata sin duda de una medida de falsa economía pues, desde que el *Frame* es eliminado por el receptor y no por el emisor, debemos usar otro tipo de confirmación con lo que perderíamos ancho de banda. La segunda alternativa es retransmitir el *Frame* como llega, mientras es copiado por la estación local.

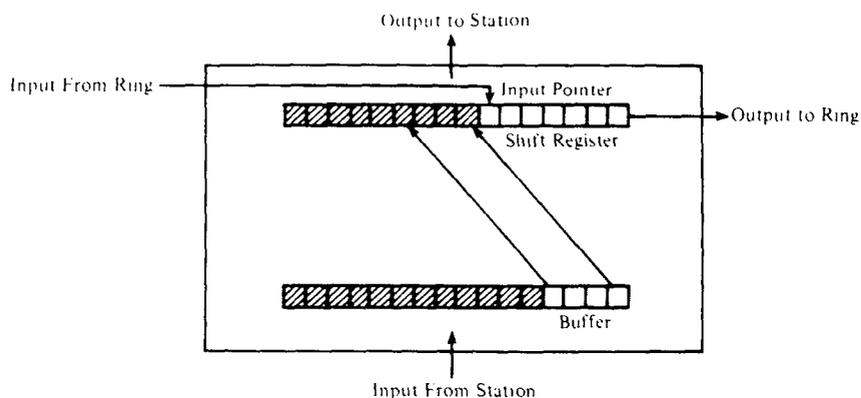


FIGURE 5-13. Register Insertion Ring

Ahora consideremos el caso en el que la estación tiene datos para transmitir. El *Frame* a transmitir es colocado en el Buffer de salida. Si la línea está desocupada y el registro de desplazamiento está vacío, el *Frame* puede ser transferido inmediatamente al registro de

desplazamiento. Sí el *Frame* tiene "n" bits, menos bits que el máximo tamaño de *Frame*, y sí por lo menos hay "n" bits vacíos en el registro de desplazamiento, los "n" bits son transferidos en paralelo y de forma inmediata a la porción vacía del registro inmediatamente adyacente a la parte llena; el puntero de entrada es ajustado de forma adecuada.

Podemos ver que va a haber un retardo en cada estación, cuyo valor mínimo es la longitud del campo de dirección y cuyo máximo valor es la longitud del registro de desplazamiento. Esto contrasta con el Anillo particionado y el *Token Ring*, donde el tiempo de retardo es sólo el retardo del repetidor (normalmente el tiempo de uno ó dos bits). Para entenderlo bien supongamos el ejemplo de una estación transmitiendo un *Frame* de 1000 bits en un Anillo de 10 Mbps controlado por inserción en registro. El tiempo que tarda la estación en transmitir el *Frame* es de $1000/10^7 = 0.10$ ms. Sí el *Frame* debe pasar 50 estaciones para llegar a su destino y sí el campo de dirección es de 16 bits, entonces el retardo mínimo, excluyendo el tiempo de propagación, es $(16 \times 50)/10^7 = 0.08$ ms. Este es un retardo considerable comparándolo con el tiempo de transmisión. Peor aún, sí cada estación tiene un registro de desplazamiento de 1000 bits, el máximo retardo que puede sufrir un *Frame* es de $(1000 \times 50)/10^7 = 5$ ms.

Esta técnica hace cumplir una forma eficiente de imparcialidad. Mientras el Anillo está vacía, una estación

con muchos datos para enviar puede enviar un *Frame* tras otro, utilizando todo el ancho de banda del Anillo. Si el Anillo está ocupado, una estación verá que, después de mandar un *Frame*, el registro de desplazamiento no acomodará otro *Frame*. La estación tendrá que esperar hasta que se acumulen los suficientes huecos intermensajes para enviar otra vez. Como un refinamiento de esta técnica, ciertos nodos de alta prioridad pueden tener registros de longitud mayor que la mínima longitud de registro (la cual coincide con la longitud máxima de *Frame*).

La ventaja principal de esta técnica es que con ella se consigue la máxima utilización del Anillo (más que cualquier otro método). Hay otras ventajas. Como en el sistema *Token*, permite longitudes variables de *Frame*, lo cual es eficiente desde el punto de vista tanto de la estación como del Anillo. Como el Anillo particionado permite muchos *Frames* en el Anillo a la vez; lo que supone un uso eficiente del Anillo.

El principal inconveniente es el mecanismo de eliminación de *Frames*. El permitir múltiples *Frames* en el Anillo requiere el reconocimiento de una dirección prioritaria para eliminar un *Frame*, tanto si es eliminado por el receptor como por el emisor. Si el campo de dirección está dañado, el *Frame* puede circular indefinidamente. Una solución posible es usar un código de detección de error en el campo de dirección; la serie 1 de IBM usa un bit de paridad. El requerimiento para el

reconocimiento también indica que cada *Frame* se retrasa en cada nodo un tiempo igual a la longitud de ese campo. En los otros dos métodos no existe ese requerimiento.

Anillo particionado:

En este Anillo (figura 5.14), circulan continuamente un número determinado de particiones de longitud fija. Esta técnica fué desarrollada por J.R. Pierce, de ahí que también se ha denominado "circuito cerrado (rizo) de Pierce" (Pierze Loop). La mayoría del trabajo de desarrollo de esta técnica fué realizado en la Universidad de Cambridge, por ello, algunas firmas británicas la comercializan bajo el nombre de "Anillo de Cambridge"

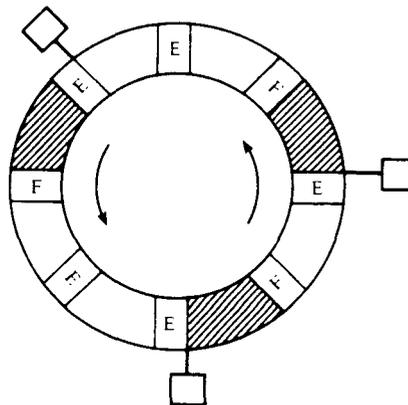


FIGURE 5-14. Slotted Ring

En el Anillo particionado, cada partición lleva delante (formando parte de él) un bit que indica si está lleno ó vacío. Inicialmente todos están marcados como

vacíos. Una estación con datos a transmitir, debe dividir estos en *Frames* del mismo tamaño que las particiones del Anillo. Entonces, la estación espera hasta que le llegue una partición vacía, la marca como llena, e inserta un *Frame* de datos a medida que la partición va pasando. La estación no puede transmitir otro *Frame* hasta que esta partición regrese. La partición llenada hace una vuelta completa, para ser marcada como vacía por la estación que la ha llenado. Cada estación conoce el número de particiones que hay en el Anillo y por tanto puede borrar el bit lleno/vacío correspondiente a medida que pasa. Una vez la estación haya liberado la partición que ha utilizado, puede transmitir de nuevo.

En el Anillo de Cambridge, cada partición contiene espacio para un byte de dirección fuente, uno de dirección de destino, dos bytes de datos, y 5 bits de control con lo que se tiene una longitud de 37 bits.

Este Anillo tiene unas características interesantes. Una estación puede decidir que sólo desea recibir datos de una determinada estación. Para ello, cada estación tiene un registro de selección de fuente. Si este registro contiene todas las estaciones, la estación puede recibir datos dirigidos a ella desde cualquier fuente (estación); si no es así, la estación sólo estará abierta a recibir datos enviados a ella por las fuentes especificadas en el registro.

El Anillo Cambridge especifica dos bits de respuesta

para diferenciar cuatro circunstancias:

- * Destino no existe/no activo.
- * Paquete aceptado.
- * Destino existe pero no se acepta el paquete.
- * Destino ocupado.

Por último, este Anillo incluye un controlador (monitor), cuya misión es liberar aquellas particiones que estén siempre ocupadas (llenas).

Normalmente habrán pocas particiones en un Anillo. Consideremos, por ejemplo, un Anillo de 100 estaciones con un promedio de 10m de separación entre cada una y una velocidad de transmisión de 10 Mbps. La velocidad de propagación típica para las señales es de 2×10^8 m/s.

En una primera observación podemos ver que la longitud en bits de los enlaces entre estaciones es $(10^7 \text{ Bps} \times 10\text{m}) / (2 \times 10^8 \text{ m/s}) = 0.5 \text{ bit}$. Si decimos, por ejemplo, que el retardo en cada repetidor es de un bit, la longitud total del Anillo es $1.5 \times 100 = 150 \text{ bit}$. Esto es suficiente para 4 particiones (de 37 bits).

La principal desventaja del Anillo particional es que hay una pérdida de ancho de banda. Primero, cada partición tiene sólo 10 bits de datos de los 37 totales. Segundo, una estación sólo puede enviar un *Frame* por vuelta completa del Anillo. Si sólo una ó pocas estaciones tienen *Frames* para transmitir, muchas de las particiones circularán vacías.

Su mayor ventaja es su simplicidad. La interacción

con el Anillo en cada nodo se minimiza, con lo que se gana fiabilidad.

Token Ring:

Esta es, probablemente la técnica más antigua de control de Anillo. Fué propuesta originalmente en 1.969 y ha llegado a ser la técnica de acceso a Anillo más utilizada en los EE.UU., y es una de las elegidas para su estandarización por el Comité 802 de IEEE. Los productos IBM así como los de un buen número de competidores son compatibles con este estándar.

Descripción:

La técnica de **Token Ring** se basa en el uso de un pequeño *Frame* de *Token* que circula a lo largo del Anillo. Cuando todas las estaciones están desocupadas el *Frame* de *Token* tiene una serie de bits (plantilla de bits) indicando que es un "Token libre". Una estación que quiera transmitir debe esperar a detectar un *Token* pasando. Entonces, lo cambia de "Token libre" a "Token ocupado". La estación transmite un *Frame* inmediatamente a continuación del *Token* ocupado. Esto se puede observar en la figura 5.15.

Ahora no hay *Token* libre en el Anillo, por lo que otras estaciones deseando transmitir deben esperar. El *Frame* que está en el Anillo hará una vuelta completa al Anillo y será retirado por la estación emisora. La

estación transmisora insertará un nuevo *Token* libre en el Anillo cuando se den las dos condiciones siguientes:

- * La estación ha completado la transmisión de su *Frame*.
- * El *Token* ocupado ha vuelto a la estación.

Sí la longitud en bits del Anillo es menor que la longitud del *Frame*, la primera condición implica la segunda. Sí no es así, una estación puede insertar un *Token* libre después de haber terminado su transmisión pero siempre antes de recibir su propio *Token* ocupado; la segunda condición no es estrictamente necesaria. No obstante, el uso de sólo la primera condición puede complicar la tarea de corrección de errores, ya que muchos *Frames* pueden estar en el Anillo al mismo tiempo. En cualquier caso, el uso del *Token* garantiza que sólo una estación pueda transmitir cada vez.

Cuando una estación emisora inserta un nuevo *Token* libre, la próxima estación (en orden) puede tomar el *Token* y transmitir.

Bajo condiciones de baja carga hay una cierta ineficiencia ya que una estación debe esperar que el *Token* le llegue para poder transmitir. Pero en condiciones de gran carga, que es donde importa, el Anillo funciona de una forma similar a la técnica *Round-Robin*, la cual es eficiente y justa. Para ver esto, fijémonos en la figura 5.15. Nótese que después de que la estación *A* transmite, libera un *Token* (tercera figura). La primera estación que

tiene posibilidad de transmitir es la D. Si D transmite, libera un *Token* y C tiene la máxima oportunidad de transmitir, y así sucesivamente. Por último, el Anillo debe ser lo suficientemente grande para mantener el *Token*. Si las estaciones están temporalmente inactivas, su retardo puede necesitar ser compensado artificialmente.

La ventaja principal del *Token Ring* es el control que proporciona sobre el acceso. En el diseño expuesto anteriormente el trato es igualitario, pero esta técnica puede modificarse para aceptar prioridades y garantizar servicios de ancho de banda.

El principal inconveniente es la necesidad del mantenimiento del *Token*. La pérdida de *Tokens* libres impide la posterior utilización del Anillo, y el duplicado del *Token* puede incluso romper la operación del Anillo. Una estación debe ser elegida "monitora" para asegurar que sólo hay un *Token* en el Anillo y para que inserte un *Token* libre si es necesario.

El *Token Ring* de IEEE 802:

La especificación del *Token Ring* del IEEE 802 es un refinamiento de lo que hemos dicho. Sus elementos principales son:

- 1.- Protocolo de *Token-único*: Una estación que ha completado su transmisión no inserta un nuevo *Token* hasta que no le regrese el *Token* ocupado. Esto no es tan eficiente, para *Frames* pequeños,

como la técnica del *Token* múltiple. No obstante este sistema de *Token*-único simplifica las funciones de prioridad y de corrección de errores.

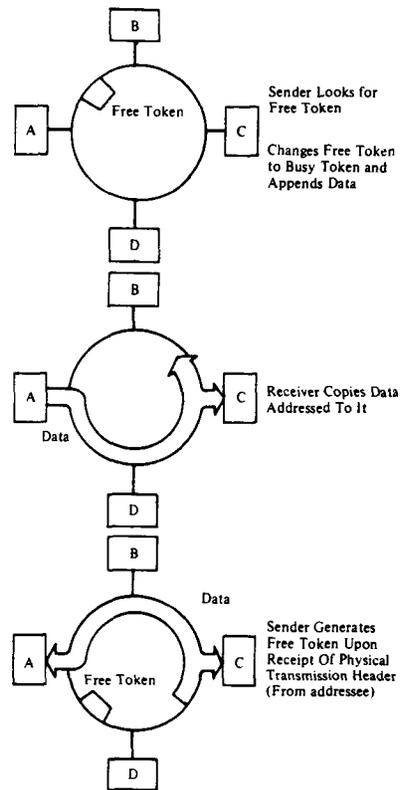


FIGURE 5-15. Token Ring

- 2.- Bits de prioridad: Indican la prioridad de un *Token* y por tanto, las estaciones con autorización para utilizarlo.
- 3.- Bit de monitor: Usado por el monitor del Anillo como se dijo antes.
- 4.- Indicadores de reserva: pueden usarse para permitir a las estaciones con alta prioridad enviar mensajes en un *Frame* para pedir que el próximo *Token* sea captado por esa estación.

- 5.- *Token-Holding Timer*: Empieza el contaje al comienzo de la transferencia de datos; y con él se controla el tiempo que una estación puede ocupar el medio antes de transmitir un *Token*.
- 6.- Bits de confirmación: Hay tres: Error detectado (E), dirección reconocida (A), y el *Frame* copiado (C). Estos bits son fijados a 0 por la estación transmisora. Cualquier estación puede fijar el bit E. Las estaciones de destino pueden fijar los bits A y C.

La figura 5.2 muestra los dos formatos de *Frame* para *Token Ring*. Los campos individuales son los siguientes:

- * Delimitador de comienzo (SD): Una plantilla única de 8 bits que se usa para empezar cada *Frame*.
- * Control de acceso (AC): tiene el formato 'PPPTMRRR', donde PPP y RRR son variables de 3 bits de prioridad y de reserva respectivamente. M es el bit de monitor, y T indica si es un *Token* ó un *Frame* de datos. En caso de que sea un *Frame* de *Token*, el único campo adicional es ED.
- * Control de *Frame* (FC): indica cuando se trata de un *Frame* de datos de LLC. Si no, los bits de este campo controlan la operación del protocolo MAC del *Token Ring*.
- * Dirección de destino (DA): Como en CSMA/CD y *Token Bus*.

- * Dirección fuente (SA): Como en el CSMA/CD y Token Bus.
- * LLC: Como en CSMA/CD y Token Bus.
- * FCS: Como en CSMA/CD y Token Bus.
- * Delimitador de final (ED): Contiene el bit de detección de error (E), y el bit de *Frame* intermedio (I). El bit I se utiliza para indicar que ese es otro *Frame* distinto al último *Frame* de una transmisión de muchos *Frames*.
- * Estado del *Frame* (FS): Contiene los bits de dirección reconocida (A) y de *Frame* copiado (C).

Consideremos en primer lugar la operación del Anillo cuando se usa una única prioridad. En este caso no se usan ni el bit de reserva ni el de prioridad. Una estación que quiere transmitir, espera a que un *Token* libre pase por ella, como indica el bit a cero del campo AC del *Token*. La estación se hace con el *Token* poniendo a 1 este bit. Los campos SD y AC del *Token* recibido funcionan ahora como los dos primeros campos de un *Frame* de datos. Luego transmite uno ó más *Frames*, continuando hasta que se termine su salida (datos a enviar) ó hasta que termine su *Frame-Holding Timer*. Cuando regresa el campo AC del último *Frame* transmitido, la estación transmite un *Token* libre ajustando el bit de *Token* a 0 y añadiéndole un campo ED.

Las estaciones en modo receptor escuchan al Anillo. Cada estación puede revisar los *Frames* que van pasando en busca de errores y poner a 1 el bit E sí se detecta un

error. Si una estación detecta su propia dirección, fija el bit A a 1; ésta puede incluso copiar el *Frame*, fijando el bit C a 1. Esto permite a la estación de origen diferenciar tres situaciones:

- * Estación no existe/no está activa.
- * Estación existe pero el *Frame* no ha sido copiado.
- * *Frame* copiado.

La operación anterior puede ser complementada con un diseño de prioridad múltiple. Por ejemplo, a los puentes se les puede dar más prioridad que a las estaciones ordinarias. La especificación 802 proporciona tres bits para ocho niveles de prioridad. Para verlo mejor, vamos a designar tres valores:

Pm = Prioridad de mensaje para ser transmitido por una estación.

Pr = Prioridad de recibida; y

Rr = Reserva recibida.

El diseño funciona como sigue:

- 1.- Una estación que desea transmitir debe esperar por un *Token* libre con $Pr \leq Pm$.
- 2.- Mientras espera, una estación puede reservar un *Token* Futuro a su nivel de prioridad (Pm). Si pasa un *Frame* de datos, fija su campo de reserva a su prioridad (Rr = Pm) siempre que el campo de reserva es menor que su prioridad ($Rr < Pm$). Si pasa, un *Token* libre, fija el campo de reserva a

su prioridad (R_r P_m) siempre que $R_r < P_m$ y $P_m < P_r$. Esto tiene el efecto de las reservas de baja prioridad.

3.- Cuando una estación coge un *Token*, fija el bit de *Token* a 1, el campo de reserva a 0 y deja el campo de prioridad descargado.

4.- Después de la transmisión, una estación lanza un nuevo *Token* con la prioridad fijada al máximo de P_r , R_r y P_m , y la reserva fijada al máximo de R_r y P_m .

Con los pasos descritos, se consigue una ordenación de las peticiones coincidentes y permite a las transmisiones con más alta prioridad coger el *Token* tan pronto como sea posible. Debido a esto, este algoritmo lleva la prioridad al nivel más alto usado y lo mantiene allí. Para permitir esto se tienen dos pilas, una para las reservas y otra para las prioridades. En esencia, cada estación es responsable de asegurar que ningún *Token* circule indefinidamente debido a su alta prioridad. La estación que detecte esto puede degradar la prioridad a una menor.

En resumen el algoritmo de prioridad funciona como sigue. Una estación con prioridad más alta que el *Token* ocupado circulante en ese momento (Frame de datos), puede reservar el próximo *Token* libre para su nivel de prioridad, a la vez que el *Token* pasa. Cuando la estación que emite en ese momento acaba, ésta lanza un *Token* libre

con la prioridad alta pedida. Las estaciones de prioridad menor no pueden hacerse con el *Token*, así este pasa a la estación que lo pidió ó a una estación anterior (en la secuencia de estaciones) con la misma prioridad o superior.

La estación que subió la prioridad es responsable de degradarla hasta su nivel anterior cuando hayan terminado de transmitir todas las estaciones de prioridad superior. Cuando esa estación ve un *Token* libre en una prioridad más alta, puede suponer que no hay ningún tráfico de mayor prioridad esperando, y por lo tanto degrada el *Token* antes de pasarlo. La figura 5.16 es un ejemplo del funcionamiento del mecanismo de prioridad.

Mantenimiento del Token:

Para salvar varias condiciones de error, se designa una estación como monitor activo. Este monitor activo lanza periódicamente un *Frame* de control (Active-Monitor-Present) para asegurar a las demás estaciones que hay un monitor activo en el Anillo. Para detectar la pérdida de un *Token*, el monitor usa un *Timer* válido de *Frame*, que es mayor que el tiempo necesario para atravesar completamente el Anillo. Este *Timer* se resetea después de cada *Token* válido ó después de cada *Frame* de datos. Si el *Timer* se agota, el Monitor lanza un *Token*. Para detectar un *Frame* de datos que circula indefinidamente, el Monitor fija un bit, llamado de monitor, a 1 en cada *Frame* de datos que

pasa por él, la primera vez que lo hace. Si el Monitor ve un *Frame* de datos con el bit de monitor ya fijado a 1, sabe que la estación emisora ha fallado y no lo ha retirado. El lo hace y transmite un *Token*. Esta misma estrategia es usada para detectar un fallo en el mecanismo de prioridad: ningún *Token* debería circular a lo largo de todo el Anillo (la vuelta completa) con una prioridad constante y diferente de cero. Finalmente, si el Monitor activo detecta alguna evidencia de la existencia de otro Monitor activo, inmediatamente pasa a un estado de espera (en lo que se refiere a su actividad de monitor).

Por otro lado, todas las estaciones activas del Anillo cooperan para proporcionar a cada estación una continua puesta al día de la identidad de su vecino. Periódicamente, cada estación envía un *Frame* de presencia de Monitor en espera (SMP). Sus vecinos (a continuación en la cadena) toman este *Frame*, toman la dirección de quien lo envía y después de una pausa envían su propio *Frame* SMP.

REDES LOCALES DE ALTA VELOCIDAD:

En este capítulo estudiaremos la estructura de las redes locales de alta velocidad. Este tipo de redes han sido usadas primordialmente en transferencia de datos a alta velocidad entre las unidades principales y controladores de almacenamiento masivo. Esto es lo que llamamos en el capítulo 1 redes de salas de ordenadores.

Brevemente, las características de HSLN son:

- * Alta velocidad de transmisión: De 50 a 70 Mbps.
- * Interface de alta velocidad: Los HSLN pretenden proporcionar un alto rendimiento específico entre el equipo de una sala de ordenadores y los periféricos de alta velocidad. Por ello el

enlace físico entre la estación y la red debe ser de alta velocidad.

- * Acceso distribuido: Como en los LANs, es aconsejable tener un control distribuido del acceso por razones de fiabilidad y eficiencia.
- * Distancia limitada: Generalmente, una HSLN será usada en una sala de ordenadores ó en un pequeño número de ellas.
- * Número limitado de dispositivos: En una sala de ordenadores el número de dispositivos de almacenamiento y de unidades principales es del orden de decenas.

Aunque las dos últimas características son apropiadas para una red de sala de ordenadores, hay también limitaciones técnicas en las HSLNs de cable coaxial que existen actualmente.

No obstante, las nuevas aplicaciones que se avecinan en el entorno de la oficina hacen que las limitaciones de las tradicionales HSLN de sala de ordenadores, sean inaceptables. Ejemplo de estas aplicaciones son los fascículos, procesadores de imagen de documento y programas gráficos para ordenadores personales. Estas aplicaciones tienen un estándar de resolución de 400x400 por página. Incluso con técnicas de compresión esto genera una tremenda carga. La tabla 6.1 compara la carga generada por un procesamiento de imagen con otras aplicaciones de oficina. Estas nuevas demandas necesitarán redes locales

de alta velocidad que sean capaces de soportar un gran número de sistemas de oficina a lo largo de mayores distancias. Como comentaremos, los sistemas HSLN de cable coaxial son inadecuados para esta tarea. Se necesitarán sistemas basados en fibra óptica.

TABLE 6.1 Network Load Component Comparison

Traffic Type	Size in Bits
Compressed Page Image (400 × 400)	600,000
Compressed Page Image (200 × 200)	250,000
Word-Processing Page	20,000
Typical Memo	3,500
Data Processing Transaction	500

Hoy en día el mercado de HSLNs está dominado por la arquitectura de Bus Coaxial. En primer lugar hablaremos brevemente de esta arquitectura para luego pasar a ver las HSLNs de fibra óptica.

6.1

SISTEMAS DE CABLE COAXIAL.

Vamos a dar unas nociones de los tres tipos de HSLN basado en cable coaxial; estos son:

- * Bus de banda ancha de canal único: Se trata de

una alternativa seleccionada de un estándar de **ANSI** anteriormente desarrollada por el Comité **X3T9.5**. Ambas alternativas se denominan "interface de datos distribuidos localmente" (LDDI).

- * Bus de banda base: Usado en la más antigua y más extendida **HSLN**, la de **HIPER Channel**.
- * Estrella pasiva: Es la otra alternativa elegida por la **X3T9.5**; se usa también para los **VAX**.

Todos estos modelos tienen, lógicamente, topología Bus. Esto es, una transmisión de cualquier dispositivo es recibida a través de un medio pasivo por todos los demás dispositivos, y sólo uno de ellos puede transmitir con éxito cada vez. Por esto, estas técnicas comparten una serie de características con las **LANs** basadas en Bus. En particular, se usa una técnica de conmutación, y debido a que el medio es multiacceso, necesita una técnica de control de acceso para determinar quien va luego. La diferencia principal entre las **LANs** de Bus y las **HSLN** de Bus es la mayor velocidad de transmisión de esta última. En este capítulo nos centraremos en las características de las **HSLNs** que resultan de esta diferencia.

Los dos primeros tipos de **HSLN** (bus puros) tienen mucho en común. Entre las características comunes podemos destacar:

- * Velocidad de 50 Mbps: Con la tecnología actual, esta es (más ó menos) la velocidad que podemos

alcanzar con una buena relación coste/efectividad.

- * Longitud máxima de 1 Km: Este límite está fijado por la velocidad, pero puede ser adecuado para la mayoría de los requerimientos de la HSLN.
- * Número de estaciones del orden de decenas: Este número también está determinado por la velocidad. Dado que las HSLNs están ideadas en principio para dispositivos caros de alta velocidad, esta restricción no resulta gravosa.
- * Previsiones para varios cables (más de cuatro): Esto aumenta el rendimiento específico y la fiabilidad.

Bus banda ancha de canal-único:

Aquí veremos, en líneas generales, las características del sistema propuesto por el Comité ANS X3T9.5.

Como en los sistemas de banda ancha y canal-único descritos en el capítulo cuarto, la HSLN de banda ancha y canal único tiene los siguientes componentes:

- * Cable coaxial CAT de 75 Ohm.
- * Terminadores de 75 Ohm.
- * Tomas o derivaciones (Taps) no direccionales.
- * Controladores para transmisión/recepción y MAC.

En las HSLN tenemos una limitación en el número de derivaciones debido a que a altas velocidades resulta más

difícil una recepción baja en error. Sí consideramos que cada bit transmitido a una velocidad alta de la HSLN ocupa menos tiempo y espacio en el cable, se necesita una menor cantidad de atenuación o distorsión para causar error.

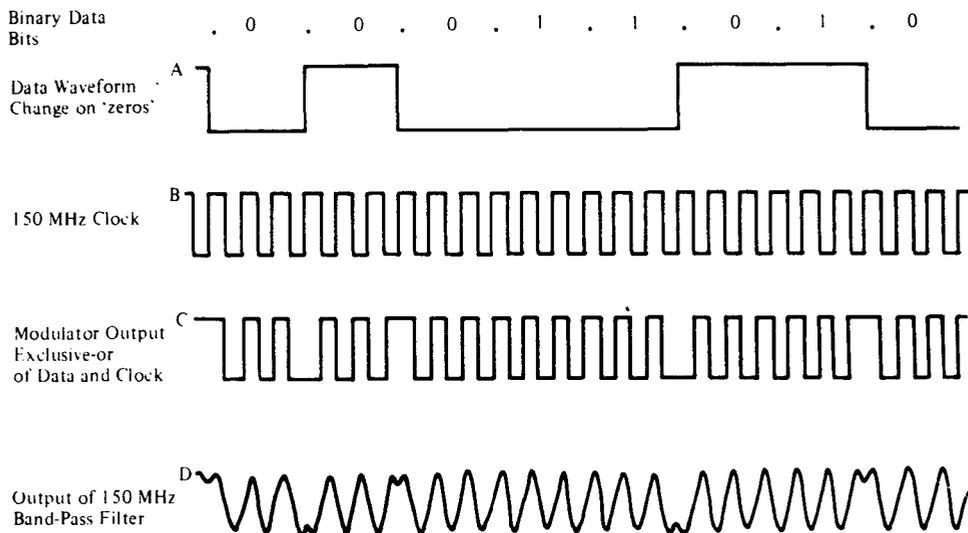


FIGURE 6-1. Idealized Transmitter Waveforms

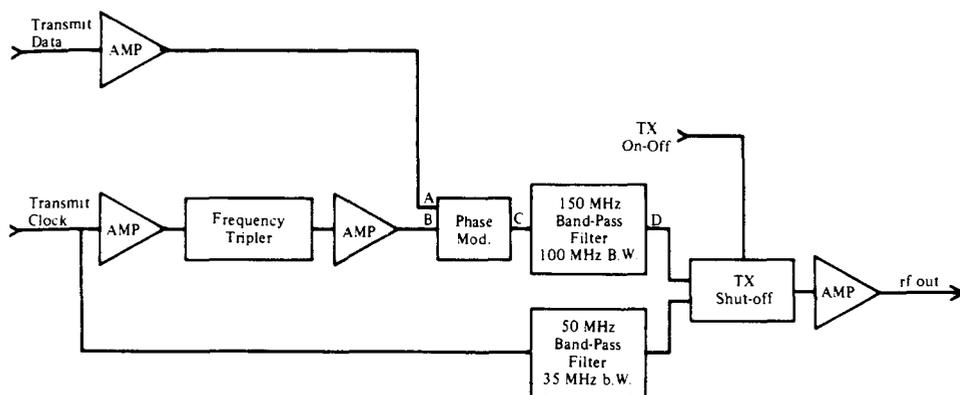


FIGURE 6-2 50-Mbps Transmitter Block Diagram

Por último, vamos a ver el modelo de modulación a usar. La técnica especificada por el X3T9.5 es la PSK de 180°. Para una velocidad de 50 Mbps, esta técnica usa una portadora de 150 MHz y una señal de reloj a 50 MHz. La figura 6.1 muestra los pasos por los que pasan los datos al ser transmitidos. La cadena de bits se codifican (digitalizan) utilizando la convención "cambio en cero"; que consiste en un cambio del nivel de voltaje al comienzo de cada Bit 0. Esta cadena de bits codificados se genera usando un reloj de 50 MHz. Para obtener codificación de fase, esta cadena de bits se modula con una cadena de pulsos digitales a 150 MHz, tomando la OR-EXCLUSIVA de ambas señales. El resultado es una cadena digital a 150 MHz que cambia la fase al comienzo de cada bit 0. La salida modulada es pasada por un filtro paso-banda para producir la señal analógica en la línea. El reloj de 50 MHz también se saca para proporcionar sincronización. En la figura 6.2 podemos ver un diagrama de bloques del transmisor.

En el receptor se produce el proceso inverso. La señal se obtiene con un bit de retraso.

Bus de banda base:

No hay mucho que decir de esta red que no hayamos comentado en las LANs. Los componentes principales vuelven a ser los mismos:

- * Cable coaxial CAT de 75 Ohm.

- * Tomas no direccionales.
- * Terminadores de 75 Ohm.
- * Controladores.

La única red disponible comercialmente es la HIPERchannel. Su velocidad es de 50 Mbps usando una codificación tipo Manchester. HIPERchannel recomienda una longitud máxima de 1.2 Km y no más de 30 estaciones.

Esta red tiene similares rendimientos a la de banda ancha de canal-único.

Estrella Pasiva:

Esta arquitectura es la misma que la mostrada en la figura 4.14. Se usan cables coaxiales de banda base de 50 Ohm. La velocidad especificada es de 70 Mbps usando codificación Manchester. El número máximo de dispositivos y el radio máximo están limitados por las fuentes de pérdidas en la red: atenuación del cable coaxial y la división de potencia en el acoplador. Para las especificaciones X3T9.5 y VAXcluster se fijan 16 nodos y un radio máximo de 45m.

Comparado con los dos sistemas anteriores, éste resulta más limitado. No obstante tiene dos ventajas sobre el Bus:

- * En esta red, el acoplador central permite la adición ó supresión de estaciones (dentro del rango (1-16) con un riesgo mínimo de disrupción eléctrica ó mecánica, tarea más difícil en un

Bus.

- * La arquitectura de Estrella pasiva facilita dos posibles mejoras: Primero, un acoplador activo permitiendo muchos mas de 16 nodos y, segundo, reemplazar el cable coaxial por fibra óptica.

6.2

SISTEMAS DE FIBRA OPTICA.

Las dos alternativas principales para redes locales de fibra óptica y alta velocidad son el Bus y el Anillo. Con la tecnología actual, el uso de un medio de fibra pasivo, como en un Bus, no es práctico para aplicaciones de alta velocidad, debido a las grandes pérdidas sufridas por cada toma en el Bus. En los Anillos de fibra, sin embargo, sólo se requieren enlaces de fibra punto a punto, y hay por lo menos un sistema en el mercado; este es el de Proteon (a 80 Mbps).

Esta sección se centrará en el estudio de la tecnología de los Anillos de fibra. Estudiaremos en concreto otro estándar del Comité **ANS X3T9.5: El FDDI** (Fiber Distributed Data Interface). La velocidad especificada en el **FDDI**. Es de 100 Mbps.

Para este estudio examinaremos tres aspectos:

- * Codificación de los datos.
- * Inestabilidad de la base de tiempo (Timing

Jitter).

* Fiabilidad.

Codificación de datos:

El tipo de codificación va a depender de la naturaleza del medio de transmisión, la velocidad, y otros factores como el coste. La fibra óptica es inherentemente un medio analógico; las señales pueden ser transmitidas sólo rango de frecuencias ópticas. Luego es de suponer que se usará una de las técnicas de codificación digital/analógica ya vistas (ASK, FSK, PSK). La FSK y PSK son difíciles de aplicar a altas velocidades y el equipamiento opto-electrónico resultaría muy caro y poco fiable. En la ASK se usa una señal de frecuencia constante y dos niveles de señal diferentes para representar los dos valores binarios. En el caso más simple, un valor es representado por la ausencia de portadora, y el otro valor por la presencia, a un valor constante, de la señal. Esta técnica también se denomina modulación de intensidad.

La modulación de intensidad, pues, proporciona un medio de codificar datos digitales para su transmisión por una fibra óptica. Un 1 binario puede ser representado por un punto de luz, y un 0 binario por la ausencia de energía óptica. La desventaja que conlleva este diseño es la ausencia de sincronización. Como las transiciones en la fibra son impredecibles, no hay modo de que el receptor sincronice su reloj con el transmisor. La solución a este

problema es garantizar la presencia de transiciones antes de codificar los datos binarios y entonces, presentar los datos codificados a la fuente óptica para su transmisión. La desventaja de esta técnica es que su eficiencia es de un 50%. Esto es, debido a que pueden haber hasta dos transiciones por tiempo de bit, se necesita una velocidad de 200 Elementos de señal por segundo (200 Mbaud) para alcanzar una velocidad de transmisión de 100 Mbps. A la velocidad alta del FDDI, ésto supone un costo y carga innecesarios.

Para aliviar la carga impuesta por la codificación Manchester, el FDDI especifica el uso de un código llamado 4B/5B. En él se codifican de 4 en 4 bits; cada grupo de 4 bits de datos se codifica en un símbolo con cinco celdas de tal manera que cada celda contiene un sólo elemento de señal (ausencia ó presencia de luz). Es decir, cada grupo de 4 bits es codificado como 5 bits. Con ésto, la eficiencia aumenta a un 80%; se consiguen 100Mbps con 125 Mbaud. El coste también se reduce de 5 a 10 veces.

Para comprender como este código obtiene sincronización, hay que saber que hay otro nivel de codificación; cada elemento de la cadena 4B/5B es tratado como un valor binario y es codificado usando la técnica de Nonreturn-To-Zero-Inverted (NRZI). En este código, se representa un 1 binario mediante una transición en el comienzo del intervalo del bit y un 0 binario se representa por la ausencia de transición en el comienzo

del intervalo del bit; no hay otras transiciones. La ventaja del NRZI es que utiliza codificación diferencial (La señal es decodificada comparando la polaridad de elementos adyacentes de la señal en vez del valor absoluto del mismo). Es por tanto más inmune al ruido.

TABLE 6.2 4B/5B Code

Decimal	Code Group	Symbol	Assignment	
<i>Line State Symbols</i>				
00	00000	Q	Quiet	
31	11111	I	Idle	
04	00100	H	Halt	
<i>Starting Delimiter</i>				
24	11000	J	1st of sequential SD pair	
17	10001	K	2nd of sequential SD pair	
<i>Data Symbols</i>				
			Hex	Binary
30	11110	0	0	0000
09	01001	1	1	0001
20	10100	2	2	0010
21	10101	3	3	0011
10	01010	4	4	0100
11	01011	5	5	0101
14	01110	6	6	0110
15	01111	7	7	0111
18	10010	8	8	1000
19	10011	9	9	1001
22	10110	A	A	1010
23	10111	B	B	1011
26	11010	C	C	1100
27	11011	D	D	1101
28	11100	E	E	1110
29	11101	F	F	1111
<i>Ending Delimiter</i>				
13	01101	T	Used to terminate the data stream	
<i>Control Indicators</i>				
07	00111	R	Denoting logical ZERO (reset)	
25	11001	S	Denoting logical ONE (set)	
<i>Invalid Code Assignments</i>				
01	00001	V or H	These code patterns shall not be transmitted because they violate consecutive code-bit zeros or duty cycle requirements. Codes 01,02,08 and 16 shall however be interpreted as Halt when received.	
02	00010	V or H		
03	00011	V		
05	00101	V		
06	00110	V		
08	01000	V or H		
12	01100	V		
16	10000	V or H		

Una vez sabido ésto, la tabla 6.2 nos muestra la codificación en símbolos usada en el FDDI. Dado que se codifican 4 bits en un patrón de 5, habrá algunos patrones que no se necesitarán. Los códigos elegidos para representar los 16 patrones de 4 bits son tales que una transición esté presente al menos dos veces por cada código de 5 celdas en el medio. Dando un formato NRZI en la fibra, no se van a permitir más de tres ceros en una fila, pues, con el NRZI, la ausencia de una transición indica cero.

En resumen:

- 1.- Se desecha la codificación de modulación simple de intensidad ya que no proporciona sincronización.
- 2.- Se elige el código 4B/5B por ser más eficiente que el código Manchester.
- 3.- El código 4B/5B es posteriormente codificado usando NRZI de tal manera que la codificación resultante pueda mejorar la fiabilidad de recepción.
- 4.- Los códigos específicos elegidos para codificar los 16 patrones de 4 bits de datos se escogen para garantizar un máximo de tres ceros en una fila para una adecuada sincronización.

Para representar los datos de entrada sólo se necesitan 16 de los 32 patrones posibles. Los símbolos restantes se declaran inválidos ó se les asigna un

significado especial como símbolos de control.

Timing Jitter:

En el capítulo 4 definimos el *Timing Jitter* como la desviación en la recuperación del reloj, que puede ocurrir cuando el receptor intenta reconstruir tanto el reloj como la sincronización a partir de la señal recibida. Si no se toman medidas en contra, el *Jitter* se acumula en el Anillo. Nosotros vimos que el estándar de IEEE especifica el uso de un sólo reloj en el Anillo, y que la estación que tiene reloj es responsable de eliminar el *Jitter* por medio de un *Buffer* elástico. Si el Anillo tiene una vuelta completa de adelanto ó de atraso con respecto al reloj nuestro, el *Buffer* elástico se agranda ó se reduce según el caso. Incluso en esta técnica, la acumulación de *Jitter* fija una limitación sobre el tamaño del Anillo.

Este modelo de sincronización centralizada es apropiado para un anillo de 100 Mbps. A 100 Mbps la duración del bit es de sólo 10 ns, mientras que a 4 Mbps es de 250 ns. Esto hace que los efectos de la distorsión sean más severos, y una sincronización centralizada introduciría demandas muy duras, y por tanto costosas, sobre la circuitería del circuito de sincronización de fase en cada nodo. Por lo tanto, el estándar FDDI especifica el uso de un diseño de sincronización distribuida: Cada estación utiliza su propia fuente (autónoma) de reloj para transmitir ó repetir la

información en el Anillo. Cada estación tiene su propio *Buffer* elástico. Los datos se meten en el *Buffer* a la velocidad recuperada de la señal entrante, pero se sacan de él a la velocidad del reloj autónomo de la estación. Este sistema es más robusto y minimiza el *Jitter*. Como consecuencia de la resincronización en cada estación, el *Jitter* no limita el número de repetidores en el Anillo.

Fiabilidad:

Al contrario que los estandars **IEEE** y **LDDI** (Local Distributed Data Interface), el **FDDI** apunta explícitamente la necesidad de la fiabilidad e incluye especificaciones para técnicas de mejora de la fiabilidad. Se incluyen tres técnicas:

- * Desvío de estación: Se pasa de una estación en mal estado ó apagada por medio de un interruptor óptico de desvío.
- * Anillos duales: Se usan dos Anillos para interconectar las estaciones de modo que si se da un fallo de cualquier estación o repetidor signifique la reconfiguración de la red para mantener la colectividad.
- * Concentrador de cableado: Ver capítulo 4.

Los enfoques de fiabilidad definidos en el estándar **FDDI** son aplicables a cualquier Anillo.

REDES LOCALES DE CONMUTACION DE LINEAS (Ó CIRCUITOS)

Hasta ahora hemos, estudiado redes locales que usan conmutación de paquetes. Para muchos profanos, ésta es la única clase de redes locales que hay. Pero hay otra alternativa, basada en el viejo enfoque de la conmutación de circuitos. Como veremos, las diferencias en la arquitectura y en las cuestiones de diseño son grandes, aunque también las similitudes lo son:

El ejemplo más importante de estas redes casi nunca recordadas es la Digital Private Branch Exchange (PBX) ó tablero conmutador digital de abonado (telefonía).

PBX (EVOLUCION):

La PBX digital es el resultado de la conjunción de dos tecnologías: conmutadores digitales y sistemas de centrales telefónicas. El precursor de la PBX digital es el tablero conmutador de abonado (PBX). Una PBX es una instalación local, perteneciente o alquilada por una organización, la cual interconecta los teléfonos dentro de la instalación y proporciona acceso al sistema público de teléfonos. Normalmente, un usuario de teléfono marca un mínimo de tres ó cuatro dígitos para llamar a otro teléfono y marca un número de un sólo dígito (generalmente el 8 ó el 9) para obtener un tono para una línea exterior, lo cual permite al llamador marcar un número del mismo modo que un usuario residente.

Las primeras centrales privadas conectadas a la red eran manuales, con uno ó más operadores encargados de realizar todas las conexiones en el tablero de control. En los años 20, estos sistemas comenzaron a ser cambiados por sistemas automáticos, llamados PABX (Private Automatic...), que no requerían operarios. Esta "primera generación" de sistemas, usaba señales analógicas y tecnología eletromecánica. Las conexiones de datos pedían realizarse vía modem. Esto es, un usuario con un terminal, un teléfono y un modem ó un acoplador acústico en su

oficina, podía marcar un número local ó lejano que llegara a otro modem e intercambiar así datos.

La "segunda generación" de PBXs fué introducida en los años 70. Estos sistemas usaban conmutación digital y tecnología electrónica. Se les denominó PBX digitales ó CBX (Computerized Branch Exchange), y fueron diseñadas principalmente para conducir el tráfico de voz analógica, con la función codificador/decodificador incluida en el conmutador de tal manera que se pueda usar internamente una conmutación digital. Estos sistemas son también capaces de manejar conexiones digitales de datos sin la necesidad de un modem .

La "tercera generación" la constituyen los llamados "sistemas de voz/datos integrados", aunque las diferencias entre esta tercera y la segunda generación son vagas. Algunas de las características que difieren de las anteriores son:

- * El uso de teléfonos digitales: Esto permite estaciones de trabajo voz/datos integradas.
- * Arquitectura distribuida: Muchos conmutadores en una configuración jerárquica ó en malla con inteligencia distribuida, lo que proporciona un aumento de fiabilidad.
- * Configuración de no bloqueo: Típicamente, se usan tareas de puertos dedicados para todos los teléfonos y dispositivos.

Dado el avance de la tecnología y las características

de ésta, se suceden continuamente mejoras que hacen difícil la clasificación de las PBXs por generaciones. No obstante, hay que señalar avances recientes que, juntos, pueden considerarse como constitución de una cuarta generación de PBXs:

- * Enlace de LAN integrado: Esta capacidad (ó facultad) proporciona un enlace directo de alta velocidad a una LAN. Esto permite una distribución óptima de dispositivos de baja velocidad (terminales) de la PBX y de dispositivos de mayor velocidad (ordenadores) de la LAN de manera totalmente transparente para el usuario.
- * Asignación dinámica del ancho de banda: Normalmente una PBX ofrece una ó un pequeño número de servicios de velocidad de datos. El incremento de la sofisticación de la capacidad de asignación dentro de la PBX le permite ofrecer virtualmente cualquier velocidad a todo dispositivo enganchado a ella. Esto permite crecer al sistema en la medida en que crecen las necesidades del usuario.
- * Canal de paquetes integrado: Hace que la PBX tenga acceso a una red de paquetes conmutados X.25.

La lógica evolución hacia una PBX digital, se debe a una serie de ventajas que esta tiene sobre su predecesora;

estas son:

- * Tecnología digital: Al manejar las señales internas de manera digital, obtenemos menores costos en los componentes LSI y VLSI. La tecnología digital se presta más fácilmente al control del software y de la microprogramación.
- * Multiplexión por división del tiempo: Las señales digitales son fácilmente tratables con técnicas TDM, lo que produce el uso eficiente de las pistas (circuitos) de datos internas, acceso a empresas públicas de transporte y, técnicas de conmutación TDM.
- * Señales digitales de control: Las señales de control son inherentemente digitales y pueden ser fácilmente integradas en un circuito (pista) de transmisión digital vía TDM. El equipo de señalización es independiente del medio de transmisión.
- * Encriptación (poner en símbolos): Esto es más fácilmente acomodado con señales digitales.

Requerimientos para el proceso de llamadas telefónicas:

La característica que distingue la PBX digital de un conmutador digital de datos es su capacidad de manejar conexiones telefónicas. Freeman lista ocho funciones requeridas para el proceso de llamadas telefónicas:

- * Interconexión.
- * Control.
- * Atención (con persona).
- * Comprobación de ocupado.
- * Alerta.
- * Recepción de información.
- * Transmisión de información.
- * Supervisión.

Para entender mejor estos requerimientos veamos la secuencia de pasos necesarios para realizar con éxito una llamada. Primero consideremos una llamada interna desde la extensión 226 a la 280:

- 1.- La 226 descuelga el teléfono. La unidad de control reconoce esta situación.
- 2.- La unidad de control encuentra un receptor digital disponible y fija un circuito desde 226 a él. También fija un circuito desde el generador de tono al 226.
- 3.- Cuando se marca el primer dígito, se libera la conexión del tono. El receptor digital acumula los dígitos marcados.
- 4.- Después de marcar el último dígito, se libera la conexión al receptor digital. La unidad de control examina la legitimidad del número. Si no es válido, el usuario es informado de algún modo, por ejemplo con una conexión a un generador de señal rápida de ocupado. Si es

válido, la unidad de control determina si 280 está ocupado. Si es así, 226 es conectado a un generador de señal de ocupado.

- 5.- Si 286 está libre, la unidad de control fija una conexión entre 226 y un generador de tono de respuesta, y una conexión entre 280 y un timbre.
- 6.- Cuando 280 responde descolgando el teléfono las conexiones del timbre y de tono de respuesta se liberan y se fija una conexión entre 226 y 280.
- 7.- Cuando cualquiera de los dos cuelgue el teléfono, la conexión entre ambos se libera.

Para llamadas al exterior se siguen los siguientes pasos:

- 1-3.- Como antes. En este caso el usuario que llama marcará un número de código de acceso para solicitar acceso a una línea saliente.
- 4.- La unidad de control libera la conexión al receptor digital y encuentra un grupo de líneas de salida libre y envía una señal de descolgado.
- 5.- Cuando se recibe un tono de marca desde la oficina central, la unidad de control repite los pasos 2 y 3.
- 6.- La unidad central libera la conexión con el receptor digital y envía el número a la línea de salida y establece una conexión entre el que llama y la línea de salida.
- 7.- Cuando cualquiera de los dos (el que llama ó la

línea de salida) cuelguen, la conexión entre ambos se liberan.

Sí la PBX realiza el *Routing* de menor coste, esperará hasta que se marque todo el número y luego elige la línea apropiada.

Por último, las llamadas de entrada, sí se pueden hacer llamadas internas directas, se producen como sigue:

- 1.- La unidad de control detecta una señal de tono de línea desde la oficina central y envía una señal de comienzo de llamada al exterior por esa línea. También fija un camino desde esa línea a un receptor digital.
- 2.- Después de que se recibe el último dígito, la unidad de control libera el camino, examinando el número, y mira sí la estación llamada está ocupada, en cuyo caso se devuelve una señal de ocupado.
- 3.- Sí el número llamado está libre, la unidad de control establece una conexión de timbre con el número llamado y una señal de tono de respuesta a la línea.
- 4.- Cuando cualquiera de los dos "suene" colgado, la conexión entre ambos se libera.

Como se ve, los requerimientos para fijar una conexión telefónica son más complejos que los de una conexión de datos.

Requerimientos para la conmutación de mensajes:

Estos requerimientos son los mismos que necesita un conmutador digital de datos. Normalmente, un usuario terminal solicitará la conexión a un puerto del ordenador. Surgen pues las mismas cuestiones de velocidad, síncrono/asíncrono, y técnica de llamada.

La PBX puede soportar estaciones de trabajo de voz/datos con un par trenzado para el teléfono y dos para el terminal. En este ordenamiento, el puerto de destino debe ser elegido desde el teléfono, no desde el terminal.

La PBX tiene la ventaja de la conexión directa con las líneas telefónicas de salida. El usuario de terminal que desee acceder a un ordenador externo debe tener un teléfono y un modem; la PBX puede proporcionar el servicio de enlace. Normalmente, la conexión es con una línea de salida analógica de voz. Para proporcionar el servicio adecuado, la PBX mantiene una colección de modems que pueden ser usados por cualquier dispositivo para comunicarse a través de las líneas externas.

La implementación del juego de modems va a depender de la arquitectura de la PBX. Si consideramos una PBX cuya capacidad de conmutación consista en un conmutador TDM en Bus (figura 7.1). Un dispositivo que quiera comunicar será conectado a un modem libre en el juego. El modem produce señales analógicas que deben ser conmutadas a una línea analógica de salida. Pero la PBX conmuta solamente señales digitales, por lo tanto la salida del modem es llevada a

un Codec (codificador-decodificador) que digitaliza la señal y la vuelve a meter en Bus TDM. Luego, los datos (digitalizados) son conducidos a un interface de línea, en donde la señal es reconvertida a analógica y enviada a su camino por la línea.

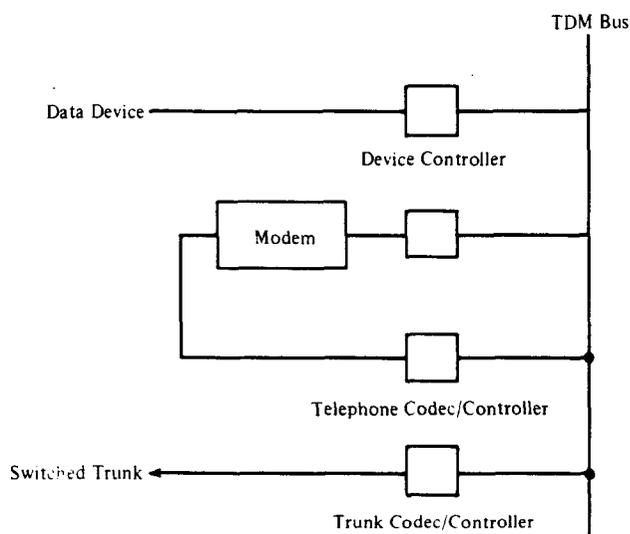


FIGURE 7-1 Use of a Modem in a Digital PBX

La característica más importante es la integración interna de los datos y la voz digitalizada. En ambos casos se usa el mismo mecanismo de conmutación.

Arquitectura de la PBX digital:

Se han desarrollado una buena variedad de arquitecturas para los constructores de PBX digitales, como éstos son sus propietarios, en la mayoría de los casos no conocemos los detalles de las mismas. En esta

sección veremos las características arquitectónicas comunes a todos los sistemas PBX.

Componentes de la PBX digital:

La figura 7.2 muestra una arquitectura del PBX genérica.

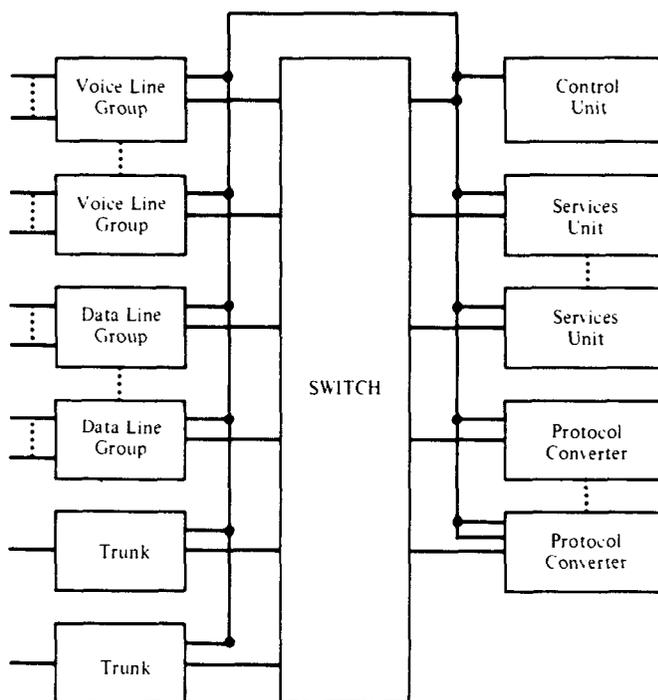


FIGURE 7-2. Generic Digital PBX Architecture

El corazón del sistema es algún tipo de red de conmutación digital. El conmutador (Switch) es responsable de la manipulación y conmutación del flujo de señales digitales multiplexadas en el tiempo. Algunos PBX no tienen una red de conmutación digital como tal, sino que

tienen simplemente un conmutador **TDM** en Bus.

Enganchados al conmutador hay una serie de unidades de interface, las cuales proporcionan acceso hacia/dese el mundo exterior. Generalmente, una interface realizará la función de multiplexado por división en el tiempo para acomodar las múltiples líneas de entrada. Por otro lado, la unidad necesita dos líneas dentro del conmutador para llevar a cabo una operación *Full Duplex*.

Se usan muchos tipos de interfaces. Una unidad de grupo de líneas de datos manejará dispositivos de datos, mientras que una unidad de grupo de líneas analógicas de voz tratará un determinado número de líneas telefónicas. Además, la unidad debe incluir **Decodecs** para las conversiones digital-analógica (entrada) y analógica-digital (salida). El rango de líneas acomodadas por unidad es generalmente de 8 a 24.

Además de estas unidades tenemos las unidades de interface para líneas interurbanas (Trunks) que se usan para conectar con localidad. Estas unidades pueden ser digitales ó analógicas (voz) y pueden transportar tanto datos como voz modulada por **PCM**. La unidad de línea interurbana debe multiplexar y demultiplexar en ambas direcciones (como se ve en la figura 7.3). La necesidad de multiplexar y demultiplexar los "n" canales multiplexados de datos entrantes y no pasarlos directamente desde la entrada al Bus, llenando "n" particiones consecutivas es que; aunque en sistemas con puerto dedicado de no bloqueo

es posible, en sistemas de asignación dinámica en particiones de tiempo, los datos de entrada deben ser almacenados en el *Buffer* y sacados en particiones de tiempo que varían a medida que las conexiones se realizan y se rompen.

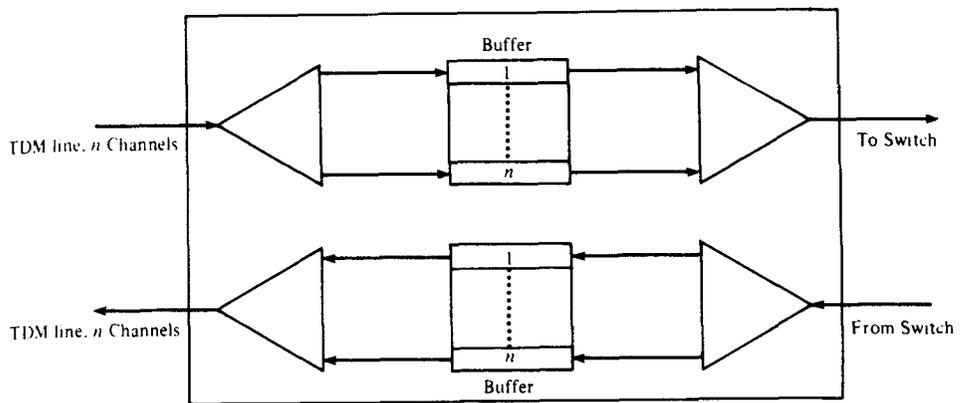


FIGURE 7-3. Operation of a Trunk Interface Unit

Las demás cajas que aparecen en la figura 7.2 pueden ser explicadas rápidamente. La unidad de control opera el conmutador digital y cambia señales de control con los dispositivos enganchados. Para ello se usa otro Bus u otro circuito de datos; así las señales de control no atraviesan el conmutador. Se implementan funciones de control y administración de la red como parte de esto ó como unidad separada. Las unidades de servicio incluirán cosas como generadores de tono y de señal de ocupado, ó/y registros de dígitos marcados. Algunos PBX tienen conversores de protocolo para conectar líneas no

similares; la conexión se hace de cada línea al conversor de protocolos.

Esta arquitectura lleva consigo un alto grado de fiabilidad ya que el fallo de una unidad de interface sólo repercute en la pérdida de un pequeño número de líneas.

Arquitectura distribuida:

Por razones de eficiencia y fiabilidad, algunos fabricantes de PBXs ofrecen arquitecturas distribuidas para sus sistemas más grandes. En ella, la PBX está organizada en un conmutador central y uno ó más módulos distribuidos, con cable coaxial ó fibra óptica entre el conmutador central y los módulos constituyendo una topología jerárquica de dos niveles en Estrella.

Los módulos distribuidos alivian en parte el trabajo en tiempo real del procesador del conmutador central (detección de descolgado). El grado en que la inteligencia central es aliviada de su trabajo varía. En un extremo, los módulos distribuidos serían réplicas del conmutador central, en cuyo caso funcionarían casi autónomamente con la excepción de algunas funciones de gestión general y de contabilidad. En el otro extremo, los módulos son tan limitados como sea posible.

Una arquitectura distribuida implica que a menudo será necesario concatenar varias conexiones para obtener una conexión entre dos dispositivos. Considerando en la figura 7.4 que se desea una conexión entre las líneas "a"

y "b", el proceso sería como sigue: En el módulo A se establece una conexión entre la línea "a" y uno de los canales en una línea externa TDM que va al conmutador central. En el conmutador central, ese canal es conectado a un canal en la línea externa TDM que va hacia B. En el módulo B se conecta este canal a la línea "b".

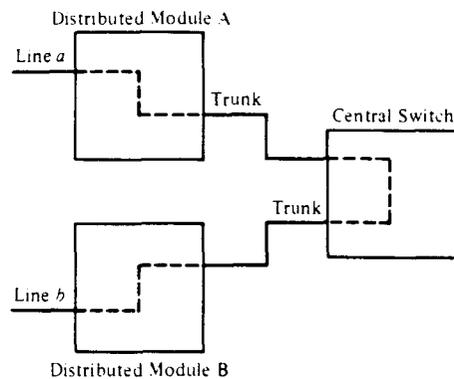


FIGURE 7-4. Circuit Establishment in a Distributed Digital PBX

Las ventajas que presenta esta arquitectura pueden resumirse en:

- * Permite el crecimiento más allá del tamaño práctico de un sólo conmutador central.
- * Proporciona un mejor rendimiento por la descarga de funciones al conmutador central.
- * Proporciona una fiabilidad mayor: La pérdida de un módulo no desarma todo el sistema.

Arquitectura Modular:

Recientemente se ha desarrollado una arquitectura de

conmutador modular, basada en el uso de un tipo de módulo para todos los niveles de conmutación. Un sólo módulo contiene tanto la conmutación de tiempo como la de espacio.

Una razón determinante del desarrollo de esta arquitectura es salvar algunas desventajas inherentes de la conmutación multinivel (tiempo - y - espacio) tradicional. Con la arquitectura tradicional, el diseñador debía decidir de antemano el tamaño (dimensiones) del intercambio, en orden a determinar el número de niveles y el tamaño del conmutador en cada uno de ellos. Estas decisiones determinan un límite inferior de tamaño. Además, se necesita un control central para fijar y liberar los circuitos (camino) a través del conmutador. A medida que el tamaño del conmutador crece, esta tarea se hace muy complicada. Como vamos a ver la arquitectura modular no tiene estas desventajas.

Las ventajas que presenta el conmutador modular frente al digital son:

- * Dimensiones flexibles: Los módulos trabajan como bloques de edificios, permitiendo un gran número de tamaños de conmutadores (de los más pequeños a los más grandes).
- * Control simplificado: La fijación y liberación de circuitos (camino) es distribuida. Cada módulo es inteligente y el control es proporcionado vía circuito.

* Fabricación, testing y mantenimiento simplificados: Hay menos partes a construir e instalar.

La desventaja principal de esta arquitectura es su aumento en el retardo de propagación.

Como cada módulo lleva a cabo una función TSI (Time-Slot-Interchange), en un conmutador grande, un circuito puede pasar por muchos módulos, haciendo que el retardo por TSI sea substancial.

Una unidad TSI opera sobre un flujo síncrono de particiones en el tiempo, ó canales, intercambiando pares de particiones para obtener un funcionamiento *Full Duplex*.

Centrex:

Por último vamos a describir brevemente otro modo de soportar dispositivos de voz y datos en un entorno de oficina. Es conocido como **Centrex**, proporciona los mismos servicios que la **PBX** digital, y aparece como lo mismo al usuario. En contradicción con la **PBX**, **Centrex** realiza las funciones de conmutación en equipos localizados en la oficina central de la compañía telefónica. **Centrex** utiliza tecnología de conmutación de oficina central aumentada para formar un conmutador privado virtual (efectivo). Todas las líneas de teléfono y voz se encaminan desde la casa del cliente al conmutador central. El usuario puede hacer llamadas locales con un número de extensión, dando así la apariencia de conmutador local.

Centrex tiene algunos beneficios frente a PBX:

- * **Fiabilidad y disponibilidad:** El equipo de la oficina central está diseñado para ser fiable, con el uso masivo de redundancia. El personal de apoyo técnico y mantenimiento está siempre disponible en el lugar donde está el conmutador (oficina central).
- * **Flexibilidad:** El usuario no es obligado a conectar un conmutador de un determinado tamaño, sino que puede ampliar o reducir los servicios de acuerdo con sus necesidades.
- * **Ahorro de gastos frente a PBX:** Esto incluye las inversiones de capital, los requerimientos de espacio, y los seguros.
- * **Continua puesta al día de funcionalidad:** Se añaden regularmente nuevas características hardware y software a las ofertas de Centrex.

Centrex no es una red local dada las distancias que se dan.No obstante, desde el punto de vista del usuario esto es irrelevante, y Centrex es un gran competidor de la PBX.

7.2

PBX DIGITAL VERSUS LAN.

Hay un claro solapamiento entre las capacidades

ofrecidas por un sistema PBX digital y una LAN. Ambos pueden soportar un gran número de dispositivos digitales. El comprador que debe elegir una de ellas debe hacerlo en base a sus requerimientos y el coste de una u otra. En esta sección vamos a comparar ambas tecnologías en base a una lista de categorías en las que pueden ser comparadas. Esta lista fué propuesta por G.M.Pfister y B.U.O'brien en su obra "Comparing CBX to the local Network-and the winner is" editada en mayo de 1.982. Estas categorías son:

- * Instalación.
- * Fiabilidad.
- * Tipos de datos.
- * Distancia.
- * Velocidad.
- * Capacidad.
- * Coste.

La instalación del cable para una LAN en un edificio ya terminado es una tarea larga y costosa. Puede que éste llegue al 50% del coste total de la LAN. En cambio la PBX necesita conexiones de teléfonos, normalmente par trenzado. La conexión de datos, usando señales digitales, requiere normalmente dos pares trenzados para cada línea *Full Duplex*. Por lo tanto, con PBX, si un usuario quiere tener un terminal y un teléfono en la oficina, sólo necesita tres líneas de pares trenzados. Por otro lado casi todas las oficinas tienen cableado de par trenzado ya instalado para los servicios tradicionales de teléfonos.

Es más, las PBX están casi instaladas al poder disponer de la instalación de la red del edificio. Así que la mayoría de las PBXs tienen un buen número de pares de cables disponibles. Esto podría suponer un enorme ahorro con respecto a las LANs.

En lo que se refiere a la fiabilidad, hay problemas en ambas. Aunque pueda parecer lo contrario, los problemas de fiabilidad pueden ser más acentuados en las LANs. Los sistemas PBX pueden hacerse totalmente redundantes, eliminando virtualmente los fallos de la red entera. Pero hay situaciones en las que se pueden quedar anuladas partes de las LANs ó incluso su totalidad.

Tanto la PBX como la LAN pueden tratar adecuadamente la mayoría de los requerimientos de la comunicación digital de datos. La PBX es superior al poder tratar la voz. La naturaleza centralizada del control de la PBX es ideal para el procesamiento de la voz en un entorno de oficina. Otro tipo de transmisión -video- sólo puede realizarse con una LAN de banda ancha.

En términos de velocidad, la LAN es superior. La tercera generación de PBX soportan normalmente velocidades de 64 Kbps. Una LAN puede, con los interfaces adecuados, acomodar conexiones en el rango de Mbps. Para muchos usuarios, 64 Kbps puede parecer infinito, no obstante, algunas de las estaciones de trabajo más nuevas (con gráficos de alta resolución) requieren velocidades superiores. Es más, las operaciones de transferencia de

ficheros pueden verse seriamente retrasadas a esas bajas velocidades.

En cuanto a la capacidad puede aparecer la PBX con ventaja sobre la LAN. La capacidad total de transferencia digital en una PBX puede llegar hasta 500 Mbps (que es, por ejemplo, la velocidad en un Bus TDM). Los buses de banda base y los sistemas de anillo tienen mucho menos, e incluso una banda ancha sólo tiene 300 Mbps. No obstante, hay que tener en cuenta la naturaleza del tráfico. La mayoría del tráfico digital en la oficina es en ráfagas por naturaleza (tráfico terminal-ordenador principal). En una LAN, la red es utilizada por un nodo sólo en lo que dura la ráfaga. Pero en una PBX, un nodo consumirá una porción dedicada de la capacidad a lo largo de la duración de la conexión.

El último factor a analizar es el coste. Aquí no existe una respuesta definitiva, en parte debido a que el coste de los componentes varía rápidamente, y en parte porque el coste de su instalación depende de factores como el lugar, la infraestructura, etc.,.

Por último hay un último punto de comparación que no está en nuestra lista. Este punto se refiere a la naturaleza del interface. En un sistema de conmutación de circuitos, la red es normalmente "transparente"; esto es, dos dispositivos conectados se comunican como si tuviesen una conexión directa. En un sistema de conmutación de paquetes, surge la cuestión del protocolo entre la red y

el dispositivo enganchado a ella. Este tema es el que trataremos en el siguiente capítulo.

INTERFACE DE RED

En los capítulos anteriores nos hemos centrado en el estudio de las características y capacidades de varios tipos de redes locales, pero hemos tratado poco el tema del dispositivo que hace posible la conexión de un ordenador a la red. Dado que el propósito de una red local es proporcionar un medio de comunicación entre una serie de dispositivos conectados a ella, la interface entre la red y los dispositivos enganchados a ella debe permitir una cooperación interactiva. En este capítulo trataremos tanto las conexiones de dispositivos digitales a redes de paquetes conmutados como lo relacionado con las redes de circuitos conmutados y los dispositivos analógicos.

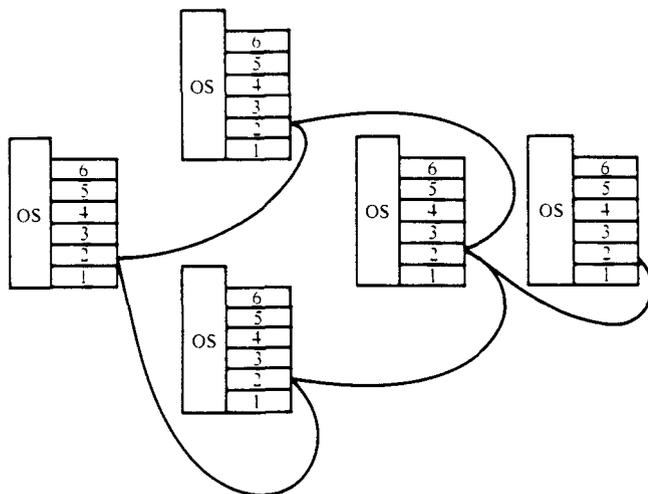
EL REQUERIMIENTO.

Para comprender la necesidad de un interface de red vamos primero a considerar desde el punto de vista del vendedor, cómo proporcionar una capacidad de conexión a una red de un ordenador. Muchos vendedores ofrecen un cierto tipo de posibilidad de conexionado a red; aplicaciones como transferencia de ficheros, correo electrónico, etc, están disponibles para ser corridas en una red de ordenadores y de terminales inteligentes. El vendedor proporciona estas aplicaciones con un paquete software de comunicaciones y de conexionado a red. Dos ejemplos son la **SNA** de IBM y la **DECNET** de DEC. Para mayor claridad, consideraremos un paquete genérico basado en el modelo OSI.

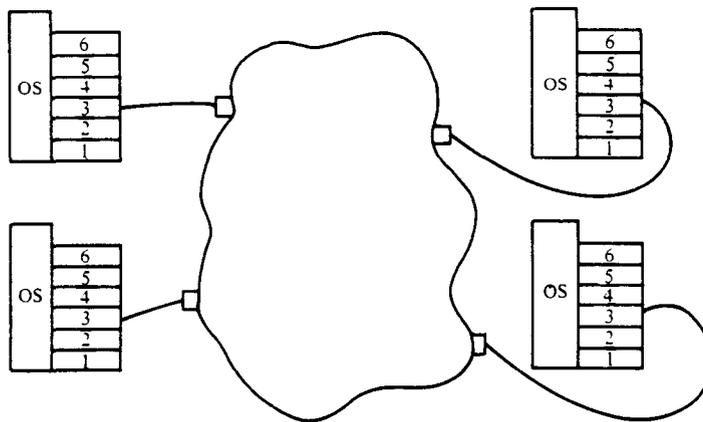
Es importante señalar que el modelo OSI no proporciona una arquitectura para la interconexión múltiple de computadoras; se trata de un modelo para comunicación entre dos computadoras, basado en una serie de protocolos. La interconexión requiere no sólo protocolos de comunicación sino la gestión de la red, facilidad de nombramiento, servicios de red, etc.

Los protocolos de comunicación, como los compatibles con el modelo OSI, proporcionan una base para la interconexión de ordenadores. Tradicionalmente, ésto ha

sido llevado a cabo de dos modos distintos, como se muestra en la figura 8.1. Una oferta común de los vendedores es la red privada (8.1a).



a. Private Network



b. Public Network

FIGURE 8-1. Approaches to Computer Networking

Los ordenadores están conectados mediante enlaces punto-a-punto, los cuales pueden ser acoplamientos

directos locales ó de larga distancia; ambas pueden ser de marcación manual ó alquilada (dedicada). En este caso no surge la necesidad de un interface de red. En la figura 8.1b se nos muestra una interconexión de ordenadores (LAN) ya tratada en el capítulo 2. Como se recordará, la LAN consiste en una serie de conmutadores y líneas de comunicación configuradas para proporcionar conectividad entre los dispositivos enganchados. la LAN proporciona, entre otros, tres servicios relevantes:

- * Routing.
- * Multiplexado.
- * Interface estandarizado.

Este último servicio permite al usuario enganchar dispositivos de diferentes vendedores sí estos respetan los standards. Sí la LAN usara un interface de uso interno, el usuario se vería forzado a procurarse el hardware y software necesarios para engancharse a la LAN, y tendría que hacer lo mismo para cada dispositivo de diferente tipo que se enganchara a la red y que éste sea standard se hace patente.

Desde el punto de vista del comprador la interface de red es una cuestión importante ya que normalmente va a tener equipos de procesado que quiere meter en la red que va a comprar. El comprador también valorará la flexibilidad que le proporcione la red para la futura adquisición de equipos de diferentes vendedores. El problema pues, para el comprador, es elegir una red local

cuyo interface acomode una variedad de equipos con la adición de poco ó ningún software especial para el mismo.

8.2

INTERFACE PARA CONMUTACION DE PAQUETES.

Procedimiento de enganche a una LAN/HSLN:

La transmisión por paquetes es usada tanto en las LANs como en las HSLNs. Como ya hemos visto, la conmutación de paquetes implica que los datos a enviar a través de la red por un dispositivo están organizados en paquetes que son mandados a través de la red uno a uno. Los protocolos deben usarse para especificar la construcción e intercambio de esos paquetes. En una red local se necesitan como mínimo, protocolos en las capas 1 y 2 para controlar la comunicación multiacceso de la red (estas capas comprenderían el LLC, MAC, y las funciones físicas especificadas por el IEEE 802).

Por lo tanto, todos los dispositivos enganchados deben compartir estos protocolos comunes de red local. Desde el punto de vista del comprador, este hecho divide en tres los modos en los que un dispositivo puede engancharse a una LAN ó HSLN (figura 8.2):

- * Procedimiento homogéneo/vendedor único.
- * Procedimiento de "standards".
- * Procedimiento de interface standard de red.

El primero es aquel en que todo el equipo (red y dispositivos enganchados a ella) está proporcionado por un sólo vendedor. Todo el equipo comparte un mismo paquete software de comunicación e interconexión.

Indudablemente muchos compradores adoptarán esta solución ya que simplifica la responsabilidad del mantenimiento y proporciona un camino fácil para la evolución del sistema. Pero se reduce la capacidad de tener los mejores equipos para una determinada aplicación (de diferentes vendedores).

El segundo procedimiento es adquirir una red local que se ajuste a un standard, y poder elegir todos los equipos que cumplan ese standard. La red local consistirá en un medio de transmisión y un juego expandible de "puntos de conexión". Este procedimiento, aunque atractivo, tiene algunos problemas. El standard de IEEE para LANs está cargado de opciones, por lo que los dispositivos etiquetados como compatibles según la IEEE, pueden no ser capaces de coexistir en la misma red. El standard para HSLN de ANSI tiene una forma todavía más borrosa. En ambos casos, los standards no puntualizan las funciones esenciales de la gestión de la red. Sin un standard para la gestión de la red, es improbable que equipos para red local de diferentes vendedores puedan ser mezclados con éxito en un única red local.

En el último procedimiento consideramos una red local que consiste no sólo en un medio de transmisión, sino

también en una serie de dispositivos inteligentes que implementan los protocolos de la red local y proporcionan una capacidad de *Interfacing* para el enganche de dispositivos a la misma. Este dispositivo se denomina NIU (Network Interface Unit). El NIU controla de, manera colectiva, el acceso hacia y a través de la red local. Los dispositivos que se enganchan a la red lo hacen a través del NIU. La conexión entre dispositivo y el NIU se realiza mediante algún standard de comunicación ó por un interface I/O. Los detalles de funcionamiento de la red se le ocultan al dispositivo.

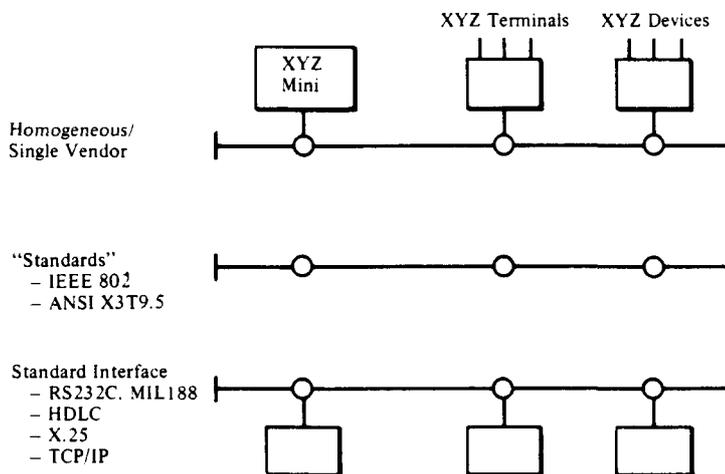


FIGURE 8-2. Approaches to LAN/HSLN Attachment

La arquitectura NIU es comunmente usada por vendedores independientes de redes locales (aquellos que venden sólo redes, no el equipo de proceso de datos que usa la red). Por tanto, en muchos casos los NIUs de una

configuración de red local provienen de un vendedor distinto al que suministra los equipos terminales y ordenadores. Este procedimiento tiene varias ventajas. Primero, los dispositivos enganchados se libran de la carga de la lógica de procesamiento de la red local. Segundo, el usuario tiene más flexibilidad para elegir el equipo que quiere meter en la red. No es necesario que el equipo soporte el tipo particular de red local que el usuario ha implementado. Sólo es necesario que el NIU y el equipo a enganchar compartan un interface estandarizado común.

La unidad de interface de red:

El NIU es un dispositivo basado en un microprocesador que actúa como controlador de comunicaciones para proporcionar servicio de transmisión de datos a uno ó más dispositivos enganchados. el NIU transforma la velocidad y el protocolo del dispositivo enganchado a los del medio de transmisión de la red local y viceversa. En términos generales, el NIU realiza las siguientes funciones:

- * Acepta datos del dispositivo enganchado.
- * Almacena (Buffer) los datos hasta que se obtiene acceso al medio.
- * Transmite los datos en paquetes direccionados.
- * Examina cada paquete que pasa por el medio en busca de su propia dirección.
- * Lee los paquetes dirigidos a él y los almacena.

* Transmite los datos al dispositivo enganchado.

El interface hardware entre el NIU y el dispositivo enganchado es típicamente un interface serial de comunicaciones como la RS-232-C. Casi todos los ordenadores y terminales soportan este interface. Para velocidades mayores se puede usar un interface paralelo, como un interface DMA. La figura 8.3 muestra una arquitectura genérica para un NIU.

El NIU puede ser tanto un dispositivo externo como interno. Como dispositivo externo, el NIU es una unidad aislada, que puede tener uno ó varios puertos de comunicación para el enganche de dispositivos. Como dispositivo interno, el NIU está integrado en el chasis del dispositivo procesador de datos (terminal ó mini). Generalmente, un NIU interno consiste en una ó varias tarjetas de circuitos impresos conectados internamente al Bus del sistema del dispositivo.

Desde el punto de vista del comprador, un NIU con opciones standards de *Interfacing* resuelve, al menos a nivel eléctrico, el problema de la interconexión. Desde el punto de vista del diseñador, el NIU es un concepto arquitectónico útil. Sea homogénea ó no la red, y sea la interface standard ó no, debe haber alguna lógica distribuida que controle el acceso a la red local. Conceptualizando esta lógica como un NIU, nos ayuda a clarificar algunas de las cuestiones arquitectónicas asociadas a las aplicaciones en una red local.

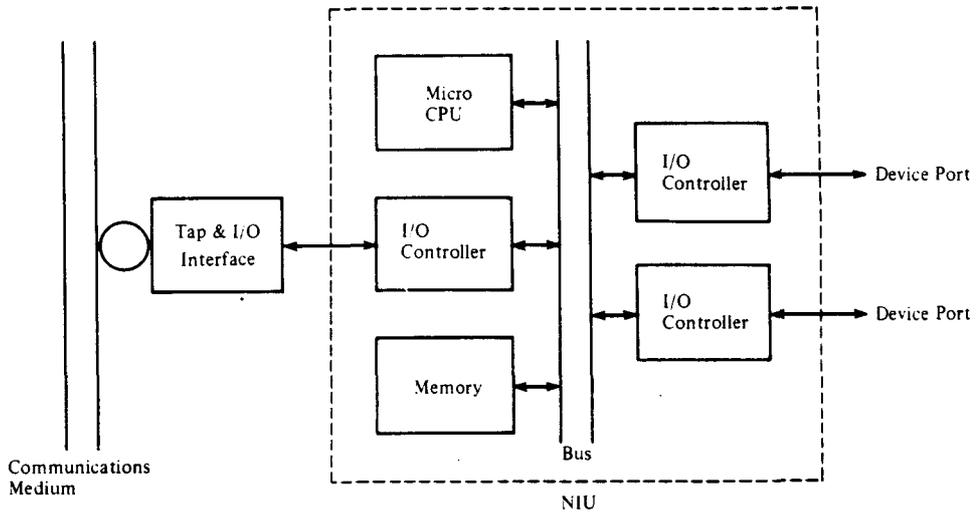


FIGURE 8-3. NIU Architecture

Las preguntas que pueden surgir son: ¿Qué capas de la arquitectura de comunicaciones deben residir en el NIU?; y por tanto ser consideradas parte del servicio de la red local. Y ¿Cuales deben residir en el dispositivo enganchado?. La elección va a depender de una serie de factores, incluyendo coste y rendimiento. Hasta hoy hay poca experiencia con la mayoría de estas alternativas que nos sirva de guía.

No obstante podemos señalar que la principal ventaja de colocar tantas capas como sea posible en el NIU es que esto hace más sencillo el enganche de dispositivos inteligentes. Por otro lado, si ponemos las menos posibles en la red, incrementamos la flexibilidad de la misma.

INTERFACE PARA CONMUTACION DE CIRCUITOS.

Las cuestiones referentes a la interface en redes locales de circuitos conmutados son más simples que en las redes de paquetes conmutados. Con una red local de conmutación de circuitos, como una **PBX** digital, el modo de enganche es esencialmente transparente.

Como antes, hay dos fases de operación, una fase de conexión y otra de transferencia de datos. La fase de transferencia de datos usa **TDM** asíncrona; por lo que no se necesita ningún tipo de lógica ni protocolos. Se trata de una conexión verdaderamente transparente.

En la fase de conexión, la cuestión principal es el medio por el cual el dispositivo enganchado solicita una conexión. Para aclarar ideas, nos vamos a fijar en la figura 7.2, en la que veíamos que cada dispositivo de datos digital se enganchaba a la red vía alguna forma de grupo de líneas de datos (líneas de transmisión de datos). Al menos se usan tres tipos de establecimiento de conexión:

- 1.- Los dispositivos de datos normalmente se conectan por medio de pares trenzados; por tanto, debe haber un excitador de línea (Line Driver) cerca del dispositivo de datos, al cual se enganche éste. Este dispositivo puede incluir

un sencillo teclado numérico para elegir destino.

- 2.- Tanto el excitador de línea ó el grupo de líneas de transmisión de datos (preferiblemente este último) pueden incluir la lógica necesaria para conducir un diálogo simple con un terminal. En este caso, el usuario del terminal entra la solicitud de conexión por medio del terminal.
- 3.- El dispositivo enganchado puede contener un programa simple de I/O que genere peticiones de conexión de forma comprensible por la red .

Independientemente de las formas la arquitectura de conmutador puede soportar la configuración de red privada mostrada en la figura 8.1a.

Por último, señalar que la facilidad que proporciona el convertidor de protocolo que aparece en la figura 7.2 actúa como puerta de acceso entre dispositivos con protocolos distintos. Este convertidor es utilizado, por ejemplo, para la conversión entre terminales ASCII asíncronos y el protocolo síncrono IBM 3270.

8.4

INTERFACES PARA DISPOSITIVOS ANALOGICOS.

Hay muy pocos casos de enganches de dispositivos analógicos a una red. El más común es el teléfono. Los

teléfonos analógicos son fácilmente acomodados en una PBX que incluya un Codec en el grupo de línea (figura 7.2). Otro lugar donde se pueden encontrar dispositivos analógicos es en una red de banda ancha. Como hemos visto, estas redes pueden acomodar fácilmente enganches de dispositivos de audio y video, sólo con dedicarles unos canales para su uso.

PARTE III

RENDIMIENTO DE LAS REDES: LAN/HSLN

Está más allá del objeto de este trabajo el proporcionar expresiones analíticas de medición del rendimiento para todos los sistemas estudiados; eso requeriría un trabajo entero sobre el tema. En este capítulo pretendemos estudiar las técnicas que pueden serle útiles al analista para realizar un cálculo aproximado del rendimiento de la red. En este sentido, el capítulo 9 tiene dos objetivos:

- * Dar una visión interna de los factores que afectan al rendimiento así como el rendimiento relativo de algunos diseños de red local.
- * Facilitar una serie de técnicas que son útiles

para el dimensionamiento de una red y para obtener unas primeras aproximaciones al rendimiento de la misma.

9.1

CONSIDERACIONES DE RENDIMIENTO EN LAN/HSLN.

Las características principales de una LAN que estructura la manera en que se analiza su rendimiento son que hay un medio de acceso compartido, que se requiere un protocolo de control del acceso al mismo, y que se usa una conmutación de paquetes. Los HSLNs comparten estas características. Ambas redes tendrán las mismas consideraciones básicas así como los mismos procedimientos de análisis de rendimientos.

Medidas de rendimiento:

Hay tres medidas del rendimiento de LANs y HSLNs que se usan frecuentemente:

- * **D:** Retardo que se produce desde que un paquete ó frame está listo para la transmisión desde un nodo hasta que se completa la transmisión con éxito.
- * **S:** La capacidad de tratamiento; cantidad total de datos transmitidos entre nodos (carga transportada).

* U: La utilización del medio de la red local; la fracción del total de la capacidad usada.

El parámetro S es frecuentemente normalizado y expresado como una fracción de capacidad. Por ejemplo, Si en un canal de 10 Mbps la suma de las transferencias realizadas con éxito entre nodos durante 1s es de 1 Mb, entonces $S = 0.1$

Los resultados para S y D son generalmente impresos como una función de la carga ofrecida G, que representa la carga actual ó la demanda de tráfico presentada a la red local. Observar que S y G son parámetros distintos. S es el porcentaje normalizado de paquetes de datos transmitidos con éxito; G es el número total de paquetes ofrecidos a la red; eso incluye paquetes de control, como Tokens, y colisiones, los cuales son paquetes destruidos que han de ser retransmitidos. También G es a menudo expresada en fracciones de capacidad. Intuitivamente vemos que D aumenta conforme lo hace G: a mayor tráfico compitiendo por tiempo de transmisión, mayor retardo para cada transmisión individual. S también aumentará con G, hasta un cierto punto de saturación por encima del cual la red no puede manejar más carga.

La figura 9.1 muestra la situación ideal: la utilización del canal aumenta con la carga hasta una carga ofrecida igual a la capacidad total del sistema; a partir de ahí la utilización del canal se mantiene al 100%. Desde luego cualquier sobrecarga ó ineficiencia producirá una

caída del rendimiento. La comparación entre S y G nos muestran el comportamiento del sistema en base a la carga actual en él.

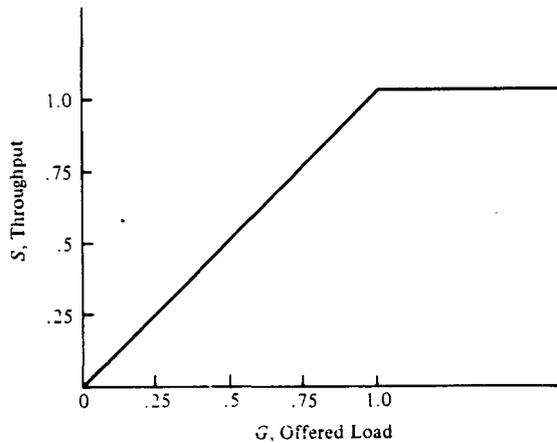


FIGURE 9-1. Ideal channel utilization.

En resumen hemos introducido dos nuevos parámetros:

G: La carga ofrecida a la red local; cantidad total de datos presentados a la red para su transmisión.

I: Carga de entrada; el total de datos generados por los dispositivos enganchados a la red local.

La tabla 9.1 es un ejemplo simplificado para mostrar la relación entre estos parámetros. En este ejemplo tenemos una capacidad $C = 1.000$ Frames por segundo. Por simplicidad, I, S y G se expresan en Frames por segundo. Se supone que un 1% del total de los Frames transmitidos se pierden y deben ser retransmitidos. Por lo tanto, con

una entrada $I = 100$ Frames por segundo se repetirá un *Frame*. Luego $S = 100$ y $G = 101$. Suponiendo que la carga de entrada llega por tandas, una vez por segundo. Entonces, para $I = 100$, $D = 0.0505$ segundos. La utilización es definida como el cociente S/C . En este caso $U = 0.1$

TABLE 9.1 Example of Relationships Among LAN/HSLN Measures of Performance^{a,b}

<i>I</i>	<i>S</i>	<i>G</i>	<i>D</i>	<i>U</i>
100	100	101	0.0505	0.1
500	500	505	0.2525	0.5
990	990	1000	0.5	0.99
2000	990	—	—	0.99

^aCapacity: 1000 frames/sec.

^b*I*, input load (frames per second); *S*, throughput (frames per second); *G*, offered load (frames per second); *D*, delay (seconds); *U*, utilization (fraction of capacity).

Los otros ejemplos de valores de *I* son fácilmente comprobables. Obsérvese que para $I = 990$ se usa la totalidad de la capacidad del sistema ($G=1000$). Si *I* aumenta por encima de este punto, el sistema no puede continuar. Sólo serán transmitidos 1000 Frames por segundo. Por tanto *S* permanecerá en 990 y *U* en 0.99 Pero *G* y *D* crecen sin límite a medida que se acumulan más y más peticiones.

El efecto del retardo de propagación y la velocidad de transmisión:

Recordando la figura 1.1, las redes locales se diferenciaban por un lado de los sistemas de

multiprocesadores y por otro de las redes de larga distancia por la velocidad empleada (R) y por la distancia de los caminos de comunicaciones (d). De hecho es el producto de estos dos términos (R x d) el que puede caracterizar las redes locales. Es más, como veremos, este término (o derivados de él) es el parámetro simple más importante para determinar el rendimiento de una red local. Veremos como el rendimiento es el mismo para un Bus de 1 Km a 100 Mbps que para uno de 10 Km a 10 Mbps.

Una buena manera de ver el significado de R x d es dividir este producto por la velocidad de propagación del medio, el cual es constante en la mayoría de ellos. Una aproximación correcta para la velocidad de propagación es de aproximadamente dos tercios de la velocidad de la luz: 2×10^8 m/s. Un análisis dimensional de la fórmula

$$\frac{Rd}{v}$$

muestra que es igual a la longitud en bits del medio de transmisión, esto es, el número de bits que pueden estar en tránsito entre dos nodos en un momento dado.

Podemos observar que esto sí diferencia a las redes locales de los sistemas multiprocesador y de las redes de larga distancia. En un sistema multiprocesador, hay generalmente sólo unos pocos bits en tránsito. Por ejemplo la última oferta de IBM sobre canales I/O opera hasta 24Mbps en una distancia de hasta 120 m, la cual admite como máximo 15 bits. La comunicación procesador-procesador

en un ordenador normalmente soporta menos bits en tránsito que estos 15. Por otro lado la longitud en bits de una red de larga distancia puede ser de cientos de miles de bits. En medio tenemos las redes locales. Podemos citar ejemplos como: un sistema Ethernet de 500 m a 10 Mbps tiene una longitud en bits de 25; tanto un HYPERchannel de 1 km a 50 Mbps con una típica LAN banda ancha de 5 Km a 5 Mbps tienen alrededor de 250 bits de longitud.

Una manera útil de considerar la longitud del medio es comparándola con el típico *Frame* transmitido. Los sistemas multiprocesadores tienen unas longitudes de bits muy cortas comparadas con la longitud del *Frame*; las redes de larga distancia tienen una longitud muy grande. Las redes locales varían desde las más cortas que un *Frame* hasta las que llegan al mismo orden de magnitud que un *Frame*.

Esto introduce una diferencia en la comparación de las redes locales con los ordenadores multiprocesador. Hablando en términos relativos, en un sistema multiprocesador las cosas suceden casi simultáneamente; Cuando un componente comienza a transmitir, el otro lo sabe casi al instante. En las redes locales, el vacío relativo de tiempo conlleva toda clase de complicaciones en los protocolos de control de acceso al medio, tal y como hemos visto. Comparando las redes de larga distancia con las locales, para obtener alguna eficiencia, el enlace de larga distancia debe permitir que hayan varios *Frames*

en tránsito simultáneamente. Esto introduce requerimientos específicos en el protocolo de la capa de enlace. Los protocolos de LAN y HSLN normalmente permiten la transmisión de un sólo *Frame* cada vez, ó sólo unos pocos en algún protocolo para Anillo. De nuevo ésto afecta al protocolo de control de acceso.

La longitud del medio, expresado en bits, en comparación con la longitud típica del *Frame* se denomina usualmente como *a*:

$$a = \frac{\text{Longitud del camino de datos (bits)}}{\text{Longitud del Frame}}$$

También podemos poner:

$$a = \frac{Rd}{VL}$$

donde *L* es la longitud del *Frame*, *d/V* es el tiempo de propagación en el medio (en el peor caso), y *L/R* es el tiempo que emplea un transmisor en insertar un *Frame* completo en el medio. Luego:

$$a = \frac{\text{tiempo de propagación}}{\text{tiempo de transmisión}}$$

Los valores típicos de *a* para un LAN van desde 0.01 a 0.1 y de 0.1 a 1 para una HSLN. La tabla 9.2 da algunos valores para una topología Bus. A la hora de calcular *a*, hay que tener en cuenta el tiempo máximo de propagación en

una red de banda ancha es el doble de la longitud del camino más largo desde el extremo. Para un Bus de banda base y para un Anillo se debe incluir el retardo del repetidor en el tiempo de propagación.

TABLE 9.2 Values of a

Data Rate (Mbps)	Packet Size (bits)	Cable Length (km)	a
1	100	1	0.05
1	1,000	10	0.05
1	100	10	0.5
10	100	1	0.5
10	1,000	1	0.05
10	1,000	10	0.5
10	10,000	10	0.05
50	10,000	1	0.025
50	100	1	2.5

El parámetro a determina un límite superior en la utilización de una red local. Supongamos un mecanismo de acceso perfectamente eficiente que permite sólo una transmisión cada vez. Tan pronto como se termina una transmisión, otro nodo comienza a transmitir. Es más, supongamos también que la transmisión es "sólo" de datos, sin bits de encabezado ni de final. (Nota: estas condiciones están muy cerca de ser encontradas en un conmutador digital pero no, ni mucho menos, en las LANs y HSLNs). En estas condiciones ¿Cuál será la utilización máxima de la red?. Esta puede ser expresada como la relación entre la capacidad de tratamiento total del

sistema (Throughput) y la capacidad ó ancho de banda.

$$\begin{aligned}
 U &= \frac{\text{throughput}}{R} = \\
 &= \frac{L / (\text{propagation} + \text{transmission time})}{R} = \\
 &= \frac{L / (d/V + L/R)}{R} = \frac{1}{a + 1} \quad (9.1)
 \end{aligned}$$

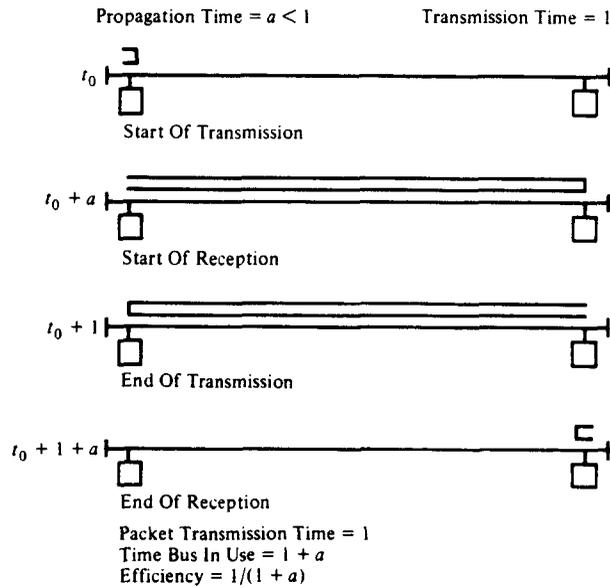


FIGURE 9-2a. Effect of a on utilization: baseband bus ($a < 1$)

Luego, la utilización varía inversamente con a . Esto puede verse intuitivamente viendo las figuras 9.2a. En ella se muestra un Bus de Banda Base con dos estaciones

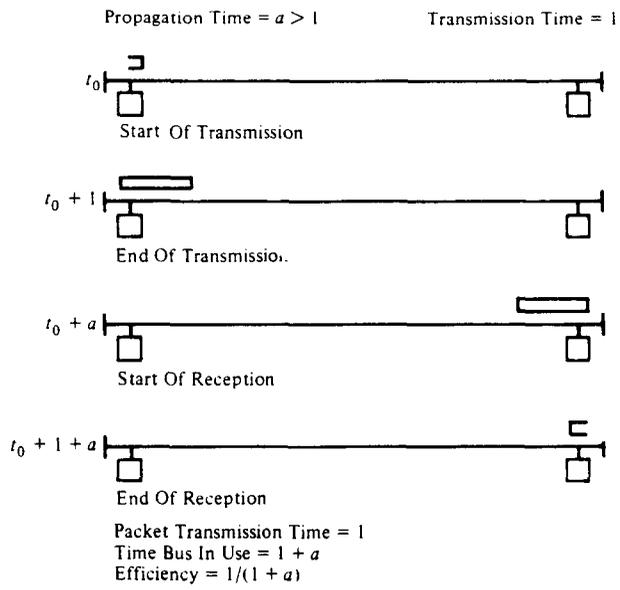


FIGURE 9-2b. Effect of a on utilization; baseband bus ($a > 1$)

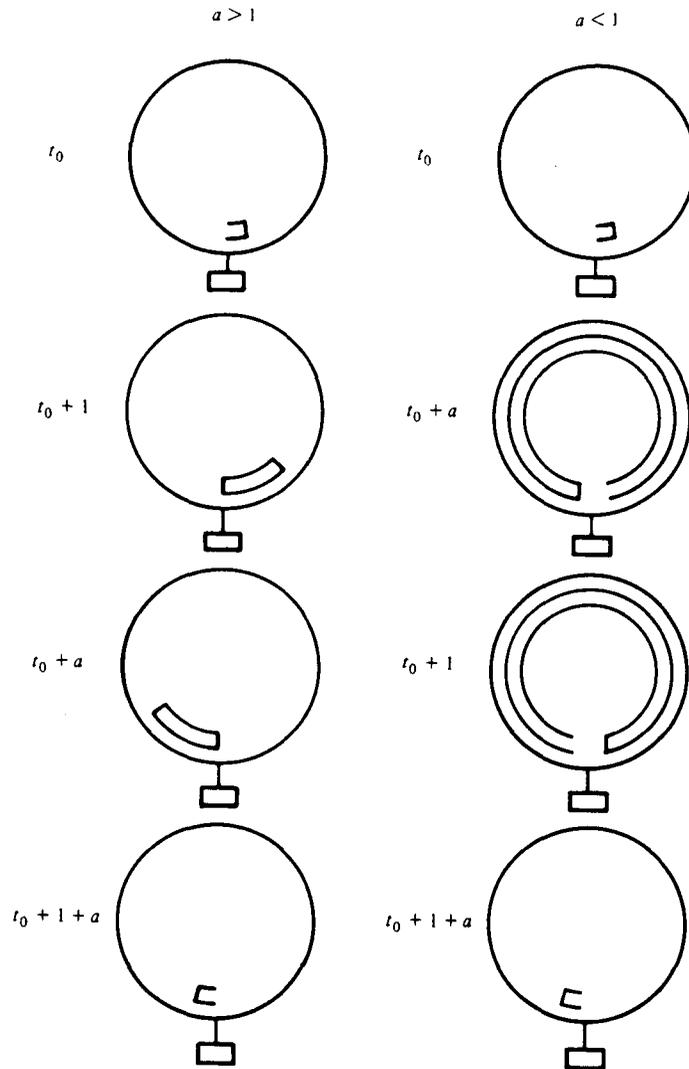


FIGURE 9-3. Effect of a on utilization: ring

tan alejadas como es posible (peor caso), las cuales se turnan para enviar *Frames*. Si suponemos que el tiempo de transmisión es 1 s, la secuencia de acontecimientos sería:

- 1.- La estación A comienza la transmisión en t_0 .
- 2.- La recepción empieza en $t_0 + a$.
- 3.- La transmisión se completa en $t_0 + 1$.
- 4.- La recepción termina en $t_0 + 1 + a$.
- 5.- La otra estación comienza a transmitir.

Si $a > 1$ (figura 9.2b), el paso 3 sucederá antes que el paso 2. En cualquiera de los dos casos el tiempo total de un "turno" de transmisión es $1 + a$, pero el tiempo de transmisión es sólo de 1 s para una utilización de $1/(1+a)$.

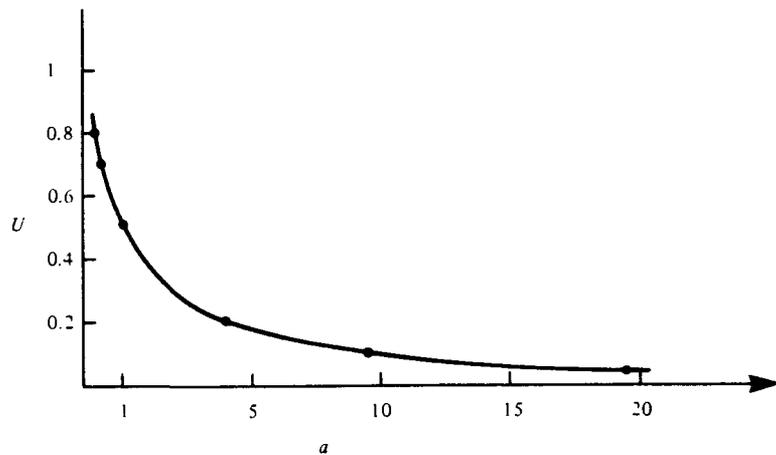


FIGURE 9-4. Utilization as a function of a

El mismo efecto puede observarse aplicado a una red en Anillo en la figura 9.3. En este caso, suponemos que

una estación transmite y espera a recibir su propia transmisión antes de que otra estación transmita. Se produce la misma secuencia de eventos que antes.

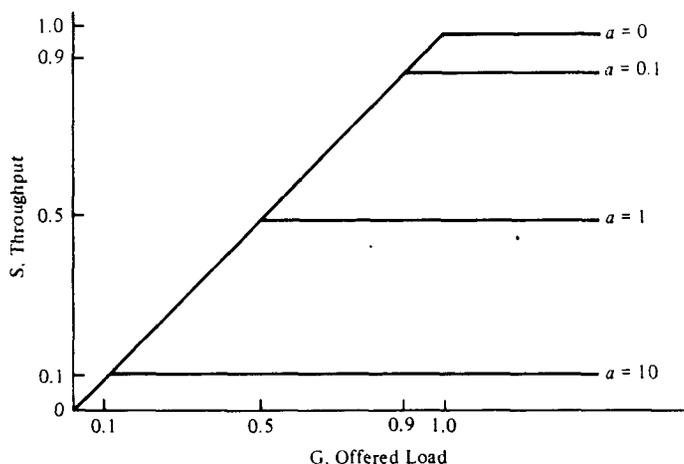


FIGURE 9-5. Effect of a on throughput

La representación gráfica de la ecuación (9.1) es la figura 9.4, y los efectos de a sobre la capacidad de tratamiento (en función de valores de a) están representados en la figura 9.5.

Podemos decir pues, que un límite superior en la utilización de una LAN ó HSLN es $1/(1 + a)$, independientemente del protocolo de control de acceso utilizado. Hay que hacer dos advertencias: a) Este ejemplo asume que en cada transmisión se consume el tiempo de propagación; b) También se supone que sólo se hace una transmisión cada vez. Estas suposiciones no son siempre ciertas; no obstante, la fórmula $1/(1 + a)$ es casi siempre un límite superior válido, dado que la sobrecarga de bits

del protocolo de acceso al medio compensa con creces la falta de validez de estas suposiciones.

La sobrecarga de bits es inevitable. Los *Frames* deben incluir bits de sincronización y direccionamiento. También hay sobrecarga administrativa para controlar el protocolo, es más hay formas de sobrecarga específicas para varios protocolos.

Tenemos aquí dos efectos distintos. Uno es que la eficiencia o utilización del canal disminuye al aumentar a . Esto, por supuesto, afecta a la capacidad de tratamiento. El otro efecto es que la sobrecarga atribuible a un protocolo ocupa ancho de banda y por tanto reduce la utilización efectiva y la capacidad de tratamiento efectiva.

Esto nos lleva a la conclusión de que es deseable mantener a lo más bajo posible. Volviendo a la fórmula Rd/LV , para una red fijada, a puede ser reducida aumentando el tamaño del *Frame*. Esto es útil sólo en el caso de que la longitud de los mensajes producidos por una estación sea un múltiplo entero del tamaño del *Frame* (excluyendo los bits de sobrecarga). De otro modo, el gran tamaño del *Frame* sería en sí una fuente de pérdidas. Es más, un *Frame* "grande" incrementa el retardo para otras estaciones. Esto nos conduce al siguiente punto: los distintos factores que afectan al rendimiento de las LAN/HSLNs.

Factores que afectan al rendimiento:

A continuación vamos a listar aquellos factores que afectan al rendimiento de una LAN ó una HSLN. Trataremos la parte que es independiente de los dispositivos enganchados, es decir, aquellos factores que están exclusivamente bajo el control del diseñador de la red local. Los factores principales son:

- * Capacidad.
- * Retardo de propagación.
- * Número de bits por *Frame*.
- * Protocolos de red local.
- * Carga ofrecida.
- * Número de estaciones.

Los tres primeros factores ya han sido estudiados; ellos determinan el valor de *a*.

El cuarto son los protocolos de red local: físico, acceso al medio, y enlace. La capa física probablemente no pueda ser considerada un factor; generalmente, ésta puede continuar con las transmisiones y recepciones con un pequeño retardo. La capa de enlaces añadirá algunos bits de sobrecarga a cada *Frame* y algunos administrativos, como la confirmación (ACK). Esta área la veremos detenidamente en la sección 9.4 ya que se considera como una parte del rendimiento punto-a-punto (end-to-end). Esto nos deja con la capa de acceso al medio la cual puede tener un efecto significativo sobre el rendimiento de la red. Este punto será tratado en las secciones 9.2 y 9.3.

Nosotros podemos pensar en los tres primeros factores de la lista como características de la red ya que generalmente se tratan como constantes ó datos conocidos. El protocolo de red local es el foco del esfuerzo del diseño, es la elección que se debe hacer. Los dos factores siguientes de la lista (carga ofrecida y número de estaciones) son a menudo tratadas como variables independientes. El analista tiene la misión de determinar el rendimiento en función de estas variables. Estas variables han de ser tratadas por separado. Sí bien es verdad que para una carga fija ofrecida a la red aumenta al aumentar el número de estaciones. El mismo incremento puede conseguir manteniendo fijo el número de estaciones y aumentando la carga ofrecida por cada una de ellas. No obstante, como veremos, el rendimiento de la red será diferente para ambos casos.

Un factor que no ha sido incluido en la lista anterior: el porcentaje de error del canal. Un error en la transmisión de un *Frame* supone la necesidad de retransmitirlo. Dado que los porcentajes de error en las redes locales son muy bajos, este no resulta un factor significativo.

RENDIMIENTO DE LAS LANs.

Se ha trabajado mucho en el análisis del rendimiento de varios protocolos de LANs para Bus/Arbol y Anillo. En esta sección resumiremos los resultados de estos trabajos para los protocolos vistos en el capítulo 5, es decir aquellos más comunes en las LANs.

Límite sobre el rendimiento:

En esta sección nos centraremos en la obtención de una técnica sencilla para determinar límites sobre el rendimiento de una LAN. Aunque se han hecho muchos esfuerzos para desarrollar modelos de simulación y de analítica detallada del rendimiento de varios protocolos LAN, buena parte de este trabajo resulta dudoso debido al carácter restrictivo de las suposiciones hechas. Es más, incluso suponiendo que los modelos fuesen válidos, éstos proporcionan un nivel de resolución que no necesita el diseñador de redes locales.

En cualquier LAN ó HSLN, hay tres regiones, de funcionamiento basadas en la magnitud de la carga ofrecida:

- * Una región de bajo retardo a través de la red, donde la capacidad es más que adecuada para manejar la carga ofrecida.

- * Una región de retardo alto, donde la red llega a constituir un cuello de botella. En esta región se gasta más tiempo controlando el acceso a la red que en la transmisión de datos actual, en comparación con la región de retardo bajo.
- * Una región de retardo ilimitado, donde la carga ofrecida excede la capacidad total del sistema.

Esta última región está claramente identificada. Por ejemplo, consideremos la siguiente red:

- * Capacidad = 1 Mbps.
- * Número de estaciones = 1000.
- * Tamaño del *Frame* = 1000 bits.

Sí cada estación genera datos a una velocidad superior a un *Frame* por segundo, entonces la carga total ofrecida supera 1 Mbps. El retardo en cada estación subiría y subiría sin límite.

La tercera región es, obviamente, una región no deseada. Pero casi siempre, el diseñador va a querer evitar también la segunda región. Esta segunda región implica un uso ineficiente de la red. Es más, sí se produce un aumento repentino de datos en esta región aumentaría el ya de por sí alto retardo. En la primera región, la red no ejerce como cuello de botella y, como veremos en la sección 9.4, normalmente aporta una pequeña cantidad al retardo punta-a-punta.

La cuestión crucial es: basándonos en las características de la red y de la carga esperada, ¿En qué

región trabajará la red?. Dado que la tercera región esta claramente definida y rechazada; es la frontera entre las dos primeras regiones la que ha de ser completada. Si la red opera por debajo de esa división, no causaría un efecto de cuello de botella en la comunicación. Si funciona por encima de la misma, habrían razones para preocuparse e incluso rediseñar la red. Ahora bien, la cuestión es: ¿Con cuanta precisión necesitamos nosotros conocer esta división?. Por un lado la carga en la red va a variar con el tiempo, luego sólo podemos estimarla. Por otro lado, dado que es poco probable que esta estimación sea precisa, no es necesario saber exactamente donde está esa frontera. Si se puede desarrollar una buena aproximación de la localización de la frontera, entonces la red puede ser dimensionada de modo que la carga estimada esté bien por debajo de ésta. En el ejemplo descrito, la carga estimada (a 1 Frame por segundo) es de 1 Mbps. Si la capacidad de la LAN es tal que la frontera está aproximadamente en los 4 Mbps, entonces el diseñador puede estar razonablemente seguro de que la red no será un cuello de botella.

Teniendo todo esto en cuenta, vamos a ver una técnica de estimación de límites de rendimiento, basada en el enfoque adoptado por el Comité IEEE 802. De entrada nos vamos a olvidar del protocolo de control de acceso al medio y a centrarnos en el desarrollo de límites para la capacidad de tratamiento y para el retardo, en función del

número de estaciones activas. Para ello hablaremos de:

- * T_{idle} = Tiempo medio que una estación esta desocupada entre los intentos de transmisión: la estación no tiene mensajes esperando ser transmitidos.
- * T_{msg} = Tiempo requerido para transmitir un mensaje una vez se accede al medio.
- * T_{delay} = Retardo medio desde que una estación tiene un mensaje que transmitir hasta que se completa la transmisión; incluyendo tiempo de transmisión y de espera en cola.
- * $THRU$ = Capacidad de tratamiento media de mensajes por segundo en la red.

Suponemos que hay N estaciones activas, cada una de ellas con los mismos requerimientos de generación de carga. Para encontrar una cota superior en la capacidad de tratamiento total, vamos a considerar el caso ideal de que no existan tiempos de espera en cola. Cada estación transmite cuando está preparada. Luego cada estación alterna el estar desocupada con la transmisión con una capacidad de tratamiento de $1 / (T_{idle} + T_{msg})$. La capacidad de tratamiento máxima sería la suma de todas las capacidades de tratamiento de las N estaciones:

$$THRU \leq \frac{N}{T_{idle} + T_{msg}} \quad (9.2)$$

Esta cota superior aumenta al aumentar N , pero es razonable hasta el punto de capacidad bruta de la red, la cual se puede expresar como:

$$\text{THRU} \leq \frac{1}{T_{\text{msg}}} \quad (9.3)$$

El punto de ruptura entre estas dos cotas se produce para:

$$\frac{N}{T_{\text{idle}} + T_{\text{msg}}} = \frac{1}{T_{\text{msg}}}$$

$$N = \frac{T_{\text{idle}} + T_{\text{msg}}}{T_{\text{msg}}} \quad (9.4)$$

Este punto de ruptura define dos regiones de funcionamiento. Con el número de estaciones por debajo de ese punto, el sistema no está generando suficiente carga como para utilizar toda la capacidad del sistema. Por encima de ese punto la red está saturada: Está utilizada al completo y no es capaz de satisfacer las demandas de las estaciones enganchadas.

Para ver la verosimilitud de ese punto de ruptura, vamos a considerar que la capacidad de la red es $1/T_{\text{msg}}$. Sí, por ejemplo, tarda 1 μs en transmitir un mensaje, la velocidad es de 10^6 mensajes por segundo. La cantidad de tráfico generado por N estaciones es $N/(T_{\text{idle}} + T_{\text{msg}})$. Sí el tráfico supera la capacidad de la red, los mensajes

se acumulan y el retardo aumenta. Obsérvese que el tráfico aumenta tanto si aumenta N como si aumenta la velocidad a la que transmiten mensajes las estaciones (disminución de T_{idle}).

Estas consideraciones nos permiten situar una cota inferior en el retardo; obviamente:

$$T_{delay} \geq T_{msg} \quad (9.5)$$

Consideremos ahora que la relación:

$$THRU = \frac{N}{T_{idle} + T_{delay}} \quad (9.6)$$

se cumple para cualquier carga; dado que $1/(T_{idle} + T_{delay})$ es la capacidad de tratamiento de cada estación. Combinando (9.3) y (9.6) tenemos:

$$T_{delay} \geq N T_{msg} - T_{idle}$$

El cálculo del punto de ruptura, combinando la ecuación anterior con la (9.5) da el mismo resultado que antes (ver figura 9.6). Tener en cuenta que estas cotas son asíntotas de las verdaderas curvas de retardo y de capacidad de tratamiento. El punto de ruptura delimita dos regiones. Por debajo del punto de ruptura, la capacidad está infrautilizada y el retardo es bajo. Por encima de éste, la capacidad se satura y el retardo se dispara.

Las cotas en la otra parte son fáciles de encontrar. El retardo será máximo si todas las N estaciones tienen un mensaje que transmitir simultáneamente:

$$T_{\text{delay}} \leq N T_{\text{msg}}$$

Combinando ésta ecuación con la (9.6) obtenemos:

$$\text{THRU} \geq \frac{N}{T_{\text{idle}} + N T_{\text{msg}}}$$

Estas cotas nos dan una idea aproximada del comportamiento de un sistema.

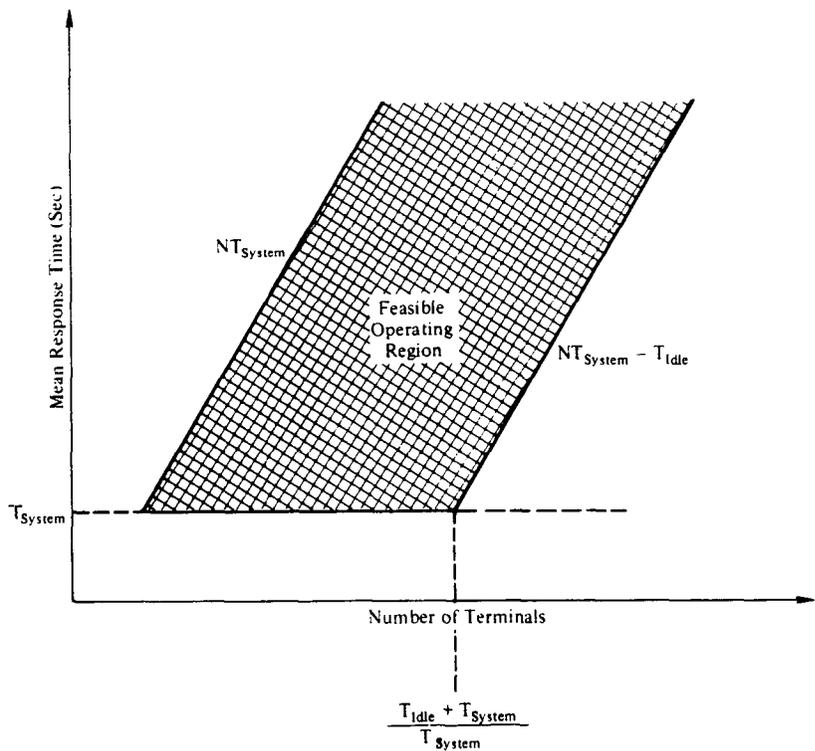


FIGURE 9-6. Feasible operating region, zero-overhead system

Para dejar claro el uso de estas ecuaciones, veamos dos ejemplos. Primero, consideremos una estación de

trabajo enganchada a una red local de 1Mbps. La estación general tres mensajes por minuto (por término medio), con una media de 500 bits por mensaje. Si el tiempo de transmisión es de 500 μ s, el tiempo medio que está desocupada es de 20 s. El punto de ruptura en el número de estaciones es aproximadamente:

$$N = \frac{20}{500 \times 10^{-6}} = 40.000 \text{ estaciones}$$

Si el número de estaciones es mucho menor a 40.000, digamos 1.000, la congestión no sería un problema. Si fuese mucho más, digamos 100.000, la congestión podría ser un problema.

Segundo, supongamos un conjunto de estaciones que generen paquetes PCM digitalizados de voz sobre una red local a 10 Mbps. Los datos se generan a una velocidad de 64 Kbps. Para 0.1 paquetes, tenemos un tiempo de transmisión por paquete de 640 μ s. Luego:

$$N = \frac{0.1}{640 \times 10^{-6}} = 156 \text{ estaciones}$$

Normalmente, no todas las estaciones (teléfonos) estarán activas simultáneamente; quizás una estimación razonable sea pensar en un cuarto, así que el punto de ruptura estaría alrededor de 600 (156x4) estaciones.

En ambos ejemplos hemos llegado rápidamente a un dimensionamiento de primer orden del sistema sin tener en

cuenta el protocolo. Todo lo que se necesita es la carga generada por estación y la capacidad de la red.

Los capítulos anteriores son para sistemas sin sobrecarga (bits). Una forma de tener en cuenta los bits de sobrecarga es reemplazando T_{msg} por T_{system} , donde este último incluye una estimación de los bits de sobrecarga por paquete. Esto se hizo en la figura 9.6.

Sí tenemos en cuenta el protocolo podemos hacer una aproximación más precisa del rendimiento del sistema. Primero vamos a estudiar el protocolo de paso de *Token*; este protocolo presenta las siguientes características:

- * Las estaciones tienen la oportunidad de transmitir en una secuencia cíclica fija.
- * Cada vez, una estación puede transmitir un mensaje.
- * Los *Frames* pueden ser de longitud fija ó variable.
- * No se permite el derecho de prioridad.

Para realizar este estudio necesitamos definir nuevos términos:

- * $R(K)$ = Capacidad de tratamiento medio (velocidad:mensajes/segundo) de la estación K .
- * T_{over} = Sobrecarga total (en segundos) en un ciclo de las N estaciones.
- * C = Duración (en segundos) de un ciclo.
- * $UTIL(K)$ = Utilización de la red debido a la estación K .

Para empezar, supongamos que cada estación tiene siempre un mensaje para transmitir; el sistema no está nunca desocupado. La fracción de tiempo que la red está ocupada tratando las peticiones de la estación K es :

$$UTIL(K) = R(K) T_{msg}(K)$$

Para hacer frente al trabajo, al sistema no se le puede presentar una carga superior a su capacidad:

$$\sum_{K=1}^N UTIL(K) = \sum_{K=1}^N R(K) T_{msg}(K) \leq 1$$

Consideremos ahora la sobrecarga en el sistema, que es el tiempo necesario para pasar el *Token* y realizar otras funciones de mantenimiento en un ciclo; un ciclo es:

$$C = T_{over} + \sum_{K=1}^N T_{msg}(K)$$

De aquí podemos deducir que:

$$R(K) = \frac{1}{C} = \frac{1}{T_{over} + \sum_{K=1}^N T_{msg}(K)}$$

Sí suponemos ahora que el medio está siempre ocupado y que algunas estaciones pueden estar desocupadas, este razonamiento nos induce a pensar en la conveniencia de cotas en la capacidad de tratamiento y en el retardo. Ya que supusimos que la red no estaba nunca desocupada, el tiempo que el sistema consume en la transmisión y en la

sobrecarga debe sumar 1:

$$\frac{T_{over}}{C} + \sum_{K=1}^N R(K) T_{msg}(K) = 1$$

Luego:

$$C = \frac{T_{over}}{1 - \sum_{K=1}^N R(K) T_{msg}(K)}$$

Obsérvese que la duración de un ciclo es proporcional a la sobrecarga; doblando el tiempo medio de sobrecarga para una carga fija, se doblará la duración del ciclo.

Una vez conocido C, podemos fijar una cota superior en la capacidad de tratamiento de cualquier fuente:

$$R(J) \leq \frac{1}{C} = \frac{1 - \sum_{K=1}^N R(K) T_{msg}(K)}{T_{over}} \quad (9.7)$$

Sí consideramos que todas las fuentes son idénticas: $R(K) = R$, $T_{msg}(K) = T_{msg}$. La ecuación (9.7) se reduce a:

$$R \leq \frac{1 - N R T_{msg}}{T_{over}}$$

Dividiendo por R:

$$R \leq \frac{1}{T_{over} + N T_{msg}}$$

Pero por definición, $R = 1 / (T_{delay} + T_{idle})$, luego:

$$T_{delay} = \frac{1}{R} - T_{idle}.$$

$$T_{delay} \geq T_{over} + N T_{msg} - T_{idle}$$

En la práctica, T_{over} puede consistir en una cierta cantidad de tiempo fijo por ciclo C_o , más un cierto tiempo C_i por cada estación que recibe el *Token*. C_o y C_i son diferentes en *Token Ring* y *Token Bus*:

$$T_{delay} \geq C_o + N(T_{msg} + C_i) - T_{idle}$$

Teniendo en cuenta la desigualdad (9.5), el punto de ruptura sería para:

$$N = \frac{T_{msg} + T_{idle} - C_o}{T_{msg} + C_i} \quad (9.8)$$

En la figura 9.7 se representa el retardo en función del número de estaciones.

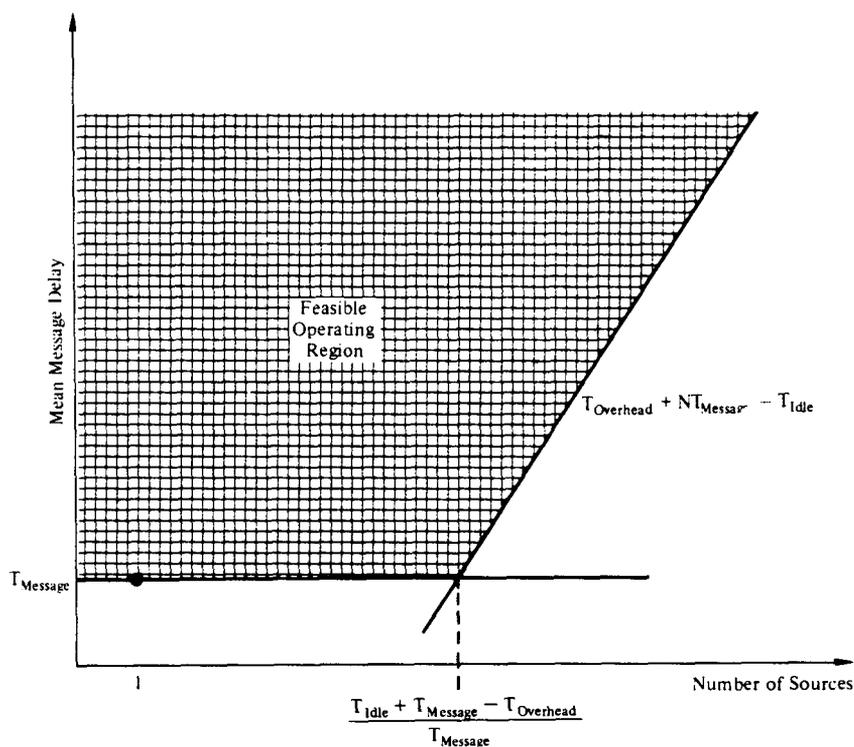


FIGURE 9-7. Bounds on token-passing performance

Un análisis similar se puede llevar a cabo para CSMA/CD. La figura 9.8 es una comparación entre los sistemas de Token y el CSMA/CD. las posiciones de las curvas dependen de las suposiciones específicas a cerca de la sobrecarga y, en el caso de CSMA/CD, del valor de a. Pero las posiciones relativas son correctas: bajo condiciones de poca carga el CSMA/CD tiene un retardo menor. pero el protocolo se viene más rápidamente al aumentar ésta.

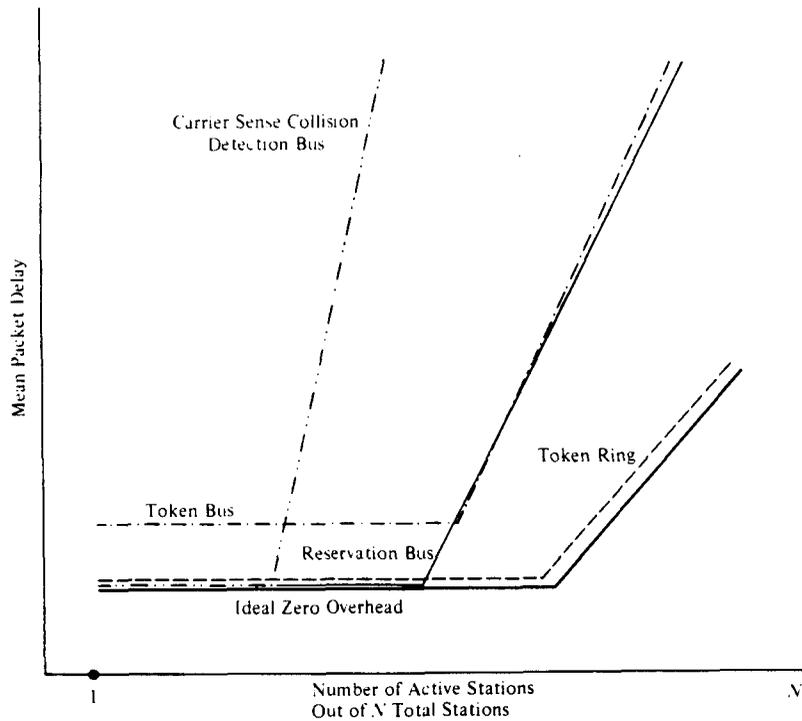


FIGURE 9-8. Comparative bounds on LAN protocols

Comparación de rendimiento en CSMA/CD y TOKEN:

Vamos a suponer una red local con N estaciones activas. Nuestro propósito es estimar la capacidad de tratamiento máxima factible en la LAN. para ello vamos a suponer que cada estación está siempre preparada para transmitir un *Frame*.

Primero veamos un **Token Ring**. El tiempo en el Anillo va a alternarse entre la transmisión de *Frames* de datos y la circulación del *Token*. Vamos a considerar un ciclo a un *Frame* de datos seguido de un *Token*, y definimos:

- * C = Tiempo medio de un ciclo.
- * DF = Tiempo medio de transmisión de un *Frame* de datos.
- * TF = Tiempo medio para pasar un *Token*.

La velocidad media del ciclo (ritmo) es:

$$1/C = 1/(DF+TF). \text{ Luego}$$

$$S = \frac{DF}{DF + TF} \quad (9.9)$$

Esto es, la capacidad de tratamiento normalizada a la capacidad del sistema; ó sea la fracción de tiempo que se emplea en transmitir datos.

Volviendo a la figura 9.3; el tiempo es normalizado tal que el tiempo de transmisión del *Frame* sea 1 y el tiempo de propagación sea a . Para $a < 1$, una estación que transmita un *Frame* en T_0 , recibe el comienzo de su *Frame* en $T_0 + a$ y termina de transmitir en $T_0 + 1$. La estación emite entonces un *Token* que tarda un tiempo a/N en llegar a la siguiente estación (suponiendo todas las estaciones equidistantes entre sí). Por lo tanto un ciclo dura $1+a/N$ y el tiempo de transmisión es 1. Así $S = 1/(1 + a/N)$.

Para $a > 1$ el razonamiento es ligeramente diferente. Una estación que transmite en T_0 , termina la transmisión en $T_0 + 1$, y recibe la cabecera de su *Frame* en $T_0 + a$. En ese punto, es libre de emitir un *Token*, que tarda a/N en

llegar a la siguiente estación.

La duración del ciclo es por tanto $a + a/N$ y $S=1/[a(1+1/n)]$. Resumiendo:

$$\text{Token: } S = \begin{cases} \frac{1}{1 + a / N} & \text{sí } a < 1 \\ \frac{1}{a (1 + 1/N)} & \text{sí } a > 1 \end{cases}$$

(9.10)

Este razonamiento es válido también para el *Token Bus*, donde podemos suponer que la ordenación lógica es la misma que la física y el tiempo de pase del *Token* es a/N .

Para **CSMA/CD**, vamos a considerar la división del medio en particiones (*Slot*) cuya longitud es del doble del retardo de propagación punto-a-punto. La duración del *Slot* es el tiempo máximo desde el comienzo de la transmisión, necesario para detectar una colisión. Supongamos otra vez que tenemos N estaciones activas, generando todas la misma carga. Obviamente, sí cada estación tiene siempre un paquete que transmitir, no habrán sino colisiones en la línea. Por tanto, vamos a suponer que cada estación se priva de transmitir durante un *Slot* disponible con probabilidad p .

El tiempo en el medio está constituido por dos intervalos. Primero, un intervalo de transmisión que dura $1/2 a$ *Slots*. Segundo, un intervalo de contención, que es

una secuencia de particiones con una colisión ó sin transmisión. La capacidad de tratamiento es la proporción de tiempo empleada en los intervalos de transmisión [razonamiento similar al realizado para la ecuación(9.1)].

Para calcular la longitud media de un intervalo de contención, empezamos por hallar A, que es la probabilidad que exactamente una estación intente una transmisión en una partición y por lo tanto consiga el medio. Esta será la probabilidad binomial de que cualquier estación intente transmitir y las otras no:

$$A = \binom{N}{1} p^1 (1 - p)^{N-1} = Np (1-p)^{N-1}$$

Esta función es máxima cuando $p = 1/N$:

$$A = \left(1 - \frac{1}{N} \right)^{N-1}$$

Nosotros queremos calcular la capacidad máxima de tratamiento del medio, por ello nos interesa el máximo de A. Esto se consigue si maximizamos la probabilidad de la toma con éxito del medio. Esto nos lleva a enunciar una regla ineludible: Durante períodos de gran uso, una estación debería retener su carga ofrecida $1/N$ (esto presupone que cada estación conoce el valor de N). Por otro lado, durante períodos de poco uso, no se puede obtener una utilización máxima dado que G es muy bajo.

Ahora ya podemos estimar la longitud media de un intervalo de contención W , en particiones:

$$E [w] = \sum_{i=1}^{\infty} i Pr = \sum_{i=1}^{\infty} i(1 - A)^i A$$

donde i son las particiones sin transmisión ó con colisión seguida de una transmisión.

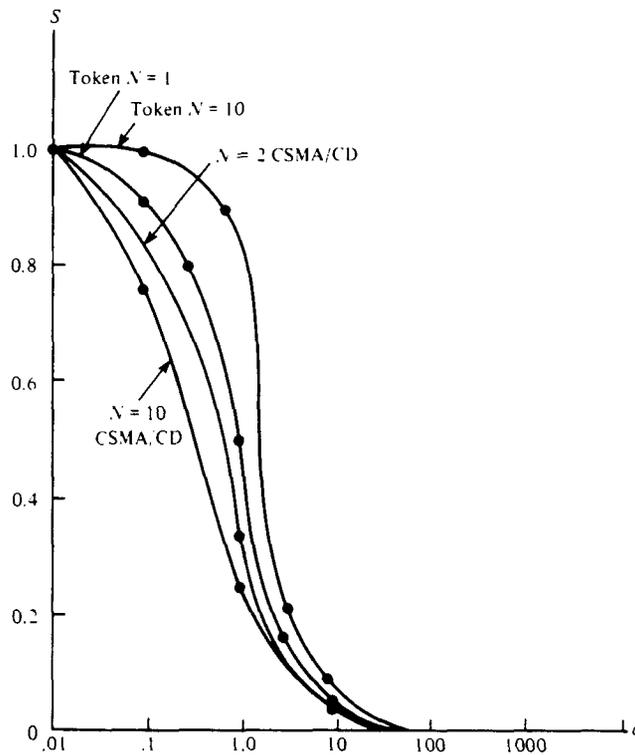


FIGURE 9-9. Throughput as a function of a for token-passing and CSMA/CD

La suma converge hacia :

$$E [w] = \frac{1 - A}{A}$$

La utilización máxima es la longitud de un intervalo de transmisión como una porción de un ciclo de dos intervalos.

CSMA/CD: (9.11)

$$S = \frac{1/2a}{1/2a + \frac{1-A}{A}} = \frac{1}{1/2a + \frac{1-A}{A}}$$

La figura 9.9 muestra la capacidad de tratamiento normalizada en función de a para varios valores de N , tanto para *Token* como para CSMA/CD. Para ambos protocolos la capacidad de tratamiento disminuye al aumentar a . Las diferencias más sustanciales entre ambos protocolos se reflejan en la figura 9.10, que nos muestra la capacidad de tratamiento en función de N . El rendimiento de los sistemas *Token* mejora en función del aumento de N , debido a que se tarda menos tiempo en pasar el *Token*. A la inversa, el rendimiento del CSMA/CD disminuye al aumentar N debido al aumento de la posibilidad de colisiones.

Siguiendo con nuestro estudio, es relativamente sencillo deducir una expresión para el retardo de los sistemas *Token*. Una vez una estación (estación 1) transmite, debe esperar a que sucedan los siguientes acontecimientos antes de que pueda transmitir otra vez:

- * Estación 1 transmite un *Token* a la estación 2.
- * Estación 2 transmite un *Frame* de datos.

- * Estación 2 transmite un *Token* a la estación 3.
- .
- .
- .
- .
- * Estación N-1 transmite un *Token* a la estación N.
- * Estación N transmite un *Frame* de datos.
- * Estación N transmite un *Token* a la estación 1.

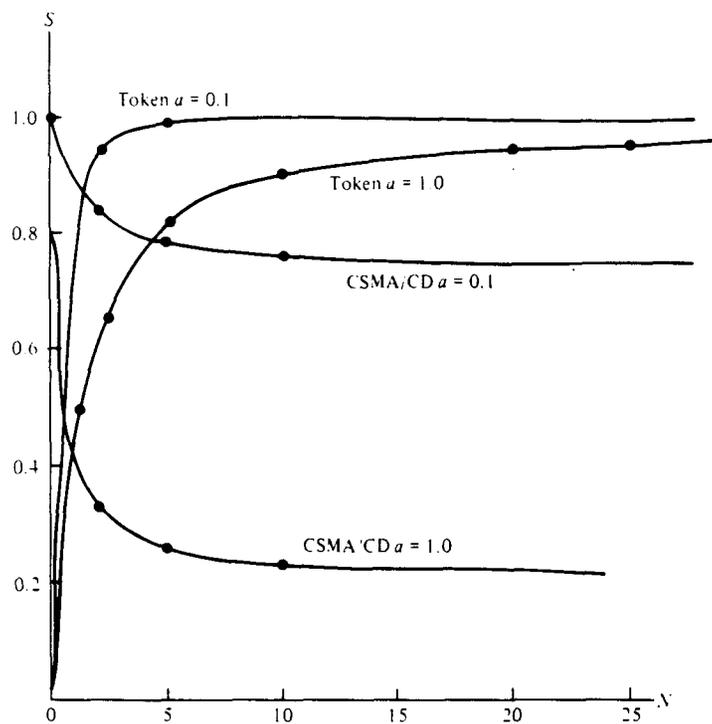


FIGURE 9-10. Throughput as a function of N for token-passing and CSMA/CD

Luego el retardo está formado por (N-1) ciclos más a/N, que es el tiempo de pase del *Token*. Tenemos pues:

$$\text{Token: } D = \begin{cases} N + a + 1 & \text{sí } a < 1 \\ aN & \text{sí } a > 1 \end{cases}$$

El retardo aumenta linealmente con la carga, y para un número fijado de estaciones, el retardo es constante y finito incluso si todas las estaciones tienen siempre algo que enviar. El retardo para CSMA/CD es más difícil de expresar y depende de la naturaleza exacta del protocolo. En general, podemos decir que el retardo aumenta sin límite a medida que el sistema se va saturando. Al aumentar N hay más colisiones y mayores intervalos de contención. Cada *Frame* debe realizar más intentos para lograr una transmisión exitosa.

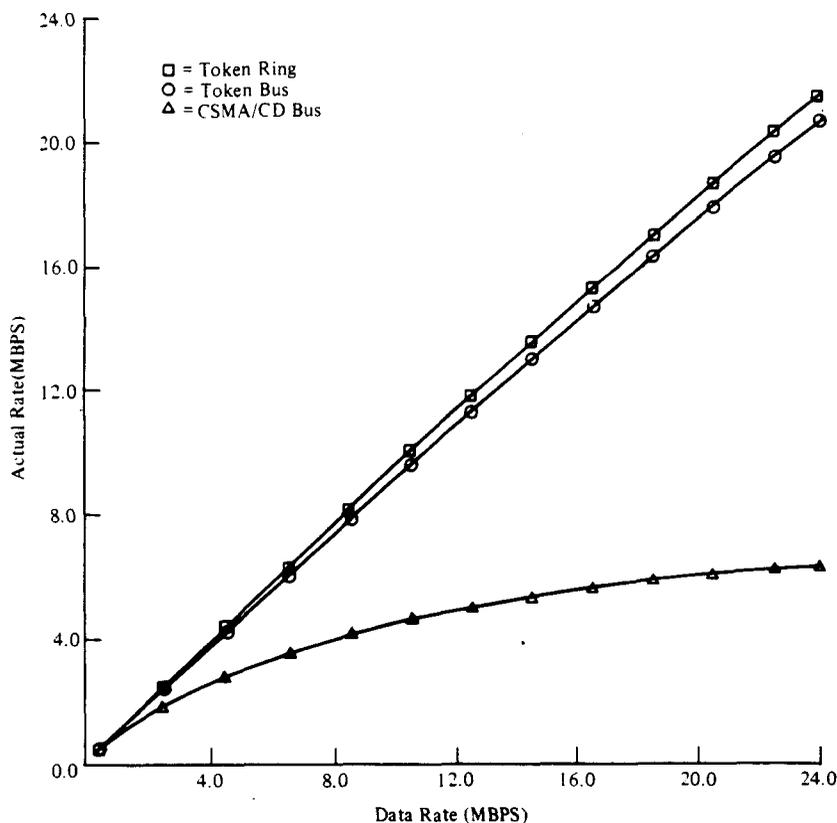


FIGURE 9-11a. Maximum potential data rate for LAN protocols: 2000 bits per packet; 1 station active out of 100 stations total

Vamos ahora a reflejar los resultados del análisis realizado por el Comité 802 de IEEE. El análisis se basa no sólo en la consideración de valores medios sino también según los momentos de retardo y la longitud del mensaje. Se usan dos tipos de estadísticas de la llegada de mensajes. En la primera, sólo 1 estación de 100 tiene mensajes que transmitir y está siempre lista para transmitir. En ese caso podemos suponer que la red no llegará a ser un cuello de botella, sino que podrá satisfacer fácilmente a la estación.

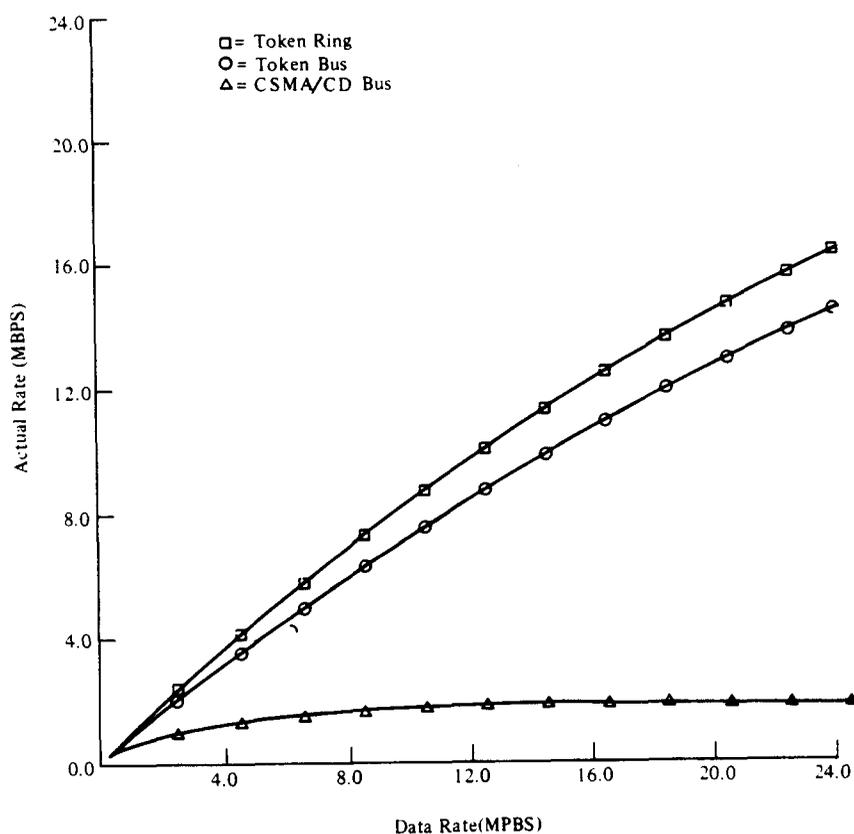


FIGURE 9-11b. 500 bits per packet; 100 stations active out of 100 stations total

En el segundo caso, tenemos 100 estaciones de 100 que siempre tienen mensajes para transmitir. Esto representa un extremo de congestión y podemos suponer que se producirá un efecto de cuello de botella.

Los resultados se pueden observar en las figuras 9.11a y 9.11b respectivamente. En ellas se observa la velocidad actual en función de la velocidad de transmisión en un Bus de 2 Km. Observar que la abscisa no tenemos la carga ofrecida si no la capacidad actual del medio. Tanto las cien estaciones como la única estación proporcionan suficiente entrada para utilizar completamente la red. Por tanto, estos gráficos son una medida de la utilización potencial máxima. En ellos aparecen curvas para tres sistemas: **Token Ring** con 1 bit de tiempo de espera por estación, **Token Bus**, y **CSMA/CD**. El análisis de estos gráficos arrojan las siguientes conclusiones:

- * Para los parámetros dados, cuanto menor sea la longitud media del *Frame*, mayor será la diferencia en el porcentaje medio máximo de capacidad de tratamiento entre el **Token Ring** y el **CSMA/CD**. Esto refleja la gran dependencia del **CSMA/CD** de a .
- * El **Token Ring** es el menos sensible a la carga del trabajo.
- * El **CSMA/CD** ofrece el menor retardo bajo condiciones de baja carga, mientras resulta el mas sensible a la carga de trabajo en

condiciones de mucha carga.

Obsérvese que incluso en el caso de tener sólo una estación transmitiendo, el Token Bus es sensiblemente menos eficiente que los otros dos protocolos. Esto es debido a que se ha supuesto que el retardo de propagación es mayor que en el Token Ring, y que el retardo en un procesamiento del Token es mayor que para el Token Ring.

Otro fenómeno digno de comentario (figura 9.11b) es que para el CSMA/CD bajo estas condiciones, la capacidad de tratamiento máxima efectiva a 5 Mbps es sólo de 1.25 Mbps. Sí la carga esperada es de 0.75 Mbps, esta configuración es perfectamente adecuada. Sí, por el contrario la carga esperada es de 2 Mbps, ni aumentando la velocidad de transmisión de la red a 10 Mbps ó incluso 20 Mbps no se podría acomodar toda (ésto es debido a la pendiente de la curva).

Como todos los demás resultados que hemos dado en este capítulo, estos dependen de la naturaleza de las suposiciones hechas, y no reflejan con exactitud la naturaleza de la carga del mundo real. No obstante, nos muestra la naturaleza inestable del CSMA/CD y de la capacidad del Token Ring y Token Bus para encarar con buen rendimiento las condiciones de sobrecarga.

Rendimiento comparativo de los protocolos en Anillos:

Es mucho más complicado hacer una comparación de rendimientos para los tres protocolos principales en

Anillo que para Bus y Token Ring. El resultado de la comparación va a depender de una serie de parámetros únicos en cada uno de los protocolos. Por ejemplo:

- * **Token Ring:** Tamaño del *Token*, tiempo de procesamiento del *Token*.
- * **Slotted Ring:** Tamaño de partición (Slot), bit de sobrecarga por partición.
- * **Inserción de registros:** Tamaño de registro.

Por ello es difícil hacer una comparación, e incluso existe una serie de estudios para cada una de las técnicas; Pocos hacen comparaciones por pares y casi ninguno lo hace a tres bandas. Por ello, en esta sección vamos a resumir los estudios más comparativos.

El trabajo más sistemático llevado a cabo hasta la fecha ha sido desarrollado por dos grupos diferentes: Hammond and O'Reilly, y Lin y Asociados. Nos centraremos en los resultados del primero; los del segundo serán virtualmente idénticos a éstos.

El análisis compara **Token Ring** y **Slotted Ring** e inserción de registro, variando a los siguientes parámetros:

- * **Número de estaciones:** 10, 100.
- * **Valor de a:** 1.0, 0.1.
- * **Relación entre el tamaño de encabezamiento y el tamaño del dato en un Slotted Ring:** 1, 0.

En la figura 9.12 se resumen los resultados. Estos muestran que la inserción de registro es la mejor para un

pequeño número de estaciones ó bajo cargas pequeñas. El Token Ring parece tener el mejor rendimiento bajo una diversidad de condiciones.

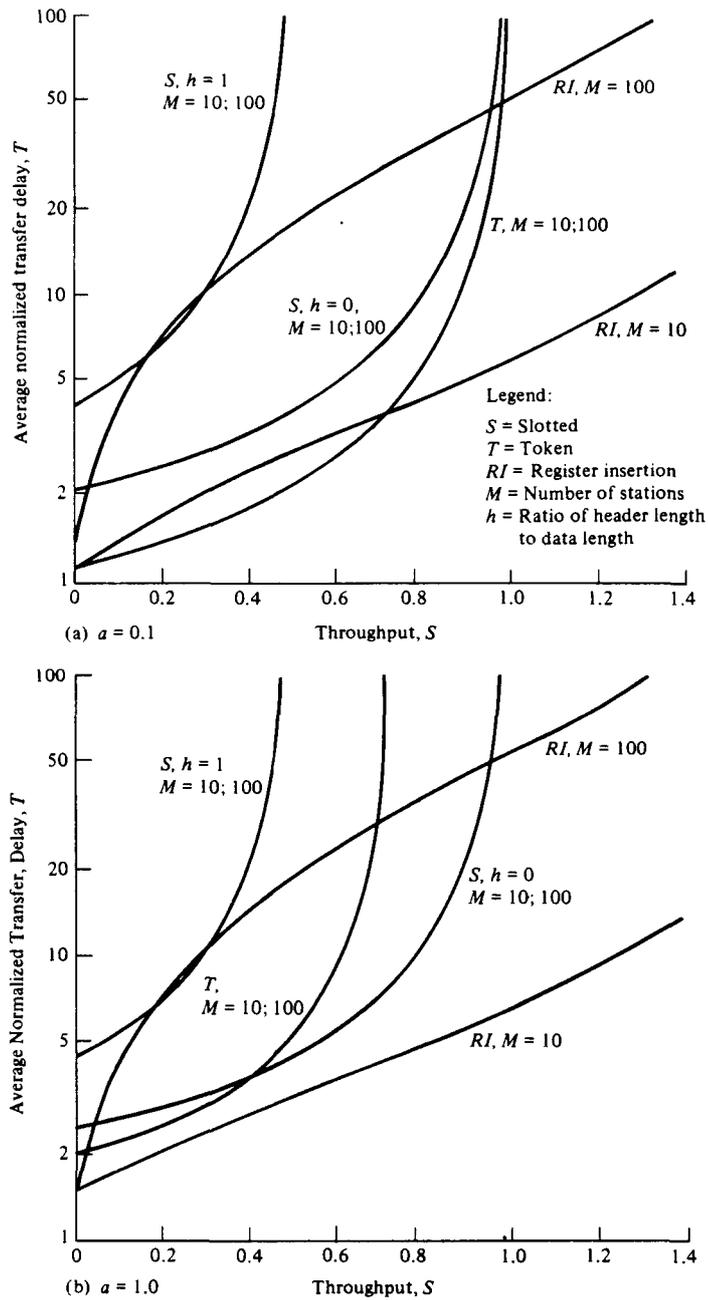


FIGURE 9-12. Delay for various ring protocols

Nótese incluso que la inserción de registro parece ser capaz de tratar cargas mayores de 0.1; ésto es debido a que el protocolo permite la circulación de varios Frames.

W. Bux realizó un estudio comparativo de Token Ring, Slotted Ring y CSMA/CD, publicado en octubre de 1.981. En él se llega a una serie de conclusiones importantes. Primero, el rendimiento retardo-capacidad de tratamiento del Token Ring frente al CSMA/CD configura lo que hemos dicho anteriormente. Esto es, que el Token Ring sufre más retardo que el CSMA/CD con pequeña carga pero menos retardo y capacidad de tratamiento más estable para cargas grandes. es más, el Token Ring tiene características de retardo superiores al Slotted Ring. El rendimiento más pobre del Slotted Ring parece tener dos causas: (1) La sobrecarga en las pequeñas particiones en un Slotted Ring es muy alta, y (2) el tiempo necesario para pasar las particiones vacías a lo largo del Anillo para garantizar un ancho de banda imparcial es alto. Bux también apuntó dos características positivas del Slotted Ring: (1) El retardo esperado para un mensaje es proporcional a su tamaño (por lo que los paquetes más cortos reciben mejor tratamiento que los mayores), y (2) el retardo global medio es independiente de la distribución de la longitud de los paquetes.

En otro estudio realizado en 1.982 por W. Cheng, se señala que el rendimiento de un Anillo aumenta con el

número de particiones en él al menos hasta igualar el número de nodos. No obstante, para las LANs, en donde típicamente $a < 1$, un Anillo con muchas particiones sólo se consigue teniendo retardos artificiales ó particiones muy pequeñas. Con particiones muy pequeñas, el encabezamiento sería proporcionalmente mayor.

Es difícil llegar a una conclusión tajante con estos estudios. El Slotted Ring parece ser el menos deseable en un gran rango de valores de parámetros, a causa de la considerable carga asociada a cada pequeño paquete. Por ejemplo, el Cambridge Ring, que es el Anillo más extendido comercialmente en Europa usa particiones de 37 bits de los cuales sólo 16 son de datos. Los diseñadores de este Anillo empezaron a desarrollar un Anillo por inserción de registro, pero lo rechazaron frente a la opción del Slotted Ring por una razón: un fallo en un registro de desplazamiento puede causar la ruptura del Anillo externo.

Entre Token Ring e inserción de registro la evidencia sugiere que al menos para algunos juegos de valores, la inserción de registro proporciona un rendimiento de retardo superior.

La ventaja principal de la inserción de registro es la alta utilización potencial que puede alcanzar. En contraste con el Token Ring, pueden haber varias estaciones transmitiendo a la vez. Es más, una estación puede transmitir tan pronto como se abra un espacio en el Anillo; no necesita esperar por un Token. Por otro lado,

el tiempo de propagación a través del Anillo no es constante, sino que va a depender de la cantidad de tráfico.

Por último, decir que para pequeñas cargas, la inserción de registro funciona más eficientemente, teniendo un retardo ligeramente menor. No obstante, ambos sistemas operan adecuadamente. Nuestro interés principal es cuando hay una gran carga. Una LAN típica tendrá $a < 1$, a menudo $a \ll 1$ de modo que una estación que está transmitiendo en un **Token Ring** añadirá un *Token* al final de su paquete. Bajo una gran carga, una estación cercana podrá ser capaz de utilizar el *Token*. Por ello se consigue un 100% de utilización, lo cual no supone una ventaja particular sobre la inserción de registro.

9.3

RENDIMIENTO DE LAS HSLN.

Dado el poco estudio que se ha realizado sobre el protocolo LDDI, en esta sección nos vamos a centrar en los resultados de la modelización de un protocolo similar: El **HIPERchannel**. téngase en cuenta que, en contraste con el LDDI, el protocolo **HIPERchannel** tiene prioridades incorporadas. Esto es; la estación con la posición más cercana en el tiempo siempre tiene la primera oportunidad de transmitir, lo que le dá mayor prioridad.

Posiblemente el grupo que más ha trabajado sobre este tema sea el de Franta y Asociados en la Universidad de Minnesota. Este grupo desarrolló un modelo que representaba un sistema HIPERchannel como un sistema de espera de fuentes finito, tal que una vez una petición de transmisión ha sido generada por un NIU, no se genera otra petición de ese NIU hasta que se realiza la primera petición. Luego desarrollaron un modelo de simulación y, finalmente obtuvieron una serie de medidas de rendimiento.

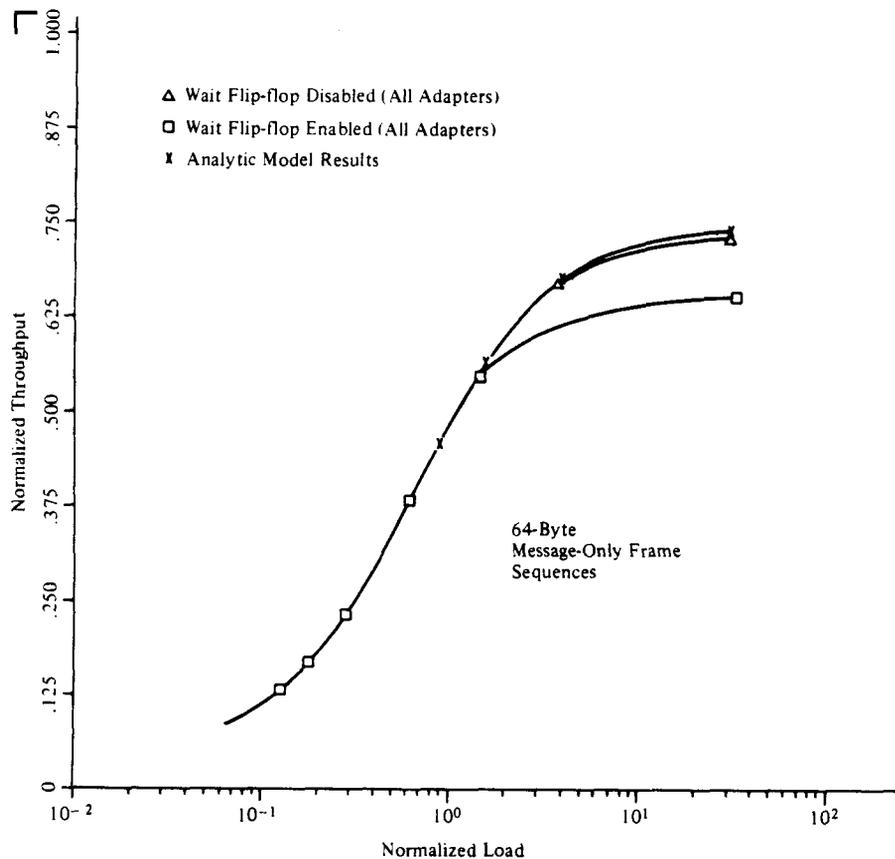


FIGURE 9-13. Performance of HIPERchannel

En la figura 9.13 se muestran los resultados para un sistema de 6 nodos y 1.000 pies. Estos resultados son para paquetes de 4 Kbytes, así α es aproximadamente 0.002. En la figura se observa que el protocolo es aceptable en el sentido de que la capacidad de tratamiento no se deteriora al aumentar la carga.

La figura incluye una curva para la inhibición del flip-flop de espera, el cual actúa del mismo modo que la bandera (Flag) de espera en el LDDI. Sorprendentemente, el rendimiento se degrada con el uso del flip-flop de espera. La razón es que el uso de este mecanismo incrementa la frecuencia con la cual aparecen intervalos de contención en el HIPERchannel. Por lo tanto hay más colisiones y un rendimiento más pobre. Dado que en el protocolo LDDI no hay intervalos de contención, el uso de la bandera de espera tendrá un efecto menor sobre el rendimiento.

Por otro lado hay que reseñar los estudios realizados en los laboratorios Lawrence Livermore sobre la modificación del HIPERchannel. El grupo de Livermore extendió sus estudios hasta incluir la modelización de la capa de enlace, llegando a la conclusión de que, como el CSMA/CD, el rendimiento del HIPERchannel se degrada bajo cargas altas. La causa de este fenómeno es que, la capa 2, un NIU (en el HIPERchannel) impide la entrada de recepciones mientras intenta establecer una conexión para transmitir. Esto nos puede llevar a un estado de "Deadlock" (interbloqueo), y a la degeneración de la

capacidad de tratamiento.

Finalmente señalaremos que unos estudios realizados en MITRE, revelaron que la velocidad de transmisión de datos que se podía obtener era de 6.18 Mbps. Esto enfatiza la importancia de no igualar la capacidad de tratamiento a la velocidad bruta de transmisión.

Todos estos resultados son aplicables al protocolo LDDI, aunque podemos esperar éste lo haga un poco mejor debido a la ausencia en él de colisiones.

9.4

RENDIMIENTO DE EXTREMO A EXTREMO.

Hasta ahora hemos estudiado algunas técnicas de estimación del rendimiento, pero en lo que se refiere al retardo y a la capacidad de tratamiento. Esto, evidentemente, no es del interés del usuario. Lo que a éste le interesa es el rendimiento extremo-a-extremo ó punta-a-punta (end-to-end). Ejemplos:

- * Dos ordenadores principales (Host) intercambian ficheros grandes. ¿Cuál es la capacidad de tratamiento que se da en la transferencia de ficheros?.
- * Un usuario de un terminal está preguntando a una Base de Datos de un ordenador principal. ¿Cuál es el retardo desde la terminación de la

pregunta hasta el comienzo de la respuesta?.

Consideremos los pasos necesarios para el envío de datos de un *Host* a otro, tenemos (en general):

- 1.- El proceso del ordenador fuente inicia la transferencia.
- 2.- El software de sistema del *Host* transmite los datos a la NIU.
- 3.- La NIU fuente transfiere los datos a la NIU de destino.
- 4.- La NIU de destino transfiere los datos al *Host* de destino.
- 5.- El software de sistema del *Host* acepta los datos, notificandose al proceso de destino.
- 6.- El proceso de destino acepta los datos.

Cada uno de estos pasos implica algún tipo de procesamiento y el uso de recursos potencialmente compartidos por otros. Lo que hemos tratado hasta ahora ha sido la comprendido en el tercer paso.

Para poder estudiar el rendimiento de extremo a extremo, el analista debe modelizar el NIU, el enlace *Host*-NIU, y el *Host*, así como el enlace NIU-NIU. Dentro de los pocos estudios llevados a cabo de esta manera, destacamos el realizado por un grupo de analistas de **CONTEL Information Systems**. En esta sección nos referiremos a los resultados de los estudios de este grupo.

La discusión que sigue hace referencia a la figura

9.14. Como mencionamos anteriormente, el retardo, digamos, desde que un mensaje es generado en un nodo A por alguna aplicación hasta que llega al nodo B, es justamente la suma de los retardos que se producen en cada paso.

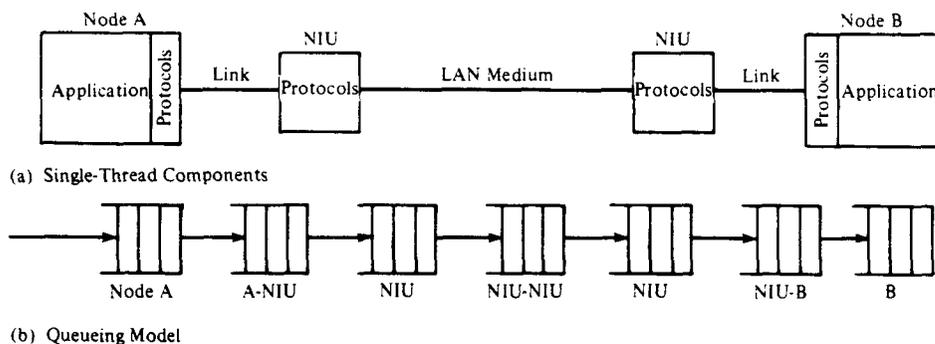


FIGURE 9-14. End-to-end local network performance model

Cuando un abonado a la red llega a un servicio del sistema y lo encuentra ocupado, se produce una situación de espera (colas). El retardo sufrido por el abonado es el tiempo empleado en la cola más el tiempo del servicio. El retardo depende de la configuración del tráfico entrante y de las características del Server. La tabla 9.3 resume algunos resultados simples.

El sistema mostrado en la figura 9.14 es un sistema de colas (de espera) en cascada con un sólo servidor, esto es, la salida de una cola es la entrada de la siguiente. En el caso general, caracterizar el comportamiento de este sistema es una tarea complicada, y no existen soluciones tajantes. No obstante, hay un teorema (el teorema de

Jackson) que dice que bajo ciertas condiciones, cada nodo de la red de colas puede ser tratado independientemente.

TABLE 9.3 Isolated Queues

Parameters

w = mean number of items waiting for service (not including items being served)

q = mean number of items in system (waiting and being served)

t_w = mean time item spends waiting for service

t_q = mean time item spends in system, waiting and being served

ρ = utilization: fraction of time a servicer is busy

S = mean service time for an item

Assumptions: Poisson arrivals with parameter λ , exponential service times

$$w = \frac{\rho^2}{1-\rho}$$

$$q = \frac{\rho}{1-\rho}$$

$$t_w = \frac{\rho S}{1-\rho}$$

$$t_q = \frac{S}{1-\rho}$$

$$\rho = \lambda S$$

Por lo tanto el retardo en cada nodo puede ser calculado independientemente luego sumados para dar el total. Estas condiciones son:

- * El trabajo llega desde el exterior según la distribución de Poisson.
- * Tiempo de servicio exponencial en cada nodo, con política de el primero que llega, es al primero que se sirve.
- * Colas no saturadas: Las colas son lo suficientemente largas para acomodar el máximo número de abonados que esperan.

Empezando por la primera cola, y con una llegada dada de f , el retardo de este paso, estará determinado como $p = fS \leq 1$, la cola es estable y la velocidad de salida es igual a la velocidad de entrada. Esta salida es ahora la entrada del segundo paso, y así sucesivamente.

Para un sistema estable, debemos tener:

$$f = \frac{1}{\text{MAX } [S_i]}$$

Esto representa la capacidad de tratamiento máxima que se puede obtener. Tan pronto como esta condición es satisfecha, el retardo total de un mensaje a través de N pasos es:

$$D = \sum_{i=1}^N D_i$$

Veamos nodo a nodo. El nodo A debe realizar tareas relacionadas con el pase de mensajes, incluyendo el procesamiento de aplicaciones. Estas tareas pueden tener varias prioridades con interrupciones adquiridas (Preenptives). Para cada tipo de tarea, la ecuación de la cola es:

$$t_{qj} = \frac{1}{1 - \sum_{i=1}^{j-1} p_i} \frac{\sum_{i=1}^j p_i S_i}{1 - \sum_{i=1}^j p_i} + S_j$$

Donde $p_i = f_i S_i$

Para resolver esta ecuación, necesitamos valores para f_i y S_i . El primero depende de la velocidad con la que son generados los mensajes. El segundo puede ser aproximado estimando la longitud del camino de ejecución de cada rutina de servicio y dividiéndola por el número de instrucciones efectivas por segundo del procesador.

El próximo retardo que encontramos es el introducido por el enlace de comunicaciones entre el nodo A y su NIU. Este retardo dependerá de la naturaleza del interface. Como ejemplo, consideremos una línea *Half-Duplex* con una velocidad de transferencia de interface dada. Aquí hay dos clases de llegadas para un único servidor: del nodo al NIU y del NIU al nodo. El f_i ($i=1,2$) depende de la velocidad con que llegan los mensajes para transmitirlos a través del enlace. El tiempo de servicio en cualquier dirección (S_1, S_2) es la longitud media dividida por la velocidad de transmisión de los datos. Luego si no hay prioridades:

$$p = f_1 S_1 + f_2 S_2$$

$$S = \frac{p}{f_1 + f_2}$$

donde S es el tiempo de servicio total. Entonces

$$t_{qj} = t_w + S_j = \frac{p S}{1 - p} = S_j \quad (j = 1, 2)$$

El NIU es la siguiente fuente de retardo y debe modelarse de la misma forma que el nodo A. A continuación viene la red local en sí. El retardo de este paso depende de la topología (Anillo, Bus ó Arbol) y del protocolo de acceso al medio. Esto lo hemos estudiado ya en las secciones 9.2 y 9.3 de este capítulo. Los pasos restantes son simétricos a éstos.

Debemos hacer dos puntualizaciones: Primera, un NIU suele tener varios puertos, por lo que la llegada de trabajo a un NIU está compuesta por las llegadas de varios *Host*. Segundo, el enlace nodo-NIU puede estar multiplexado ya que las entradas pueden venir de varios nodos remotos.

Como ejemplo vamos a considerar que el nodo A es un *Host* y el B una estación de trabajo inteligente. En el nodo A, hay un programa de aplicación que intercambia mensajes con la estación de trabajo. Hay cinco clases principales de actividades asociadas a la aplicación. Suponemos que éstas están servidas para el *Host*. Las actividades, en orden descendente de prioridades, son:

- 1.- **Link-in:** Funciones de nivel de enlace para mensajes de llegada desde el NIU.
- 2.- **Link-out:** Funciones de nivel de enlace para mensajes de salida hacia el NIU.
- 3.- **Protocols-in:** Funciones de protocolo de alto nivel para mensajes de llegada.
- 4.- **Protocols-out:** Funciones de protocolo de alto nivel para mensajes de salida.

5.- **Application:** Procesamiento de la aplicación.

Se supone que el interface **Host/NIU** tiene una velocidad de transferencia efectiva de 800 Kbps, mientras que el interface estación de trabajo/**NIU** tiene una de 9.6 Kbps. Este podría ser el caso de una **NIU** integrada en el **Host** y de una **NIU** independiente de terminal.

Suponemos también que el **NIU** implementa la capa de transporte con las siguientes prioridades:

- 1.- **Network Link-in.**
- 2.- **Node Link-in.**
- 3.- **Network Link-out.**
- 4.- **Node Link-out.**
- 5.- **Higher Layer Protocols.**

Por último se supone un sistema **CSMA/CD** no persistente que funciona a 1.544 Mbps.

Los resultados del ejemplo están resumidos en la tabla 9.4, los cuales muestran que, dentro de la utilización moderada del Bus, el Bus contribuye solamente con un 5% del retardo. Como consecuencia (como ya vimos anteriormente) se deduce que el efecto de la topología y del control de acceso al medio sobre el total de retardo es despreciable hasta que el medio se acerca a la saturación. Más que la determinación del punto de saturación, el estudio del rendimiento de un sistema debe centrarse en la cuestión del retardo de extremo-a-extremo.

TABLE 9.4 End-to-End Delay, CSMA/CD Network

<p><i>Traffic parameters</i> Arrival rate: 0.017 message per second Aggregate load: 100,000 bps</p> <p><i>CSMA/CD parameters</i> Propagation: 30 μs Retransmission interval: 5</p> <p><i>MSG lengths</i> Input: 800 characters Output: 12,000 characters</p> <p><i>I/F Transfer rates</i> Host: 800,000 bps Workstation: 9600 bps</p>	<p><i>Protocol path-length parameters</i> Node protocols Send: 12,000 instructions Receive: 12,000 instructions</p> <p>Node access link layer Send: 75 instructions Receive: 75 instructions</p> <p>Network access link layer Send: 75 instructions Receive: 75 instructions</p> <p>TCP/IP: 12,000 Multiprogram level: 32</p> <p><i>Processor capacities</i> Host: 1.100 MIPS BIU: 0.615 MIPS Workstation: 0.115 MIPS</p> <p>Host application program path length: 50,000 instructions Cable utilization: 0.0565 Total normalized traffic, including retransmissions: 0.06</p>
--	---

Delay Categories

Throughput	Response	Host	HI/F	WI/F	HBIU	WBIU	W/S	Cable
0.50	2.0066	0.04	0.01	0.84	0.01	0.02	0.02	0.05
1.00	2.0252	0.04	0.01	0.84	0.01	0.02	0.02	0.05
1.50	2.0444	0.04	0.01	0.84	0.01	0.02	0.02	0.05
2.00	2.0645	0.04	0.01	0.84	0.01	0.02	0.02	0.05
2.50	2.0853	0.04	0.01	0.83	0.02	0.02	0.02	0.05
3.00	2.1071	0.04	0.01	0.83	0.02	0.02	0.02	0.05
3.50	2.1298	0.04	0.01	0.83	0.02	0.02	0.02	0.05
4.00	2.1536	0.04	0.01	0.83	0.02	0.02	0.02	0.05
4.50	2.1785	0.05	0.01	0.83	0.02	0.02	0.02	0.05
5.00	2.2047	0.05	0.01	0.83	0.02	0.02	0.02	0.05
5.50	2.2324	0.05	0.01	0.83	0.02	0.02	0.02	0.05
6.00	2.2616	0.05	0.01	0.82	0.03	0.02	0.02	0.05
6.50	2.2927	0.05	0.01	0.82	0.03	0.02	0.02	0.05
7.00	2.3259	0.05	0.01	0.82	0.03	0.02	0.02	0.05
7.50	2.3615	0.06	0.01	0.82	0.03	0.01	0.02	0.05
8.00	2.4001	0.06	0.01	0.81	0.03	0.01	0.03	0.05
8.50	2.4424	0.06	0.01	0.81	0.03	0.01	0.03	0.05
9.00	2.4892	0.06	0.01	0.80	0.04	0.01	0.03	0.05
9.50	2.5423	0.07	0.01	0.79	0.04	0.01	0.03	0.05
10.00	2.6041	0.07	0.01	0.78	0.05	0.01	0.03	0.05

INTERNETWORKING

En muchos casos, quizás en la mayoría, una red local no será una entidad aislada. Una empresa puede tener más de un tipo de red local en un mismo sitio, para satisfacer necesidades diferentes. Esta empresa puede querer interconectarlas para tener un control del intercambio de información distribuido.

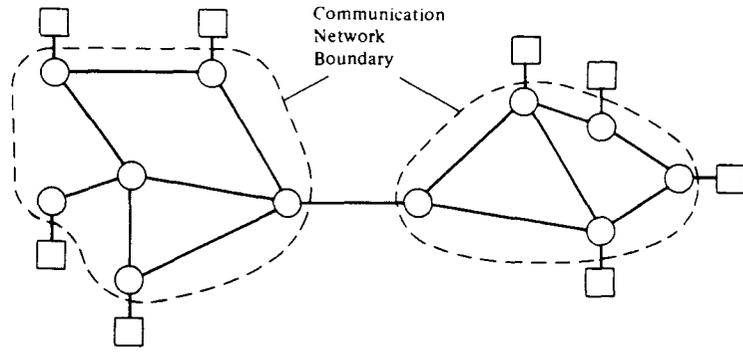
Este capítulo se encarga de las cuestiones involucradas en la conexión de una red local con otras redes. Esto es a lo que se denomina "Internetworking". El término "Internet" se utiliza para referirse a varias redes conectadas entre sí.

ENFOQUES ARQUITECTONICOS:

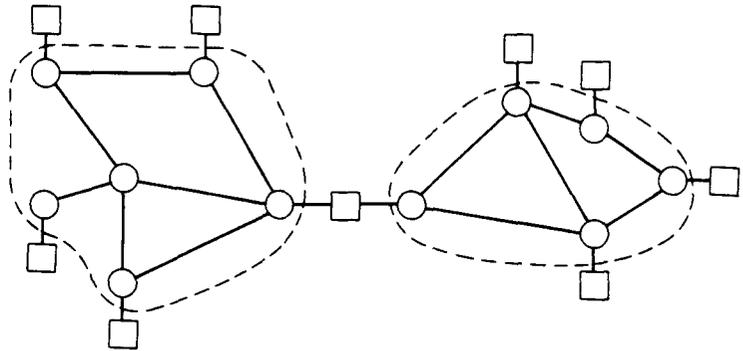
Como veremos, se necesita algún tipo de función de acceso (Gateway) para interconectar redes. La cuestión clave en el diseño de dicha función tiene que ver con la arquitectura que se use. Esencialmente hay dos dimensiones que determinan esta arquitectura:

- * La naturaleza del interface.
- * La naturaleza del servicio de transmisión.

Hay dos tipos de interface: entre nodos (DCE) y entre estaciones (DTE) (figura 10.1). Un interface a nivel DCE implica, como mínimo, que las redes tienen un interface de acceso a la red común. Esto no implica necesariamente que ambas redes tengan los mismos protocolos internos; si los tienen, la función de enlace se reduce a un puente (Bridge). En cualquier caso, hay un formato standard para los paquetes que entran y salen de cada red. La principal ventaja de esto es que, con la excepción de un espacio expandido de la dirección, los *Host* no notan que hay más de una red. Si el sistema se diseña de forma apropiada, no se necesitan cambios en el software de los ordenadores principales. Si dos *Host* pueden conectarse mediante una red única, también lo podrán hacer vía múltiples redes con el mismo interface de acceso a red.



(a) Node-level Interface



(b) Station-level Interface

FIGURE 10-1. Internetwork Interfacing

Sí no es posible estandarizar el interface de acceso a la red, se hace necesario algún tipo de traducción, ó al menos de manipulación. En el caso peor, se ha de construir una función de acceso especializada para cada par de redes. Un procedimiento mejor es estandarizar los objetos que van a pasar de una red a otra. En cualquier caso esta función es realizada por una estación que se enganche a dos estaciones.

La otra dimensión que caracteriza la arquitectura de Internetworking es la naturaleza del servicio de

transmisión, el cual puede ser extremo-a-extremo ó red-a-red. En el caso de extremo-a-extremo supone que todas las redes ofrecen al menos un servicio de datagramas ineficaz; esto es, si una secuencia de paquetes es enviada de un *Host* a otro en la misma red, algunos pero no necesariamente todos llegarán a su destino, y deben haber duplicaciones y reordenación de la secuencia. La transmisión a través de varias redes requiere un protocolo de extremo-a-extremo común, para facilitar un servicio extremo-a-extremo eficaz. En el caso de red-a-red, la técnica consiste en proporcionar un servicio eficaz dentro de cada red y entonces enlazar segmentos individuales a través de varias redes.

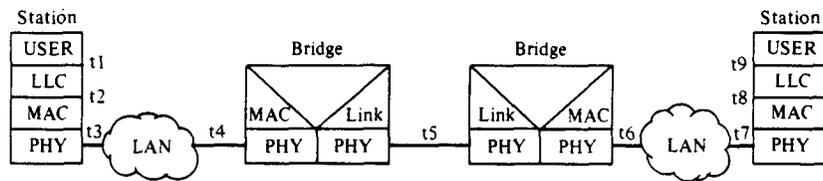
En el caso de situarnos en un interface a nivel **DTE** tenemos la desaprobada arquitectura red-a-red. En este caso, nos encontramos con redes que no tienen un interface de acceso común ni un protocolo extremo-a-extremo común. La única manera de interconectarlas es proporcionar un verdadero traductor de protocolos entre ambas redes para cada función de acceso (Gateway). (Software específico).

La otra opción de la arquitectura extremo-a-extremo a nivel **DTE**. Esta arquitectura es implementada usando un protocolo por encima de la capa red, llamado Internet Protocol (IP). El IP fué desarrollado originalmente para **ARPANET** y ha sido estandarizado por el Departamento de Defensa de los Estados Unidos. ISO también tiene un standard muy similar.

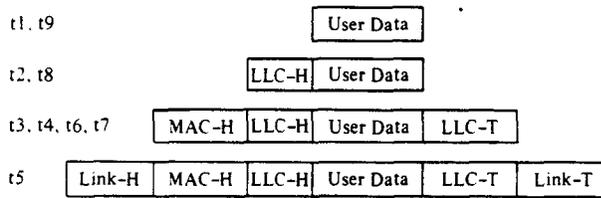
REDES LOCALES HOMOGENEAS.

El tipo más simple de red local múltiple es el que está formado por redes locales homogéneas. Dichas redes tienen el mismo interface para los dispositivos enganchados y generalmente usan el mismo protocolo interno para el acceso medio.

Un ejemplo sencillo de este principio es el repetidor usado en sistema de redes múltiples. El repetidor se usa simplemente para alargar la longitud del cable de banda base. Este amplifica y retransmite todas las señales, incluyendo las colisiones. Luego el sistema se comporta, desde cualquier punto de vista, como una red simple.



(a) Architecture



(b) Operation

FIGURE 10-2. Bridge Over a Point-to-Point Link

Un verdadero sistema con redes separadas pero homogéneas necesita un puente (Bridge) para conectarlas. Este concepto fué tratado en el capítulo 4 como una forma de enlazar varios Anillos.

Un puente, en esencia, está formado por NIUs enlazadas. Considerando una conexión entre las redes A y B, el puente debe realizar las siguientes funciones:

- * Leer todos los *Frames* transmitidos por A, y aceptar aquellos que van dirigidos a B.
- * Retransmitir esos *Frames* a B, usando el protocolo de control de acceso al medio para B.
- * Hacer lo mismo para el tráfico de B a A.

Además de estas funciones básicas, hay una serie de consideraciones de diseño a tener en cuenta.

- 1.- El puente no hace ninguna modificación en el contenido ó forma de los *Frames* que recibe, ni los encapsula con una cabecera adicional. Sí se hace algún tipo de modificación ó adición, nos encontraríamos con un dispositivo más complejo: un acceso (Gateway).
- 2.- A pesar de lo dicho en el punto 1, el puente puede ser concebido internamente para que utilice otro protocolo. La figura 10.2 nos muestra un puente formado por dos NIUs conectadas con un enlace punto-a-punto, que puede ser un enlace HDLC. Para atravesar ese enlace, se enrollan uno ó más *Frame* de LAN en un

Frame HDLC.

- 3.- El puente contendrá suficiente espacio de *Buffer* como para hacerse cargo del total de las demandas, ya que durante un corto período de tiempo los *Frames* pueden llegar más rápidamente de lo que pueden ser retransmitidos.
- 4.- El puente debe también tener inteligencia en cuanto a *Routing* y direccionamiento. Como mínimo, debe saber que direcciones corresponden a cada red para saber que *Frames* pasar. Dado que pueden haber más de dos redes en cascada, el puente debe ser capaz de pasar *Frames* dirigidos a redes adicionales.

Esta descripción es la del tipo más sencillo de puente; pero éste puede ser más sofisticado.

Todo lo dicho de puentes está referido a redes locales de paquetes conmutados. En el caso de circuitos conmutados, la función del puente resulta innecesaria. Una configuración de Estrella Jerárquica actúa como una red sencilla pero presenta las ventajas antes mencionadas de redes homogéneas.

10.3

REDES HIBRIDAS.

Por lo dicho en los capítulos 1 y 3, es evidente que

hay tres tipos de redes (LAN, HSLN, PBX digital) tienen puntos fuertes diferentes y complementarios. En algunos lugares, la mezcla de dos o tres tipos puede servir mejor las necesidades de una empresa u organización.

Por ejemplo, todos los teléfonos, terminales de baja velocidad, y microordenadores podrían engancharse en una PBX digital. Esto cuenta con la ventaja del bajo coste de las conexiones a la PBX digital de dispositivos que no tienen requerimientos de alta velocidad. La mayoría de los miniordenadores y algunos periféricos de alta velocidad pueden ser enganchados a una LAN. Por último los grandes ordenadores (Mainframes) que constituyen la estructura principal de un sistema así como los dispositivos de almacenamiento masivo pueden ser conectados a una HSLN.

Los terminales y los ordenadores personales enganchados a la PBX digital pueden desear acceder a aplicaciones realizadas por los miniordenadores ó bien acceder a los datos controlados por un *Mainframe*, etc...

La figura 10.3 muestra una posible arquitectura híbrida de redes locales. En ella podemos apreciar que una PBX digital podría engancharse a una LAN vía uno ó mas puentes de un NIU. Un terminal que desee conectar con algún dispositivo LAN solicitaría primero una conexión NIU y luego accedería a la LAN como si estuviese directamente enganchado. La PBX digital puede, a través de su acceso a red de telecomunicaciones de larga distancia, proporcionar una conexión con la LAN para terminales remotos.

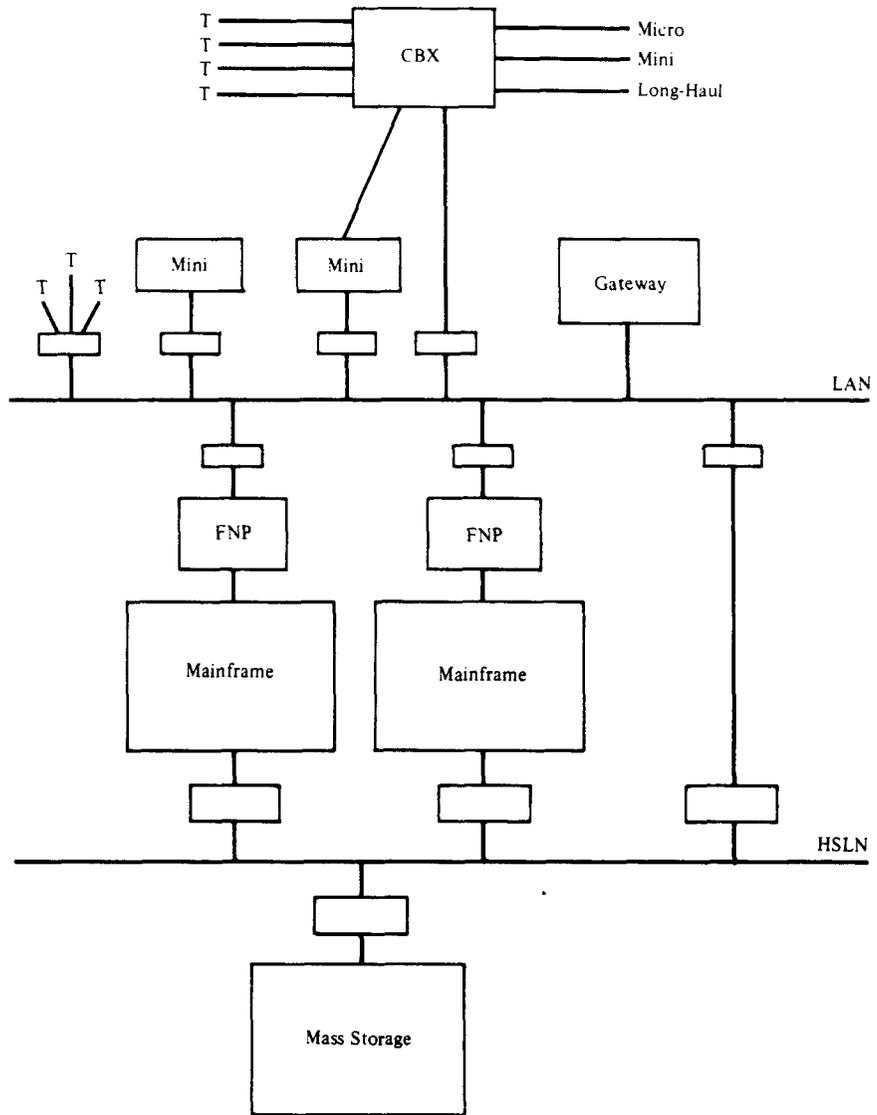


FIGURE 10-3. Hybrid Local Network Architecture

Otro enlace posible PBX-LAN es a través de los puertos de E/S de un Host (mini) conectado a la LAN. Si los enlaces PBX-Host están dedicados a una única conexión lógica, la PBX está suministrando un servicio de conexión de puerto. Si la PBX proporciona un protocolo servidor

para algún protocolo de multiplexado como el X.25, entonces el enlace PBX-Host puede realizar varias conexiones lógicas. La PBX está ahora actuando como un concentrador de terminales.

Consideremos ahora las conexiones LAN-HSLN. El tráfico que va a ser tratado en esta conexión entra dentro de una de estas dos categorías: interactivo ó transferencia de ficheros. Un ejemplo de tráfico interactivo es un terminal enganchado a una LAN (directamente ó vía PBX-NIU) que desea usar una aplicación de tiempo compartido de una Base de Datos de un *Mainframe*. Este tipo de tráfico supone unos mensajes bastante cortos. Está pues claro que este tipo de tráfico debería ser mantenido fuera de la HSLN, ya que esta funciona mejor con paquetes largos. La conexión apropiada es tener el procesador central (FNP) del *Mainframe* conectado directamente a la LAN. El FNP está diseñado exactamente para este tipo de tráfico.

El tráfico de transferencia de ficheros puede ser manejado de forma diferente. Un ejemplo puede ser: una aplicación de entrada de datos está corriendo en un *Host* conectado a una LAN. Periódicamente, se deben mandar a archivar en un dispositivo de almacenamiento masivo. Este tráfico podría ir directamente a través de un enlace NIU-NIU. Este enlace sería un puente ya que la HSLN y la LAN pueden usar formatos de *Frame* diferentes, pero no es mucho más complejo que ésto.

Por último, los enlaces de larga distancia pueden ser tratados de dos modos. Con una conexión **PBX** con las redes de circuitos conmutados de larga distancia, se pueden obtener algunos servicios simples como el acceso de terminales remotos. Otras aplicaciones se consiguen vía *Gateway* a unas redes de paquetes conmutados. El *Gateway* puede ser un *Host* ó un **NIU** enganchado a la **LAN**. Esta función de acceso (*Gateway*) es la que se suele denominar **Internetworking**.

Una red híbrida idealmente podría proporcionar alto rendimiento a los usuarios que la necesiten, conexiones de bajo coste para aquellos con necesidades más modestas, y un camino para proporcionar mejor rendimiento a más personas a medida que ésta se abarata.

A continuación vamos a dar una serie de ejemplos gráficos de combinaciones de distintas redes:

Ethernet y PBX:

La ventaja de esta disposición es que los terminales que necesitan un ancho de banda grande, como estaciones de gráficos y ordenadores personales sin **Disk Drivers**, la obtienen conectándose a una **Ethernet**; y las estaciones que necesitan menor ancho de banda (terminales y ordenadores personales con disketera) lo obtienen vía **PBX**. Suponiendo que no haya muchas estaciones de alta velocidad, las limitaciones en el largo de los cables y las distancias en **Ethernet** no es un problema. En cambio sí hay muchas

estaciones de baja velocidad, la PBX resulta muy atractiva.

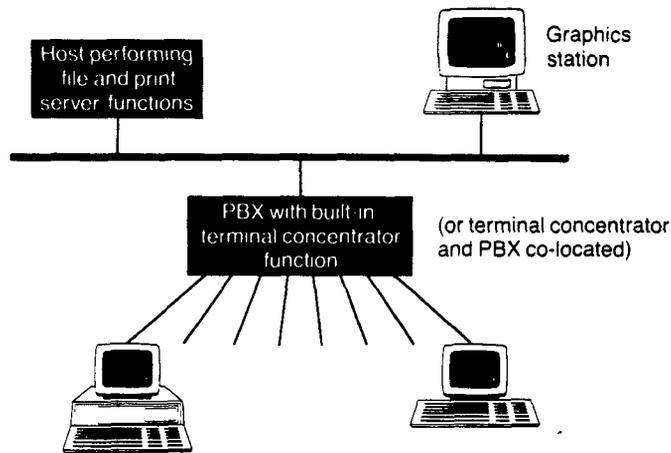


FIGURE 10-4.

Por otro lado, la PBX no necesita ser diseñada para soportar un ancho de banda tan grande como el necesario para trabajar con estaciones de gráficos. Por último, el número de estaciones tanto de alta velocidad como baja velocidad puede ser alterado de un modo razonable sin producir daños.

Token Ring y PBX:

Las ventajas de esta combinación son básicamente las mismas que se señalaron en la anterior, teniendo en cuenta las ventajas e inconvenientes del Token Ring, en vez de las de la Ethernet.

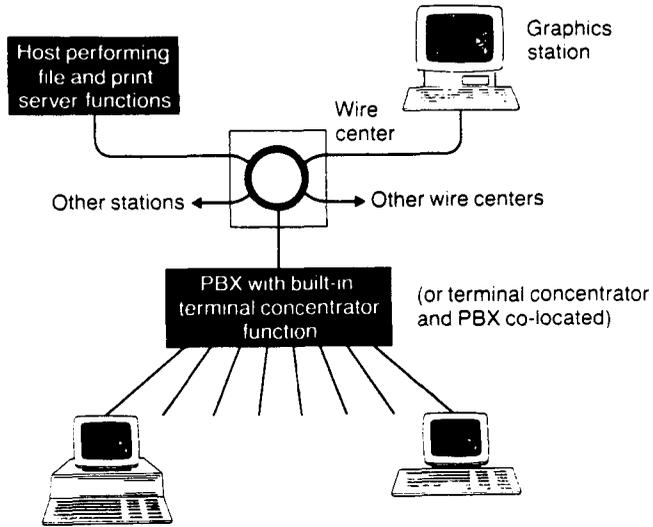


FIGURE 10-5.

Ethernet y concentrador de terminales de larga distancia:

Aquí se sustituye la PBX por el concentrador.

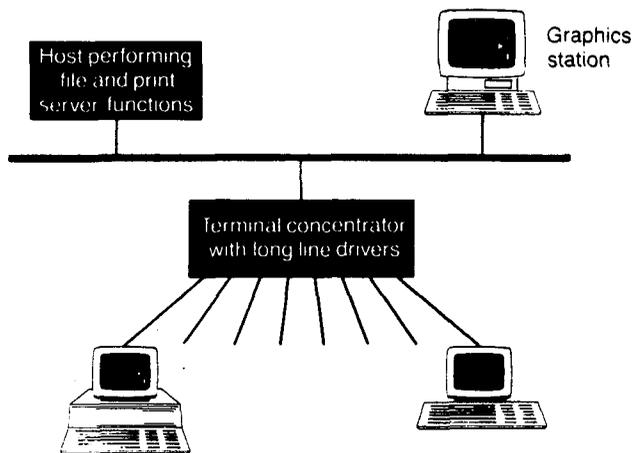


FIGURE 10-6.

Token Ring y concentrador:

Es lo mismo que antes pero hay que tener ahora en cuenta las ventajas e inconvenientes del Token Ring.

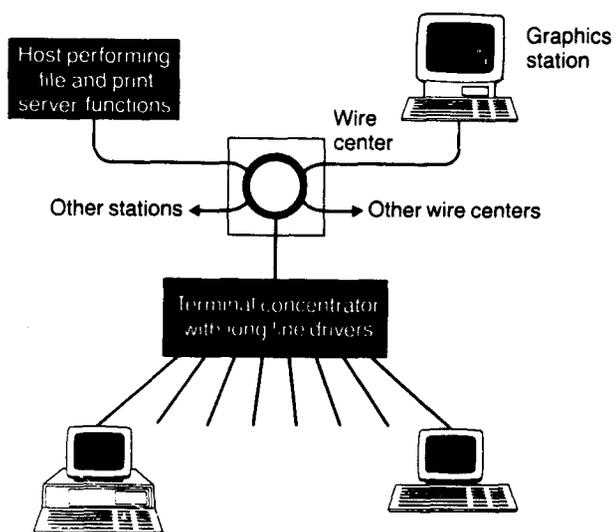


FIGURE 10-7.

Ethernet, Token Ring y PBX:

En este sistema los terminales de ancho de banda grande se enganchan al Token Ring ó a la Ethernet, dependiendo del vendedor del equipo. La gran aceptación y simplicidad de las conexiones Ethernet es aquí una ventaja. Las estaciones con necesidad de una ancho de banda menor se enganchan a la PBX, donde el bajo coste de las conexiones y la oportunidad de integrar señales de voz constituyen un gran atractivo. La gran capacidad de manejo

de tráfico, de conversión a fibra óptica y de distancia hacen del Token Ring una buena espina central del sistema.

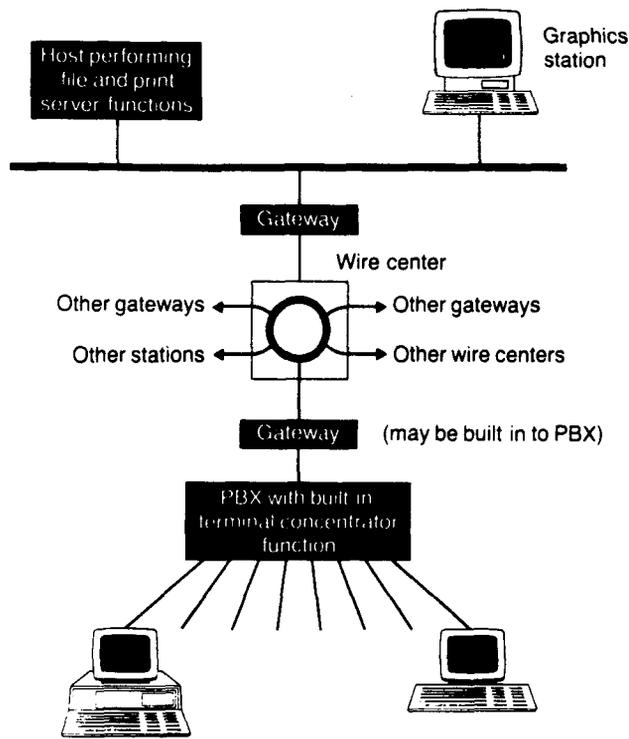


FIGURE 10-8.

Ethernet, Token Ring y Ethernet:

En este diseño, los terminales con necesidad de un ancho de banda pequeño (64 Kbps) se enganchan a la Ethernet vía concentradores de terminales.

APENDICE A

EJEMPLO DE DISEÑO PRACTICO DE UNA RED DE AREA LOCAL

En este último apartado del proyecto, abordamos la tarea del diseño de una red local en base a unas necesidades concretas.

Nuestro ejemplo parte del encargo "teórico" del diseño de una Red de Area Local para la Escuela de Telecomunicaciones de Las Palmas. El objetivo es interconectar un número de PC's del orden de la decena y un μ VAX II de DIGITAL.

El primer paso es el de la elección de la topología más adecuada. Esta elección depende de varios factores, entre ellos la fiabilidad, la capacidad de expansión y el rendimiento. De las tres topologías existentes (y estudiadas), resulta obvio que las Estrella y Anillo son las menos adecuadas a nuestras necesidades. La primera se utiliza en sistemas donde los terminales no poseen mucho más que una simple lógica de aceptación y petición de datos. Las estaciones sólo tienen que tener los requerimientos simples de una comunicación con enlace punto a punto. En la topología Estrella, todo el control

lo ejerce el nodo central, de ahí su gran complejidad y elevado coste. Resulta evidente que nuestra red no necesita un despliegue de medios tan grande, pues se trata de una red pequeña.

La topología en Anillo tiene, en nuestro caso, la misma desventaja que la Estrella; es "demasiado" (grande y cara) para nuestras necesidades. No quiero decir con esto que no se pudiese montar un Anillo una decena de PC's y un μ VAX II, pero la relación coste/utilización/seguridad no resultaría rentable. Los Anillos son utilizados para comunicaciones de alta velocidad (fibra óptica) y gran tráfico de datos. En nuestro caso no se necesitan esas altas velocidades, por lo que, el montar un Anillo supondría un desperdicio de su gran capacidad.

Por último llegamos a la topología Bus/Arbol. Es la topología más flexible de las tres. Con ella podemos manejar un amplio rango de dispositivos (en términos de número de ellos), de velocidades y de tipos de datos. En esta topología la red es simplemente el medio de transmisión (no hay ni nodos como en las anteriores), conectamos las estaciones directamente al medio a través del interfase Hardware apropiado. La red está libre de la carga del procesamiento en la comunicación; desde el punto de vista de la comunicación es un mero medio pasivo de transmisión. De cara al futuro crecimiento de la red tiene

la ventaja de una expansión sencilla con el uso de repetidores; alargando la longitud del Bus, aseguramos el poder aumentar el número de equipos enganchados a la red.

También hemos de tener en cuenta que su coste es menor que el de otras topologías al carecer de nodos y controladores complejos, y por utilizar cables baratos (par trenzado o cable coaxial). Por otro lado, ésta topología es capaz de soportar técnicas de Control de Acceso al Medio (MAC) tanto distribuidas como centralizadas.

Pasando al segundo punto de diseño (los MAC), en nuestro caso convendría que el MAC fuese centralizado en el μ VAX II. Dada la capacidad de tratamiento de éste, podría hacerse cargo del control del acceso al medio descargando así a los PC's de ésta tarea. Obsérvese que no se trata de un nodo central que controle y haga posible la comunicación entre todos los nodos de la red (como en el caso de la topología Estrella). Se trata de una estación más del Bus pero con más responsabilidades en el tema de acceso al medio; por supuesto los PC's deben cumplir los protocolos de comunicación, entrando así a formar parte del control de acceso al medio junto con el μ VAX II.

Nos falta decidir qué técnica de MAC es la más adecuada y, por supuesto, el medio físico que más nos conviene.

Al ser la Bus/Arbol una topología con un medio multipunto (esto es, cuando hay más de dos dispositivos conectados al medio y capaces de transmitir a través de él), quedaría fuera de liza la fibra óptica. Ya comentamos que, hoy en día, las tomas (taps) necesarias para enganchar una estación a un Bus de fibra óptica son tan caras que no resulta una red rentable (sin mencionar los problemas técnicos de pérdida de energía de la señal). Nos quedan pues el par trenzado y el cable coaxial.

El par trenzado parte con una desventaja evidente: su falta de fiabilidad y de seguridad. Es el medio más barato pero el más afectado por el ruido. Y es, además, el más débil físicamente hablando.

El cable coaxial, aunque algo más caro, resulta mucho más rentable en sistemas multipunto debido a que tienen menos pérdidas y por lo tanto soportan, sin repetidores, más dispositivos a mayor distancia.

Hasta ahora tenemos un Bus/Arbol de cable coaxial con MAC centralizado. Sigamos.

De los dos tipos de cable coaxial (50 y 75 Ohm.) debemos elegir para nuestra red el de 50 Ohm. por dos razones:

- * Se ajusta más a nuestras necesidades en tanto en cuanto no desperdiciamos Ancho de Banda. En el caso de elegir el de 75 Ohm. estaríamos

desperdiciando una capacidad de transmisión que el cable tiene y que nunca vamos a usar en nuestra red.

* Menor coste.

Una tercera razón es que nos abre la puerta a los sistemas de Banda Base. Estos sistemas son muy utilizados en las LAN's. En ellos se usan señales digitales que ocupan todo el Ancho de Banda (no hay FDM). Son bidireccionales y la distancia que pueden cubrir sin repetidores es de alrededor de 1Km.

Por último hemos de elegir la técnica de control de acceso al medio que nos resulte más eficiente para nuestro Bus coaxial de banda base.

Típicamente, los MAC's utilizados en la topología Bus/Arbol son:

- * CSMA/CD
- * Token Bus
- * Reserva centralizada

La reserva centralizada es una técnica usada en sistemas de banda ancha (no es nuestro caso) y necesita de un controlador muy complejo, lo cual supone un incremento en el coste de la red.

La Token Bus es más compleja que la CSMA/CD y, aunque tiene innegables ventajas, la complejidad de su algoritmo hace que a bajas cargas (predeciblemente éste sea nuestro

caso) una estación puede tener que esperar muchos pases de Token para coger turno.

La CSMA/CD tiene un algoritmo sencillo, lo que repercute en costes, fiabilidad y mantenimiento. Es una técnica equitativa (todas las estaciones tienen las mismas oportunidades de transmitir) y tiene un buen rendimiento y un retardo bajo a cargas bajas y medias (que son precisamente las que se van a dar en nuestra red). También tiene la ventaja de poder usarse tanto en banda ancha como en banda base (que es nuestro caso).

Llegamos pues a la conclusión de que nuestra red ha de estar compuesta por:

- * Topología Bus/Arbol
- * Cable coaxial de 50 Ohm (banda base)
- * MAC: CSMA/CD

La especificación Ethernet cumple las características que hemos detallado anteriormente. Pero es también labor del diseñador el dimensionar la red, combinando cuestiones como la velocidad de datos, el número de tomas, etc... Hay que tener en cuenta la relación de estos parámetros. Por ejemplo, cuanto menor sea la velocidad, mayor puede ser la longitud del cable (esto es debido a la atenuación).

La especificación Ethernet y el standard original de IEEE especifican el uso de un cable coaxial de 50 Ohm.(como queríamos) y de 0,4 pulgadas de diámetro a una

velocidad de 10Mbps. Con estos parámetros la longitud del cable puede ser de hasta 500m. La distancia entre toma y toma es de 2,5m y se permiten hasta 100 estaciones enganchadas en cada tramo de cable. A este sistema se le denomina "10 base 5".

Existe otro sistema denominado "Cheapernet" que resulta menos costoso al utilizar un cable más delgado. Claro está, soporta menos estaciones, y la longitud máxima sin repetidores es menor que en el '10 base 5'.

En la figura 4.2 podemos ver el esquema de una Ethernet. Consta de cinco elementos:

- * Transceptor (Transceiver)
- * Cable del Transceptor
- * Controlador
- * Cable coaxial de 50 Ohm
- * Extremos del cable coaxial (Terminadores)

El transceptor se conecta mediante una toma de cable coaxial. Transmite señales desde la estación al Bus y viceversa. También se encarga de detectar la presencia de una señal en el cable y de la detección de las colisiones.

El cable del Transceptor es un cable llamado "par gemelo", formado por dos pares trenzados.

El controladores una implementación de todas las funciones necesarias (menos las realizadas por el Transceptor) para manejar el acceso al cable coaxial.

Por último, el sistema de transmisión es un cable coaxial de 50 Ohm con terminadores en sus extremos. Estos terminadores absorben las señales, evitando reflexiones desde los extremos del cable (Bus).

Llegamos pues a la conclusión de que el mejor sistema para nuestras necesidades es una Ethernet cuyo presupuesto adjunto a continuación.

P R O P U E S T A E C O N O M I C A

OFERTA NUM.: GNJ892C20344-A

FECHA: 14/4/89

DIGITAL EQUIPMENT CORPORATION
 CERRO DEL CASTAÑAR, 72
 MIRASIERRA
 28034 MADRID

UNI. POLI. DE CANARIAS
 Esc. Poli. de Telecomunicaciones
 Pza del Toro,1
 3504 LAS PALMAS
 Atn.:Carlos Ramirez

Nos complace remitirle nuestra oferta con la siguiente configuración:

Item	Cant.	Descripción	Precio total
		SW Y HW PARA CREAR UNA RED DE PC'S CON EL MICROVAX II *****	
1	1	QL-DO4AN-AA Licencia de uso del DECnet/VMS End Node y del VMS serv for MS-DOS.	298.300,--
2	1	DELQA-M Tarjeta de red local Ethernet para MicroVAX. Mantenimiento mensual 3.250,--	500.000,--
3	1	CK-DELQA-YB Kit de cables para conexión del DELQA a la cabina BA23 del MV II.	28.500,--
4	1	EO-BNE3H-10 Cable transceiver de 10 metros.	17.000,--

digital

Item	Cant.	Descripción	Precio total
5	1	DESTA-AA Adaptador a red local Ethernet "Thin Wire" para el MicroVAX II. Mantenimiento mensual	55.000,-- 585,--
6	1	QA-A93AA-H5 Kit de distribución y documentación del VMS services for MS-DOS en TK50 (se requiere uno solo por red). Es la parte del SW de integración de PC's que se ejecuta en el VAX.	123.500,--
7	1	QGEL1-H5 Kit de distribución y documentación del DECnet/PCSA en TK50 que incluye * MS-DOS con utilities * DECnet/DOS * MS-Net y NETBIOS interface * MS-Windows * MS-WRITE * VT200 terminal emulator * Información on-line (se requiere uno solo por red). Es la parte del SW de integración de PC's que se ejecuta en MS-DOS.	142.500,--
8	1	DEPCA-BA Kit de integración de IBM's PC/AT/ XT/PS/2-30 ó compatibles en red Thin Wire Ethernet necesario para soportar el VMS services for MS-DOS que incluye : tarjeta de red local Ethernet , cable coaxial fino (Thin Wire) y licencias del DECnet/DOS y del PCSA. Se requiere uno por PC a integrar. Mantenimiento mensual	120.400,-- 1.536,--

TOTALES

Total hardware	720.900,--
Total software	564.300,--

TOTAL NETO EXCLUIDO IVA	1.285.200,--
	=====
Total Mantenimiento hardware /mes	5.371,--

Notas

Condiciones de pago:

- 25% a la recepción del pedido
- 75% a treinta días fecha factura

Estos precios no incluyen I.V.A.

La presente oferta incluye:

- . Doce meses de garantía hardware.
- . Instalación Hardware.

Validez de la oferta 30 días.

Plazo de entrega : 8 semanas.

DIGITAL EQUIPMENT CORPORATION ESPAÑA S.A. JUAN CALLEJA

digital

GLOSARIO

ALOHA.

Técnica de control de acceso al medio para medios de transmisión de acceso múltiple. Cada estación transmite cuando tiene datos para enviar, repitiéndose las transmisiones no confirmadas.

ANS X3T9.5.

Comité patrocinado por el Instituto Americano de Standards nacionales (ANSI) que es responsable de los standards de varios sistemas de interconexión. Este comité ha dado borradores de standards para buses de cable coaxial a alta velocidad y para redes locales en Anillo con fibra óptica.

ARPA.

Siglas de **Advanced Research Projects Agency** (Agencia para la investigación de proyectos avanzados); es una agencia del Departamento de Defensa de los EE.UU. Ahora se conoce bajo las siglas de **DARPA** (Defense Advanced Research Projects Agency).

ARPANET.

Red de ordenadores, utilizada sobre todo en las universidades norteamericanas (pero con otras muchas conexiones, incluyendo transoceánicas). Esta red está en uso desde los 60 y ha sido la cuna de muchos avances en las comunicaciones de ordenadores. Ha sido patrocinada por **ARPA**.

BASE BAND (BANDA BASE).

Transmisión de señales sin modulación. En una red local de banda base, la señal digital (0's y 1's) es insertada directamente en el cable en forma de pulsos de voltaje. La señal consume la totalidad del espectro del cable. No acepta multiplexado por división en frecuencia.

BAUD (BAUDIO).

Número de veces que un sistema cambia de estado en un segundo. Especialmente un canal de transmisión de datos. En un canal binario la tasa de baudios es

igual al número de bits por segundo:

1 baudio = 1 bit por segundo.

Bps.

Bits por segundo, una medida de la velocidad de transmisión.

BRIDGE (PUENTE).

Dispositivo que une (enlaza) dos redes locales de conmutación de paquetes homogéneas. Este acepta todos los paquetes provenientes de cada estación los cuales vayan destinados a estaciones de la otra, los almacena (Buffer), y los retransmite en la otra red.

BROADBAND (BANDA ANCHA).

El uso de cable coaxial para proporcionar transferencia de datos por medio de señales analógicas de RF. Las señales digitales se pasan por un modem y se transmiten por una de las bandas de frecuencia del cable.

BUS.

Topología en la que los dispositivos están enganchados a un medio de transmisión compartido. El medio de transmisión es un cable lineal; las transmisiones se propagan por todo lo largo del medio, y son recibidas por todas las estaciones.

CARRIERBAND (BANDA PORTADORA).

Es lo mismo que una banda ancha de canal único.

CATV.

Siglas de Community Antenna Television. El cable CATV se usa en redes locales de banda ancha.

CENTRALIZED BUS ARCHITECTURE (ARQUITECTURA DE BUS CENTRALIZADO).

Es una topología Bus en la que el Bus es muy corto y los enlaces a los dispositivos enganchados son relativamente mucho más largos.

CHEAPERNET.

Red de área local de banda base que usa un cable más delgado y componentes más baratos que la Ethernet ó que el standard original IEEE 802.3. Aunque la velocidad es la misma (10 Mbps), la extensión de la red y el número de estaciones es menor para Cheapernet.

CIRCUIT SWITCHING (CONMUTACION DE CIRCUITOS).

Método de comunicación en donde se establece un camino de comunicaciones entre dispositivos a través de uno ó varios nodos de conmutación intermedios. Al contrario que en la comunicación de paquetes (Packet Switching), los datos digitales se envían como una

hilera continua de bits. El ancho de banda está garantizado, y el retardo está limitado esencialmente al tiempo de propagación. el sistema de teléfonos usa **Circuit Switching**.

CODEC.

Codificador-decodificador. Transforma voz analógica en una sucesión de bits (codifica), y las señales digitales en voz analógica (decodifica) usando modulación (PCM).

COLLISION (COLISION).

Situación en la que dos paquetes están siendo transmitidos a través de un medio a la vez. Su interferencia hace inteligible a ambos.

CONTENTION (CONTENCION).

La condición en que dos estaciones ó más intentan usar el mismo canal al mismo tiempo.

CRC.

Siglas de **Ciclyc Redundancy Check** (comprobación de redundancia cíclica). Es un valor numérico derivado de los bits de un mensaje. La estación emisora calcula un número que es añadido al mensaje. La estación receptora realiza el mismo cálculo. Si los resultados son diferentes, uno ó más bits son

erroneos.

CSMA.

Siglas de **Carrier Sense Multiple Acces** (acceso múltiple con portadora guiada). Técnica de control de acceso al medio para medios de transmisión de acceso múltiple. Una estación que quiere transmitir, primero mira el medio y transmite sólo si éste está desocupado.

CSMA/CD.

Siglas de **Carrier Sense Multiple Acces With Collision Deteccion** (CSMA con detección de colisiones). Es una versión refinada del CSMA en la cual una estación cesa de transmitir si detecta una transmisión.

DATAGRAM (DATAGRAMA).

Un servicio de conmutación de paquetes en el que los paquetes (datagramas) son encaminados por separado y pueden llegar desordenados.

CDE.

Siglas de **Data Circuit-Terminating Equipment** (equipo terminal de circuito de datos). Nombre genérico para los dispositivos de los propietarios de una red que proporcionan un punto de enganche a la

red para los dispositivos de los usuarios.

DIFFERENTIAL ENCODING (CODIFICACION DIFERENCIAL).

Un modo de codificar datos digitales en una señal digital de modo que un valor binario es determinado por un cambio de señal en vez de por un nivel de señal.

DIFFERENTIAL MANCHESTER ENCODING (CODIFICACION MANCHESTER DIFERENCIAL).

Una técnica de señalización digital en la cual hay una transmisión en medio de cada bit para proporcionar sincronización. La codificación de un 0 (1) es representada por la presencia (ausencia) de una transmisión al comienzo del período del bit.

DIGITAL PRIVATE BRANCH EXCHANGE (DBX).

Red local basada en la arquitectura PBX y que proporciona un servicio voz/datos integrado.

DTE.

Siglas de Data Terminal Equipment (equipo terminal de datos. Nombre genérico para los dispositivos propiedad de los usuarios de la red (estaciones que están enganchadas a la red).

DUAL CABLE (CABLE DUAL).

Un tipo de sistema de banda ancha en el que se usan dos cables separados: uno para la transmisión y uno para la recepción.

ETHERNET.

Especificación de red de área local de banda base a 10 Mbps desarrollada en conjunto Xerox, Intel, y Digital Equipment. Es el precursor del standard IEEE 802.3 CSMA/CD.

FRAME.

Grupo de bits que incluye datos más una ó más direcciones.

FREQUENCY-AGILE MODEM (MODEM DE FRECUENCIA AGIL O VARIABLE).

Un modem usado en algunos sistemas de banda ancha, el cual puede cambiar las frecuencias con el fin de comunicarse con estaciones en bandas dedicadas diferentes.

FDM.

Siglas de Frequency Division Multiplexin. Es una técnica para combinar varias señales en un circuito, separandolas en frecuencias.

FREQUENCY TRANSLATOR (CONVERSION DE FRECUENCIAS).

En sistemas de cable de banda ancha dividida, el dispositivo en el extremo final que convierte las frecuencias de transmisión en frecuencias de recepción y viceversa.

FSK.

Siglas de Frequency-Shift Keying (modificación por cambio de frecuencia. Se trata de una técnica de modulación digital analógica en la que se usan dos frecuencias diferentes para representar los 0's y los 1's.

GATEWAY (ACCESO, ENTRADA).

Dispositivo que une dos sistemas, especialmente si ambos sistemas usan protocolos diferentes. Por ejemplo, un "Gateway" es necesario para conectar dos redes locales independientes, ó para conectar una red local a una red de larga distancia.

GRADO DE SERVICIO.

Para un sistema de circuitos conmutados es la probabilidad de que, durante un período específico de máximo tráfico, una llamada ofrecida no encuentre un circuito disponible.

HEADEND (EXTREMO O CABEZA FINAL).

El punto final de una red banda base en Bus ó Arbol. La transmisión desde una estación va hasta el extremo final (Headend). La recepción viene desde el Headend.

HIGHSPLIT.

Es un tipo de sistema de cable banda ancha en el cual las frecuencias disponibles están divididas en dos grupos: uno para la transmisión (5 a 174 MHz) y otro para la recepción (232 a 400 MHz). Necesita un conversor de frecuencias.

HIGH-SPEED LOCAL NETWORK (HSLN).

Una red local diseñada para proporcionar una alta capacidad de tratamiento entre dispositivos caros y de alta velocidad como **Mainframes** (unidades centrales) ó unidades de almacenamiento masivo de datos.

HOST.

La colección de Hardware y Software que se incorpora a una red y usa esa red para proporcionar comunicación interprocesos y servicios del usuario.

HYBRID LOCAL NETWORK.

Una red local integrada, formada por más de un

tipo de red local (LAN, HSLN, PBX digital).

IEEE 802.

Comité del IEEE, organizado para producir un standard de LAN.

INBOUND PATH (CAMINO DE ENTRADA).

En una LAN de banda ancha, es el camino de transmisión usado por las estaciones para enviar paquetes hacia el extremo final (Headend). Es "camino de entrada" en lo referente a la entrada en el medio (salida de la estación).

ILD.

Siglas de Injection Laser Diode (diodo de inyección de laser). Es un dispositivo de estado sólido que trabaja bajo los principios del laser para producir una fuente de luz para las fibras ópticas.

INTERNET.

Es una colección de redes de conmutación de paquetes conectadas entre sí mediante Gateways.

INTERNETWORKING.

Comunicación entre dispositivos a través de múltiples redes.

IP.

Siglas de Internet Protocol. Es un protocolo de la capa de red usado en el ARPANET.

MANCHESTER ENCODING (CODIFICACION MANCHESTER).

Técnica de señalización digital (transmisión digital de señales) en la que hay una transmisión en la mitad de cada bit. Un 1 se codifica con un nivel alto en la primera mitad de bit; un 0 se codifica con un nivel bajo en la primera mitad del bit.

MAC.

Siglas de Medium Access Control. Para las topologías Bus, Anillo y Arbol, es el método de determinar que dispositivo tiene acceso al medio de transmisión en cada momento. Como ejemplo podremos citar los métodos de Token y CSMA/CD.

MESSAGE SWITCHING (COMUNICACION DE MENSAJES).

Es una técnica de comunicación que usa un almacenamiento de mensajes y un sistema de avance. No se establecen caminos dedicados. Por el contrario, cada mensaje contiene una dirección de destino y es pasado desde la fuente al destino a través de nodos intermedios. En cada nodo, se recibe el mensaje, se almacena brevemente y entonces es pasado al siguiente nodo. Así hasta llegar a su destino.

MIDSPLIT.

Un tipo de sistema de cable de banda ancha en la cual las frecuencias disponibles están divididas en dos grupos: uno para la transmisión (5 a 116 MHz) y otro para la recepción (168 a 400 MHz). necesita un conversor de frecuencias.

MODEM.

Modulador/Desmodulador. Transforma una hilera de bits en una señal analógica (modulador) y viceversa (desmodulador). La señal analógica puede ser enviada por líneas telefónicas, ó puede ser RF ú ondas de luz.

NIU (UNIDAD INTERFACE DE RED).

Siglas de Network Interface Unit. Es un controlador de comunicaciones añadido a la red local. Se encarga de implementar los protocolos de la red local y proporciona un interface para el enganche de dispositivos a la misma.

NONBLOCKING NETWORK.

Es una red de conmutación de circuitos en la que siempre hay al menos un camino disponible entre cualquier par de puntos finales desocupados, independientemente de los puntos finales ya conectados.

OPTICAL FIBER (FIBRA OPTICA).

Un filamento delgado de cristal ó de otro material transparente a través del cual una señal codificada en un haz de luz puede ser transmitida por medio de la refracción interna total.

OUTBOUND PATH (CAMINO DE SALIDA).

En una LAN de banda ancha, el camino de transmisión usado por las estaciones para recibir paquetes provenientes del extremo final (Headend). Es "camino de salida" en el sentido de salida del medio (entrada a la estación).

PACKET (PAQUETE).

Grupo de bits que incluyen los datos más una dirección de fuente y de destino.

PACKET SWITCHING (CONMUTACION DE PAQUETES).

Un método de transmisión de mensajes a través de una red de comunicaciones, en el que los mensajes largos se dividen en paquetes cortos. Los paquetes son entonces transmitidos del mismo modo que en el **Message Switching**. Normalmente la conmutación de paquetes es más eficiente y rápida que la conmutación de mensajes.

PASSIVE HEADEND (HEADEND PASIVO).

Es un dispositivo que conecta los dos cables banda ancha de un sistema de cable dual. No proporciona conversión de frecuencias.

PASIVE STAR (ESTRELLA PASIVA).

Una configuración de red local en topología Estrella en la cual el conmutador central ó nodo es un dispositivo pasivo. Cada estación se conecta al nodo central mediante dos enlaces, uno para transmitir y otro para recibir. Una entrada de señal en uno de los enlaces de transmisión pasa a través del nodo central, donde es dividido equitativamente y sacado por todos los enlaces de recepción.

PBX.

Siglas de Private Branch Exchange. Es un tablero de conmutación de abonado. Proporciona una facilidad de conmutación para teléfonos ó líneas de extensión dentro del edificio y acceso a la red pública de teléfonos. Puede ser manual (PMBX) ó automática (PABX).

PCM.

Siglas de Pulse Code Modulation (modulación por codificación de impulso). Es un método común para la digitalización de la voz. La velocidad usada

normalmente para un canal único de voz digitalizada es de 64 Kbps.

PROPAGATION DELAY (RETARDO DE PROPAGACION).

El retardo entre el momento en que una señal entra en un canal y el momento en que es recibida.

PROTOCOL (PROTOCOLO).

Un juego de reglas que gobiernan el intercambio de datos entre dos entidades.

REGISTER INSERTION RING (ANILLO DE INSERCIÓN DE REGISTRO).

Es una técnica de control de acceso al medio para Anillos. Cada estación tiene un registro que puede mantener (retener) temporalmente un paquete que circula. Una estación puede transmitir siempre que haya un hueco en el Anillo y si es necesario retiene un paquete entrante hasta que haya terminado la transmisión.

REPETIDOR.

Dispositivo que recibe datos en un enlace de comunicación y los transmite, bit a bit por otro enlace, tan rápidamente como son recibidos. No se almacenan. Es una parte integral de la topología Anillo. Se usa también para conectar segmentos lineales en una red local de banda base.

RING (ANILLO).

Topología en la que las estaciones están enganchadas a los repetidores conectados en forma de circuito cerrado. Los datos son transmitidos en un sentido a través del Anillo, y pueden estar disponibles a todas las estaciones enganchadas.

RING WIRING CONCENTRATOR (CONCENTRADOR DE CABLEADO DEL ANILLO).

Lugar a través del cual pasan los enlaces entre repetidores para todo ó parte de un Anillo.

SINGLE-CHANNEL BROADBAND (BANDA ANCHA DE CANAL UNICO).

Un diseño de red local en el que el espectro total del cable se dedica a un único camino de transmisión; no usándose la multiplexación por división de frecuencia. También se conoce como **BANDA PORTADORA** (Carrierband).

SLOTTED ALOHA.

Técnica de control de acceso al medio para los medios de transmisión multiacceso. Es la misma técnica que la **ALOHA**, excepto que los paquetes deben ser transmitidos en particiones (Slots) bien definidas.

SLOTTED RING.

Técnica de control de acceso al medio para Anillos. El Anillo es dividido en particiones (Slot), las cuales deben ser designadas llenas o vacías. Una estación puede transmitir cuando pasa un Slot vacío marcándolo como lleno e insertando un paquete en el Slot.

SPACE-DIVISION SWITCHING (CONMUTACION POR DIVISION DE ESPACIO).

Es una técnica de conmutación de circuitos en la que cada conexión a través del conmutador toma un camino dedicado y separado físicamente.

SPECTRUM (ESPECTRO).

Rango absoluto de frecuencias.

SERVER (SERVIDOR).

Un programa y posiblemente un sistema dedicado de computadoras que proporciona un servicio a los usuarios de un LAN, como acceso compartido a un sistema de ficheros, el control de una impresora, ó el almacenamiento de mensajes en un sistema de correo electrónico.

SPLITTER (DIVISOR).

Dispositivo analógico para dividir una entrada

en dos salidas y para combinar dos salidas en una entrada. Se usa para conseguir una topología de Arbol en redes CATV de banda ancha.

STAR (ESTRELLA).

Topología en la que todas las estaciones estan conectadas a un conmutador central.

STAR WIRING.

Es un método de disposición (colocación) del medio de transmisión que se instala para una red local. Todos los cables están concentrados en un armario de cableado, con un cable dedicado desde el armario hasta cada dispositivo de la red.

STATISTICAL TDM.

Un método de TDM (multiplexado por división en el tiempo) en el que los Slot de tiempo en una línea de transmisión compartida son distribuidos (colocados) en canales de E/S a solicitud.

SUBSPLIT.

Es un tipo de sistema de cable banda ancha en el que las frecuencias disponibles están divididas en dos grupos: uno para la transmisión (5 a 30 MHz) y otro para recepción (54 a 400 MHz). Necesita un conversor de frecuencia.

SYNCHRONOUS TDM.

Un método de TDM en el que los Slot de tiempo en una línea de transmisión compartida son asignados a canales de E/S, mediante unos bases determinadas y fijadas previamente.

TAP (TOMA, DERIVACION).

Un dispositivo analógico que permite la inserción o extracción de señales de un par trenzado o de un cable coaxial.

TCP.

Siglas de Transmisión Control Protocol (protocolo de control de transmisión) es el protocolo de nivel de transporte usado en ARPANET.

TDM BUS SWITCHING.

Una forma de comunicación por división en el tiempo en la cual los Slots de tiempo se usan para transferir datos a través de un Bus compartido entre el receptor y el transmisor.

TERMINATOR (TERMINADOR).

Una resistencia eléctrica en el final de un cable, que sirve para absorber la señal de la línea.

TDM.

Siglas de Time-Division Multiplexing (multiplexación por división en el tiempo). Técnica para combinar múltiples señales en un único circuito, separándolas en el tiempo.

TIME-DIVISION SWITCHING (CONMUTACION POR DIVISION EN EL TIEMPO).

Técnica de conmutación de circuitos en la que los Slot de tiempo de un flujo de datos multiplexados en el tiempo son manipulados para pasar datos desde una entrada a una salida.

TIME-MULTIPLEXED SWITCHING (TMS) (CONMUTACION POR MULTIPLEXACION EN EL TIEMPO).

Es una forma de conmutación por división de espacio en la cual cada línea de entrada es un flujo TDM. La configuración de conmutación puede cambiar para cada Slot de tiempo.

TIME-SLOT INTERCHANGE (INTERCAMBIO DE PARTICIONES DE TIEMPO).

Es el intercambio (permuta) de Slot de tiempo dentro de un flujo TDM.

TIMING JITTER (INESTABILIDAD DE LA BASE DE TIEMPOS u OSCILACIONES CICLICAS).

Desviaciones en la reconstrucción (recuperación) de reloj que puede ocurrir cuando un receptor intenta reconstruir la sincronización, al igual que los datos de la señal recibida.

TOKEN (MARCA, SIGNO).

En una LAN, es una combinación única de bits, cuya recepción (por parte de una estación) indica permiso para transmitir.

TOKEN BUS.

Es una técnica de control de acceso al medio para Bus/Arbol. Las estaciones de un Anillo lógico alrededor del cual se pasa el Token. Una estación que reciba el Token puede transmitir datos, y entonces debe pasar el Token a la siguiente estación del Anillo.

TOKEN RING.

Es una técnica de control de acceso al medio para Anillos. Un Token circula a lo largo del Anillo. Una estación puede transmitir capturando el Token, insertando un paquete en el Anillo, y entonces transmitiendo el Token.

TOPOLOGY (TOPOLOGIA).

La estructura, formada por caminos y conmutadores que proporciona interconexiones de comunicación entre nodos de una red.

TRANSCEIVER (TRANCEPTOR).

Un dispositivo que transmite y recibe.

TRANSMISSION MEDIUM (MEDIO DE TRANSMISION).

Es el camino físico entre transmisores y receptores en una red de comunicaciones.

TREE (ARBOL).

Topología en la que las estaciones están enganchadas a un medio de transmisión compartido (común). El medio de transmisión es un cable ramificado que surge de un extremo final (Headend), sin circuitos cerrados. Las transmisiones se propagan a lo largo de todas las ramas del Arbol, y son recibidas por todas las estaciones.

VIRTUAL CIRCUIT (CIRCUITO VIRTUAL).

Es un servicio de conmutación de paquetes en el cual se establece una conexión (Virtual Circuit) entre dos estaciones al comienzo de la transmisión. Todos los paquetes siguen la misma ruta (no necesitan por tanto llevar una dirección completa) y llegan en

orden.

WIRING CLOSET (ARMARIO DE CABLEADO).

Es un armario especialmente diseñado para el conexionado de redes de comunicación de voz y datos. El armario sirve como punto de concentración para los cables que interconectan dispositivos y como facilidad de remiendo para añadir ó quitar dispositivos de la red.

BIBLIOGRAFIA

- * **LOCAL NETWORKS: An introduction. (segunda edición)**
Autor: William Stalling.
Editorial: Macmillan. 1987.

- * **LOCAL AREA NETWORK: An introduction to the tecnology.**
Autor: John E. McNamara.
Editorial: Digital Press. 1985.

- * **MICROCOMPUTER LANs: Network design and implementation**
Autor: Michael F Hordeski. 1987.

- * **MEASURING A LOCAL NETWORK PERFORMANCE.**
Autores: Amer, P.D.; Rosenthal, R.;y Toense, R.

Editorial: Data communications. 1983.

* **LOCAL NETWORK STANDARDS: No Utopia.**

Autor: Dahod, A.M.

Editorial: Data Communications. 1983.

* **PERFORMANCE ANALYSIS OF LOCAL COMPUTER NETWORKS.**

Autores: Hammond, J. ; y O'Reilly, P.

Editorial: Addison-Wesley. 1983.

* **COMPUTER COMMUNICATIONS: Architecture, Protocols, and Standars.**

Autor: William Stallings.

Editorial: IEEE Computer Society Press. 1985.

* **PERFORMANCE ANALYSIS OF MULTIPLE ACCESS PROTOCOLS.**

Autor: Tasaka, S.

Editorial: MIT Press. 1985.