



UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
ARAGON

"ANALISIS DE LA INTEGRACION
DE FDDI EN ATM"

TESIS PROFESIONAL
QUE PARA OBTENER EL TITULO DE
INGENIERO MECANICO ELECTRICISTA
(ELECTRICO ELECTRONICO)
P R E S E N T A N
HERNANDEZ REYES MARCOS
MORENO COSIO ZABDYEL ALEJANDRO

DIRECTOR DE TESIS:
ING. DAVID BERNARDO ESTOPIER BERMUDEZ



SAN JUAN DE ARAGON, ESTADO DE MEXICO,

1996

TESIS CON
FALLA DE ORIGEN



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

TESIS CON FALLA DE ORIGEN

A esas dos personas que con su ejemplo y comprensión me han hecho creer en mi mismo, que con su apoyo y consejos me han ayudado a lograr mis objetivos y llegar a este momento. Papá y Mamá, lo hemos logrado.

A mis hermanos Erick, Kytzia y Silvia que con su cariño me impulsan a ser mejor cada día, los quiero mucho y se que siempre seguiremos compartiendo nuestro desarrollo personal y profesional.

A toda mi familia, gracias por su apoyo y consejos que en su momento me ayudaron a superar las dificultades para seguir adelante.

A Marcos, por compartir conmigo este trabajo siendo la parte mas importante para llevarlo a cabo.

A mis amigos y compañeros de la DTD, quiero agradecerles todo lo que me han enseñado y hacer el compromiso de no defraudar la confianza que me han tenido.

*En la vida, ganar
no es lo importante,
es lo único.*

Vince Lombardi

A MIS PADRES

Marcos y Catalina

Con todo mi agradecimiento. Porque gracias al amor y confianza que siempre me han brindado he podido alcanzar una de mis más grandes metas. Espero que este trabajo sea para ustedes motivo de orgullo.

A MIS HERMANOS

Adriana, Patricia, Miguel y María Eugenia

Porque estuvieron y han estado siempre a mi lado

A MI NOVIA

Patricia Caballero

Por su apoyo y cariño

*Empieza por hacer lo necesario, luego lo
que es posible y de pronto te encontrarás
haciendo lo IMPOSIBLE*

San Francisco de Asís

Agradecemos Profundamente

A NUESTRO ASESOR

Ing. David Bernardo Estopier Bermúdez

Por todas sus atenciones, ayuda y conocimientos brindados. Esperando que esto sirva como aliciente y lo motive a seguir colaborando como profesor en la UNAM.

A LOS SIGUIENTES PROFESORES EN LA ENEP ARAGÓN

Ing. Raúl Barrón

Ing. Juan Gastaldi

Ing. Narciso Acevedo

Ing. David Terán

Por las facilidades prestadas para la realización de este trabajo.

Al Ing. Juan Méndez Moreno

Porque seguirá siendo un ejemplo a seguir como ingeniero y persona

A LOS SIGUIENTES INGENIEROS EN LA DTD

Ing. Daniel Pompa

Ing. Roberto Rodríguez

Ing. José Luis Legorreta

Porque nos han permitido aplicar los conocimientos adquiridos en la Universidad y nos han apoyado para continuar con nuestro desarrollo profesional

*A Nuestra Universidad De
La Cual Orgullosamente
Somos Parte*

*A La E.N.E.P. Aragón
Que Nos Brindo La
Oportunidad De Un
Desarrollo Profesional*

INDICE

INTRODUCCION

Breve reseña del surgimiento de redes LAN y FDDI.....	I
Situación a nivel mundial.....	III

CAPITULO I. REDES I

1.1 Concepto de Red	3
1.1.1 Definición del concepto.....	3
1.2 Definición de parámetros	3
1.2.1 Jerarquías.....	3
1.2.2 Factor de Carga.....	6
1.2.3 Topologías.....	7
1.2.4 Medios de transmisión.....	10
1.2.5 Anchos de banda.....	28

CAPITULO II. REDES LAN 31

2.1 Definición del concepto	33
2.1.1 Introducción.....	33
2.1.2 Concepto de redes LAN.....	33
2.1.3 Componentes de una red LAN.....	34
2.2 Definición de parámetros	36
2.2.1 Topologías de redes LAN.....	38
2.2.2 Cableado de redes LAN.....	43
2.2.3 Anchos de banda.....	48
2.3 Protocolos	50
2.3.1 Introducción.....	50
2.3.2 SDLC.....	52
2.3.3 HDLC.....	56
2.3.4 Estándares IEEE 802.....	61
2.3.4.1 Introducción.....	61
2.3.4.2 IEEE 802.2.....	62
2.3.4.3 IEEE 802.3.....	65
2.3.4.4 IEEE 802.5.....	68

INDICE

2.3.5 TCP/IP	72
2.3.6 SONET	82
CAPITULO III. FDDI	89
3.1 Principios básicos de operación de FDDI	91
3.1.1 Introducción	91
3.1.2 Componentes del protocolo FDDI	91
3.1.3 Configuraciones de redes FDDI	93
3.1.4 Mecanismos para superar fallas en el anillo	96
3.2 Trama de FDDI	99
3.2.1 Formato de trama de FDDI	99
3.2.2 Codificación de bits en FDDI	107
3.3 Control de acceso al medio	109
3.3.1 Protocolo MAC de FDDI	109
3.3.2 Parámetros de tiempo en un anillo FDDI	111
3.3.3 Operación del anillo FDDI	112
3.4 Ruteo en FDDI	117
3.4.1 Enrutamiento	117
3.4.2 Protocolo de resolución de direcciones (ARP)	118
3.4.3 Protocolos de ruteo	122
3.4.4 Configuración de ruteadores	133
CAPITULO IV. ATM	139
4.1 Antecedentes	141
4.1.1 SDH	141
4.1.2 DQDB	147
4.2 Arquitectura ATM	156
4.2.1 Introducción	156
4.2.2 Modelo B-ISDN	157
4.2.3 Capas y subcapas ATM	158

INDICE

4.3 Estructura ATM	163
4.3.1 Concepto de celda	163
4.3.2 Conexiones ATM: VPI's y VCI's	165
4.3.3 Formato de celdas ATM (UNI y NNI)	166
4.4 Capas de adaptación ATM	170
4.4.1 AAL 1	170
4.4.2 AAL 2	171
4.4.3 AAL 3/4	172
4.4.4 AAL 5	175
4.5 Prioridades y control de tráfico ATM	178
4.5.1 Acciones para el control de tráfico ATM	178
4.5.2 Parámetros que definen la clase de servicio (QOS)	181
4.5.3 Multiplexaje estadístico	183
4.5.4 Operación de un switch ATM	185
CAPITULO V.	
INTEGRACION DE REDES FDDI A TRAVES DE ATM	187
5.1 Antecedentes	189
5.1.1 Introducción	189
5.1.2 Concepto <i>internetworking</i>	189
5.2 Planteamiento del problema	191
5.2.1 Escenario de trabajo	191
5.2.2 Estructura funcional del adaptador FDDI-ATM	194
5.2.3 Encapsulación de tramas FDDI en celdas ATM	195
5.3 TCP/IP en redes ATM	197
5.3.1 Introducción	197
5.3.2 Mapeo de dirección IP en una red ATM	197
5.3.3 Utilización de paquetes ATMARP para resolver una dirección IP hacia una conexión ATM.	201

INDICE

5.4 Estudio técnico y económico para llevar a cabo la implementación de este proyecto	202
5.4.1 Adaptador FDDI-ATM	202
5.4.2 Red ATM.....	207
CONCLUSIONES	209
BIBLIOGRAFIA	213

INTRODUCCION

BREVE RESEÑA DEL SURGIMIENTO DE REDES LAN Y FDDI

El almacenamiento y el análisis de información han sido los más grandes problemas a que se ha enfrentado el hombre desde que inventó la escritura. No es sino hasta la segunda mitad del siglo XX que se han podido resolver, parcialmente, estos problemas gracias a la invención de la computadora.

A principios de los 80's las microcomputadoras habían revolucionado por completo el concepto de la computación electrónica, así como sus aplicaciones y mercado. Sin embargo, los gerentes de los departamentos de informática fueron perdiendo el control de la información puesto que el proceso de la información no estaba centralizado.

A esta época se le podría denominar la era del *floppy disk*. Los vendedores de microcomputadoras proclamaban "*en estos 30 diskettes puede usted almacenar la información de todo su archivo*".

Sin embargo, de alguna manera, se había retrocedido en la forma de procesar la información, porque nuevamente había que acarrear la información almacenada en los diskettes de una micro a otra y la relativa poca capacidad de los diskettes hacía difícil el manejo de grandes cantidades de datos.

Con la llegada de la tecnología del disco duro se lograron dispositivos que permitían enormes almacenamientos de información. Una desventaja de esta tecnología era el alto costo que significaba la adquisición de un disco duro.

Estas razones, principalmente aunadas a otras como poder compartir recursos de relativa baja utilización y alto costo, llevó a diversos fabricantes y desarrolladores a idear las redes locales.

En un principio, las redes de microcomputadoras se formaban por simples conexiones que permitían a un usuario acceder recursos que se encontraban residentes en otra microcomputadora tales como otros discos duros, impresoras, etc. Estos equipos permitían a cada usuario el mismo acceso a todas las partes de un disco y causaban obvios problemas de seguridad y de integridad de los datos.

INTRODUCCION

Hacia 1983, la compañía Novell, Inc. Fue la primera en introducir el concepto de file server (servidor de archivos) en el que todos los usuarios pueden tener acceso a la misma información, compartir archivos y contar con niveles de seguridad.

A partir de 1985 las redes lucharon por colocarse como una tecnología reconocida contra todo tipo de adversidades. En un principio, IBM no consideraba a las redes basadas en microcomputadoras como equipo confiable.

No es sino hasta 1987, cuando IBM acepta esta tecnología como el reto del futuro y acuña el término de conectividad. Después de esto se desata un crecimiento acelerado de la industria de las redes locales. Todos los fabricantes se lanzan a adaptar sus equipos y a proponer nuevas posibilidades en esta área.

HISTORIA DEL SURGIMIENTO DE FDDI

FDDI (Fiber Distributed Data Interface) es un estándar de ANSI (American National Standards Instituted) que soporta la transferencia de datos a velocidades de 100 Mbps, este estándar fue desarrollado por la ASC (Accredited Standards Committee) X3T9.5 en respuesta a las necesidades para mejorar ejecuciones en canales de entrada/salida.

El comité X3T9 es responsable de tratar de computadoras y equipos periféricos. El comité X3 es responsable del desarrollo de estándares de sistemas de procesamiento de información y es el antecesor del comité X3T9. La figura (a) ilustra la posición del comité X3T9.5 dentro de ISO (International Standards Organization).

Anterior al desarrollo de este estándar, el comité X3T9 estaba desarrollando el concepto LDDI (Locally Distributed Data Interface). Aunque LDDI reunía especificaciones para operar a 50 Mbps, tenía significantes limitaciones en velocidad, complejidad de conexión y costo. Esas limitaciones de LDDI junto con los avances de la tecnología de fibra óptica, contribuyeron al desarrollo de FDDI.

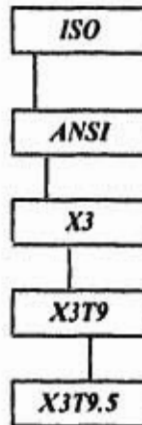


FIGURA (a) POSICION DEL COMITE X3T9.5 DENTRO DE ISO

La propuesta inicial del desarrollo de FDDI fue hecha en octubre de 1982, por James Hamstra un ingeniero de Sperry (ahora Unisys), y otros miembros del comité. Esta propuesta fue aprobada por la X3 ASC en 1983, esta propuesta satisfacía algunas necesidades de las redes LAN tales como un gran número de estaciones interconectadas y una operación descentralizada. A menos de un año, en junio de 1983, fue hecha una propuesta para control de acceso al medio (MAC) de FDDI y para la capa física (PHI). El MAC de FDDI fue hecho un estándar en 1986 por ANSI. La primera demostración pública de la interoperabilidad de FDDI por la ANTC (Advanced National Testing Center) fue hecha en 1984.

SITUACION A NIVEL MUNDIAL

En nuestros días, las redes de alta velocidad no son un lujo, son una necesidad. T-1 (1.544 Mbps) fue rápidamente aceptado cuando hizo su aparición. Más tarde las redes de área local (LAN's), las cuales eran consideradas de alta velocidad, fueron compradas ansiosamente por usuarios quienes necesitaban velocidades más altas. FDDI, introducido en 1983, fue la primera tecnología de alta velocidad que usaba fibra óptica.

INTRODUCCION

Al comienzo de los 90's, FDDI pudo llegar a ser la mejor opción porque soportaba velocidades más grandes que las existentes redes LAN, por lo menos esto fue verdad hasta antes de que el concepto de ATM fuera introducido. Los usuarios ahora tienen muchas opciones para escoger, FDDI, ATM, Frame Relay y Fast Ethernet las más importantes.

FDDI y ATM son una buena opción a escoger, ambas tecnologías son caras pero FDDI tiene muchos vendedores que la respaldan, sin embargo aunque ATM es una nueva tecnología, parece ser la mejor opción.

FDDI podría llegar a ser la red mundial, esto es respaldado por los líderes en ventas de equipo de cómputo IBM, DEC, HP, ICL y Siemens. FDDI es muy aceptada principalmente en el Reino Unido, Alemania y Francia debido a sus avances tecnológicos en fibra óptica.

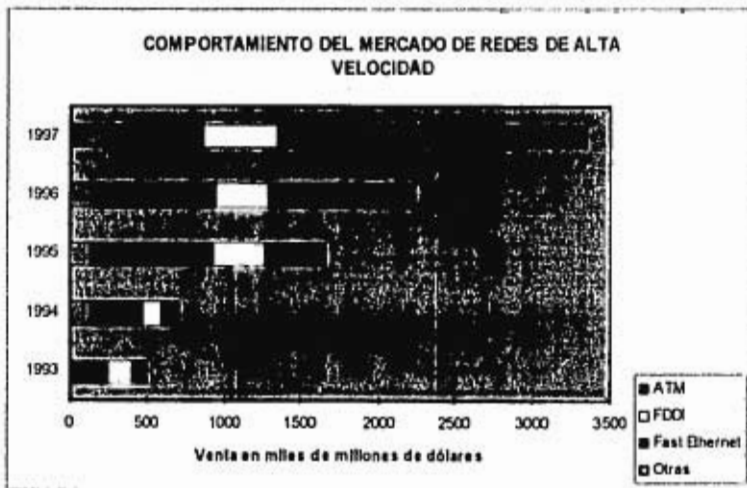
FDDI es una de las pocas tecnologías que han sido aceptadas e instaladas en Norte América e internacionalmente en el mismo lapso de tiempo. Típicamente una tecnología es instalada en los Estados Unidos y aceptada en el mercado mundial en dos años. FDDI, no obstante ha sido aceptada internacionalmente en muy poco tiempo.

FDDI es usada en muchos países. Nodos de alta velocidad, se estiman por 18.6% del mercado de redes LAN de Europa del Oeste en 1996. Japón ha usado fibra óptica por muchos años y le es muy familiar esta tecnología. Por esta razón, Japón tiene algunas de las primeras y más grandes instalaciones con puentes (Bridges) FDDI-to-Ethernet.

FDDI también es instalado en Génova, Suiza, y se suman aplicaciones militares de muchas otras naciones que ven en FDDI seguridad, velocidad y veracidad. Para ATM los datos y las predicciones son muy buenas, ATM crecerá rápidamente debido a aplicaciones multimedia, en 1992 se estimó que había 4000 nodos de ATM y se prevé que para 1997 este número crezca a 854,000, entonces la velocidad de crecimiento actual de 1992 a 1997 es de 192%.

El grupo Yankee de Boston predice que las ventas para 1996 podrían llegar a ser de 619 millones de dólares, y también se espera que 275 millones de dólares sean gastados en investigación sobre ATM sólo en Estados Unidos.

Se espera que la ventas en redes veloces, como ATM, FDDI, Fast Ethernet y otras, crezcan de 478 millones de dólares de 1993 a 3700 millones de dólares en 1997, como se aprecia en la gráfica (b). Existen otras alternativas de alta velocidad, pero tienen antecedentes y bases tecnológicas que pueden limitarlas con mejores opciones para muchas aplicaciones. ATM, que no tienen esas limitantes, será la mejor opción para todas la aplicaciones actuales y de los próximos años.



GRAFICA (B). COMPORTAMIENTO DEL MERCADO EN REDES

CAPITULO I

REDES DIGITALES

1.1 CONCEPTO DE RED

1.1.1 DEFINICION DEL CONCEPTO

Una red esencialmente está formada por nodos, interconectados por medio de enlaces de transmisión. Estos enlaces de transmisión pueden ser vía par torcido, cable coaxial, microondas, satélite o fibra óptica. La red puede estar dedicada a la transmisión de voz (red telefónica), de datos, o ambas. Una red permite que muchos usuarios se conecten de forma rentable, además de que ofrece servicios y funciones de los cuales de otra forma los usuarios individualmente no podrían disponer. Entendiéndose por usuario no sólo personas, pueden ser sistemas automatizados de respuesta de voz, una computadora personal, una terminal de vídeo, una impresora controlada por un computador remoto, etc.

1.2 DEFINICION DE PARAMETROS

1.2.1 JERARQUIAS

Una red puede tener muchas funciones, tales como, compartir recursos de hardware, como impresoras y plotters, pero una de las más importantes es compartir información o un espacio en disco para tener acceso a esta información. En un sistema de red es absolutamente necesario tener un control estricto sobre los derechos de acceso a estos recursos de hardware y software dentro de la red. Este control de acceso está dado por la jerarquía de los usuarios dentro de la red. La jerarquización se refiere a la capacidad de tener usuarios potencialmente con más ventajas en la red para acceder a diferentes directorios, archivos y dispositivos.

Esta jerarquía esta basada sobre un organigrama de personal dentro de la empresa o institución, esta jerarquía otorga ciertas ventajas y desventajas a los usuarios según sus derechos o necesidades en la red. Como un ejemplo de tener una jerarquía en una red, es que el personal de captura de datos no debe tener acceso a la información de nomina de una empresa, o que el personal de vigilancia no debe hacer uso de plotters o impresoras.

Por estas razones es necesario establecer ciertos niveles de seguridad con sus respectivos accesos a los recursos de la red. Como ejemplo, en seguida se describe una clasificación de niveles de seguridad hecha por Novell.

Novell permite precisar un esquema de seguridad controlando el acceso a la red, el uso de subdirectorios y ficheros, y las tareas que realiza cada usuario, para ello utiliza cuatro niveles de seguridad:

1. *Password (clave de acceso)*
2. *Trustee Directory and File Rights (derechos de usuario y grupos)*
3. *Directory Rights (derechos de áreas)*
4. *File Attributes (atributos de archivos)*

1. Password (clave de acceso)

Es indispensable para que una persona pueda acceder a la red que exista como usuario de la misma. El administrador de red es la persona facultada para definir los usuarios de la red.

Cada usuario debe tener una clave secreta (password) de acceso a la red que sólo el conoce (ni siquiera la conoce el administrador). Dicha clave evita la posibilidad de que otra persona entre a la red con nuestro nombre.

2. Trustee Directory and File Rights (derechos de usuario y grupos)

Cuando un usuario es definido en la red por el administrador, éste establece los derechos del usuario; áreas de la red a las que tiene acceso el usuario y con que privilegios trabaja. De esto depende, en gran parte, el buen funcionamiento y la seguridad de la red.

Existen 8 tipos de derechos:

1. R (READ), lectura de archivos abiertos
2. W (WRITE), escritura de archivos abiertos
3. O (OPEN), abrir archivos existentes
4. C (CREATE), crear archivos y directorios

5. D (DELETE), borrar archivos y directorios
6. S (SEARCH), buscar archivos y directorios
7. M (MODIFY), modificar nombre y atributos de un archivo y nombre de un directorio
8. P (PARENTAL), derecho de propiedad que permite acceso a otros usuarios.

Los derechos en grupo son los mismos que existen en usuarios individuales, con la diferencia de que estos se asignan a un grupo de usuarios con funciones similares.

3. Directory Rights (derechos de áreas)

Cada subdirectorio (áreas) tiene sus propios derechos (son los mismos señalados anteriormente). Estos derechos restringen las posibilidades de los usuarios en dicha área.

- a) Los derechos de usuario y de grupo se asignan para una área específica y no en general para toda la red.
- b) Los derechos de usuarios y de grupo vistos como conjuntos, se unen y este "total" se intercepta con los derechos de área para dar los derechos efectivos del usuario en dicho lugar.

4. File Attributes (atributos de archivos)

Es el nivel final de seguridad de la red Novell. Por ejemplo si un usuario tiene derechos efectivos para borrar archivos en un área específica, pero los atributos de archivo, no lo permiten, no podrá borrarlos. Los atributos de los archivos son:

- Read Only: El archivo y el nombre de este archivo no puede ser cambiado o borrado.
- Shareable: Este archivo puede ser leído por muchos usuarios simultáneamente.
- Hidden: Este archivo está oculto en el directorio y no puede ser listado.
- System: Este archivo es uno de los archivos que operan el sistema y no puede ser borrado o cambiado por el usuario.

CAPITULO I. REDES

- **Transaccional:** Este atributo es una característica de seguridad que usualmente se aplica en archivos de bases de datos.
- **Purge:** Este atributo indica que un archivo que ha sido depurado después de que fue borrado, ya no es posible ser recuperado después.
- **Archive Needed:** Identifica los archivos modificados después del último respaldo.
- **Copy Inhibit:** Este archivo no podrá ser copiado.
- **Rename Inhibit:** Este archivo no podrá ser renombrado.
- **Delete Inhibit:** Este archivo no podrá ser borrado.
- **Execute Only:** Este archivo sólo puede ser ejecutado.

1.2.2 FACTOR DE CARGA

El factor de carga se aplica en función de los tipos de usuario que utilizan la red. En la red telefónica se tienen definidos los siguientes factores de carga:

CARGA	VOZ	COMERCIAL	30%
		EMPRESARIAL	70%
	RESIDENCIAL	15%	
DATOS	COMPILACION		20%
	TEXTO	ENVIAN TEXTO	10%
		CONSULTAS	5%

Para una red de datos Novell dividió en 5 tipos de usuario, los cuales se describen a continuación:

Tipo 1.- Es aquel usuario que el 100% del tiempo usa la misma aplicación, procesador de palabra u hoja electrónica, a este usuario se le da el peso de 1.

Tipo 2.- Es el usuario que el 70% del tiempo usa aplicaciones del tipo 1, y el 30% restante usa bases de datos, a este usuario se le asigna un peso de 5.

Tipo 3.- Es el usuario que el 70% del tiempo usa aplicaciones del tipo 2, y el 30% aplicaciones de tipo 1, a este usuario se le da un peso de 15.

Tipo 4.- Es el usuario que el 100% del tiempo usa bases de datos y se le da un peso de 30.

Tipo 5.- El tipo 5 es el usuario que utiliza todo el tiempo compilaciones y se le da un peso de 70.

1.2.3 TOPOLOGIAS

A la hora de realizar la planificación de una red, su topología, representación de los elementos conectados entre sí, sin tener en cuenta su naturaleza, es uno de los factores que más influyen en su rendimiento y en su capacidad para permitir la incorporación de nuevos elementos en la red, y como consecuencia inmediata, de hecho, la necesidad de soportar un mayor volumen de tráfico. Los factores para el análisis y elección de una topología son los siguientes:

- a) Flexibilidad para agregar o eliminar nodos.
- b) Repercusiones sobre falla en algún nodo.
- c) Protocolo de comunicación física.
- d) Problemas en el flujo de información.
- e) Versatilidad en el diseño del cableado.
- f) Posibilidad de crecimiento.

La diferencia que existe entre redes de voz y datos, en este momento, no tiene importancia, ya que si bien la naturaleza de ambas transmisiones son diferentes, el objetivo pretendido es el mismo: enviar cierta información desde un punto origen hacia un punto destino, de forma eficaz.

De igual forma que no es posible la conexión directa entre todos y cada uno de los abonados, no resulta necesario, ni sería práctico, la interconexión directa entre todas las centrales o nodos de interconexión; en consecuencia es necesario agrupar estos elementos conforme a ciertos modelos, de los cuales los más empleados son el de *estrella* (figura 1.1a) y el de *mall*a (figura 1.1b), o bien una combinación entre ambos.

En ciertas aplicaciones, principalmente en redes LAN, también es de uso común el modelo de *anillo* (figura 1.1c) o de *bus* (figura 1.1d).

Topología en estrella

En esta topología todos los elementos de la red, terminales o nodos secundarios, se conectan a un nodo central, que es el encargado de controlar todas las comunicaciones entre ellos. En este tipo de redes es bastante común que el nodo central posea una gran capacidad de proceso y este dotado de un gran número de puertas, suficiente para admitir todas las conexiones, actuando en cierta forma como un concentrador. La función de conmutación realizada por este nodo puede ser de circuitos, caso de redes de voz, estableciéndose una conexión física entre la central de origen y la de destino que permanece todo el tiempo que dura la comunicación; o de paquetes, caso de redes de datos, siendo almacenados en este caso los paquetes en el nodo central, donde son procesados y reenviados posteriormente a su destino.

El principal punto débil de las redes que hacen uso de este tipo de topología es su total dependencia del nodo central; cualquier fallo en este limita el funcionamiento de la red, si bien puede aumentarse su fiabilidad mediante el empleo de elementos redundantes, a costa de perder la economía conseguida por el ahorro de elementos. También es destacar que los límites de expansión de la red se ven determinados tanto por la capacidad de crecimiento como de proceso del nodo central.

Topología en malla.

Este tipo de topología es, actualmente, la más utilizada en redes de amplia cobertura (WAN's), ya que es la idónea para garantizar la existencia de rutas alternativas de enlace y es la que resulta más económica al permitir compartir recursos por los diversos usuarios.

Esta topología es adecuada para soportar cualquier tipo de aplicaciones, siendo su rendimiento alto y pudiéndose adaptar dinámicamente a los volúmenes de tráfico existentes en cada momento, no teniendo limitación alguna en cuanto a los medios de transmisión que pueden ser utilizados. Por el contrario presentan un retardo de transmisión más alto que el de otras configuraciones, ya que no siempre la ruta que toman los mensajes es la más corta.

Topología en anillo

La estructura en anillo es otra configuración bastante usada, la topología en anillo se llama así por el aspecto circular del flujo de información. En la mayoría de los casos, la información fluye en una sola dirección, y cada nodo recibe la señal y la retransmite al siguiente nodo en el anillo. La organización en anillo resulta atractiva porque con ella son bastantes raros los embotellamientos, tan frecuentes en los sistemas en estrella. Además, la lógica necesaria para poner en marcha una red de este tipo es relativamente simple. Sin embargo, como todas las topologías, la topología en anillo tiene algunos defectos. El problema más importante es que todos los componentes del anillo están unidos por un mismo canal. Si falla en canal entre dos nodos, toda la red se interrumpe.

Por eso algunos fabricantes han ideado diseños especiales que incluyen canales de seguridad, por si se produce la pérdida de algún canal. Otros fabricantes construyen conmutadores que redirigen los datos automáticamente, saltándose el nodo averiado, hasta el siguiente nodo del anillo, con el fin de evitar que el fallo afecte a toda la red.

Topología en bus

La topología en bus es frecuentemente utilizada en las redes de área local (LAN's). Es relativamente fácil controlar el flujo de tráfico entre los distintos nodos, ya que el bus permite que todos los nodos reciban todas las transmisiones, es decir, un nodo puede difundir la información a todos los demás.

La principal limitación de una topología en bus está en el hecho de que suele existir un sólo canal de comunicaciones para todos los dispositivos de la red. En consecuencia, si el canal de comunicaciones falla, toda la red deja de funcionar, además de que como la información viaja en un sólo medio puede presentarse el problema de las colisiones. Otro inconveniente de esta topología consiste en la dificultad de aislar las averías de los componentes individuales conectados al bus.

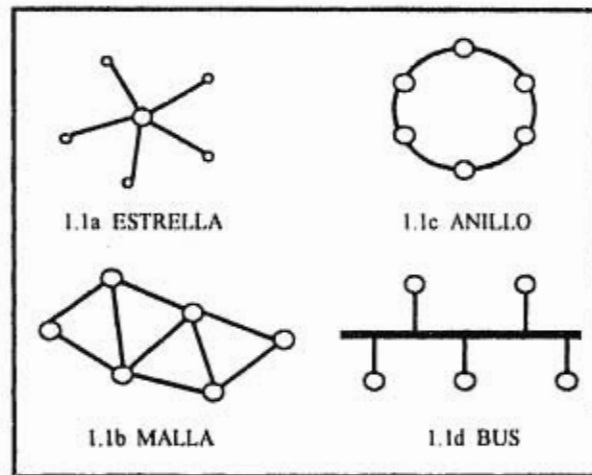


FIGURA 1.1 TOPOLOGIAS DE UNA RED

1.2.4 MEDIOS DE TRANSMISION

Uno de los componentes más importantes que afectan a la operación de una red de comunicaciones, es el medio de transmisión. Hay una gran cantidad de medios disponibles para el diseñador de la red; el medio elegido debe adaptarse a los requisitos de entorno y costo, además de a los operacionales del sistema. Lo primero que hay que considerar en un medio de transmisión es si soportará las velocidades de transmisión que se esperan de la red.

Un segundo aspecto de la elección del medio de comunicación es el costo en función de la longitud y de la conexión. Los medios tradicionales, como el cable de par torcido o el coaxial, se están reemplazando por nuevos portadores, como fibras ópticas, cuyo costo desciende con la misma rapidez con que avanza esa tecnología.

Otro elemento importante en la elección del portador es la facilidad de instalación y mantenimiento. Una red debe ser fácil de extender añadiéndole nodos y por lo tanto longitudes adicionales al medio. La facilidad de instalación y mantenimiento también reducirá el costo total del sistema.

A continuación se tratarán los distintos medios de transmisión a tener en cuenta para una red de comunicaciones.

Par de cables torcidos

Un tipo de cable comúnmente usado en las redes actuales se llama *par torcido*. Un par torcido tiene dos hilos entrelazados con una inclinación calculada para reducir los efectos de la interferencia electromagnética que generan las señales de alta frecuencia transmitidas. Este tipo de medios de comunicación puede soportar frecuencias de transmisión de datos hasta 100 MHz sin un grado de atenuación alto. Se pueden extraer los datos de la señal recibida después de haber sido transmitida a lo largo de varios cientos de metros de cable. En el lado receptor se utiliza un amplificador para reforzar la señal (figura 1.2).

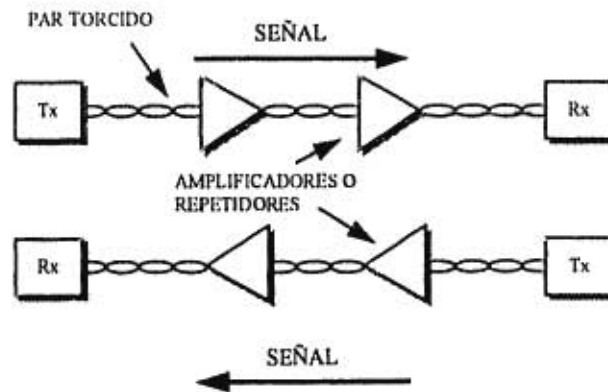


FIGURA 1.2 CABLE DE PAR TORCIDO

Una gran ventaja del par torcido como medio de transmisión es que resulta más barato y fácil de instalar. El costo solía relacionarse con el del cobre que se usaba como conductor, pero ahora se usan aleaciones baratas con buenas propiedades de conducción. La instalación de nuevos pares de tramos es sencilla. En general, habrá un enchufe estándar adecuado para determinada red y cada sección del medio tendrá uno conectado a cada extremo. Por tanto, la extensión de la red sólo implicará la separación y unión de enchufes.

CAPITULO I. REDES

El par torcido se puede clasificar en dos tipos: El par torcido blindado (STP, Shielded Twisted Pair) y el par torcido sin blindar (UTP, Unshielded Twisted Pair).

El cable STP ha llegado a ser bastante popular, el cable STP tiene algunas características mejores que el UTP, tales como la resistencia a la adición de ruido y a la alta velocidad de transmisión de datos. El cable STP puede proveer confiablemente transmisión de datos por encima de 100 Mbps a distancias por encima de 1000 metros.

El cable UTP, conocido de otra manera, ordinariamente como cable telefónico, ha sido usado tradicionalmente para transmisión de voz y de datos a baja velocidad. Este puede ser plano o redondeado, este cable UTP no puede lograr velocidades ni la inmunidad al ruido como el STP, pero es más barato que este. Otro factor a considerar sobre este cableado es que requiere hardware adicional tal como filtros y equalizadores.

La EIA/TIA ha definido la especificación EIA/TIA 568 para estandarizar la instalación y premisas del cableado. Esta especificación define los siguientes niveles de par torcido.

NIVEL 1	UTP, TRADICIONAL CABLE TELEFONICO, ESTE ES USADO PARA TRANSMISION DE VOZ PERO NO PARA DATOS
NIVEL 2	UTP, CERTIFICADO PARA TRANSMISION A 4 Mbps, SIMILAR AL SISTEMA DE CABLEADO TIPO 3 DE IBM.
NIVEL 3	SOPORTA VELOCIDADES DE TRANSMISION DE 10 Mbps Y ES USADO POR REDES TOKEN RING (4 Mbps) Y ETHERNET 10 BASE-T(10 Mbps)
NIVEL 4	ESTA CERTIFICADO PARA VELOCIDADES DE TRANSMISION DE 16 Mbps Y ES USADO PARA TOKEN RING (16 Mbps)
NIVEL 5	ESTE CABLE SOPORTA VELOCIDADES DE 100 Mbps Y ES USADO POR TECNOLOGIAS TALES COMO FAST ETHERNET Y ATM.

TABLA 1.1 NIVELES DE UTP DEFINIDOS POR LA EIA/TIA

Fibra óptica

Durante los últimos años se han obtenido resultados significativos en el campo de los sistemas de transmisión ópticos. Se han puesto en servicio numerosos sistemas de transmisión utilizando fibra óptica. Esto es debido a las mejoras en la fabricación de fibras ópticas y de cables, el desarrollo de nuevas técnicas de evaluación de los cables de fibra óptica y el establecimiento de normas de diseño de los mismos.

Transmisión Por Fibra Optica

En la figura (1.3) se ilustra en forma esquemática la construcción básica de un sistema de transmisión por medio de cable de fibra óptica. En un sistema de transmisión óptico, la fuente óptica y el detector, que operan como conversores (eléctrico/óptico), así como la fibra óptica, son los elementos básicos más importantes. En especial, cumple un papel muy importante en la construcción del sistema, el desarrollo de diodos láser tan pequeños en tamaño como transistores.

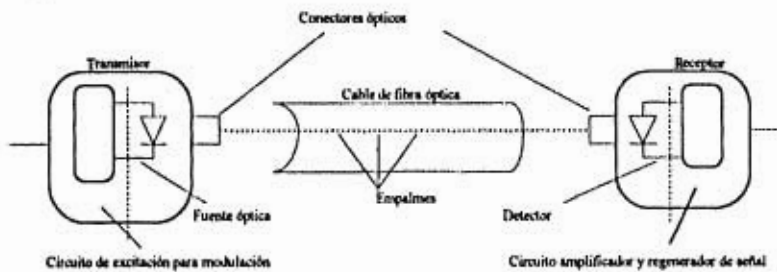


FIGURA 1.3 CONSTRUCCION BASICA DE UN SISTEMA DE TRANSMISION CON F.O.

Las principales características de un cable de fibra óptica son las siguientes:

- (1) El cable de fibra óptica posee muy bajas pérdidas en comparación con los cables convencionales. En consecuencia la separación entre repetidores en una línea de transmisión óptica puede ser varias veces mayor a la necesaria en el caso de cables comunes.

(2) Es de reducido tamaño y tiene una amplia respuesta en frecuencia. Pueden propagarse simultáneamente en una fibra, ondas ópticas de varias longitudes de onda. Se cuenta, en definitiva, con una capacidad de transmisión sumamente elevada.

(3) Puede tener una línea de transmisión altamente confiable ya que la fibra no es afectada por acoplamientos eléctricos ni magnéticos debidos a cables de tensión o fenómenos atmosféricos.

(4) Pueden fabricarse cables muy livianos ya que el peso específico del vidrio es la cuarta parte del que tiene el cobre.

Todos estos rasgos característicos del cable de fibra óptica se han dado comparados con los de un cable convencional. A diferencia de los cables convencionales, la fibra óptica mantiene características de transmisión de banda ancha y reducidas pérdidas, independientemente del tamaño, debido a una reducción de impurezas y con un estricto control del índice de refracción. Se han obtenido tales resultados tras mejorar el proceso de fabricación de la fibra.

Estructura básica y clasificación del cable de fibra óptica

En la figura 1.4 se esquetmatiza la estructura de la fibra. En ella se observa que dentro de la fibra se distinguen dos regiones con diferentes índices de refracción.

Una de ellas, en el interior de la fibra, constituye el denominado núcleo (core), mientras que la otra, que recubre la anterior, es llamada revestimiento (cladding). Es necesario que el índice de refracción n_1 del núcleo sea mayor que el n_2 correspondiente al revestimiento.

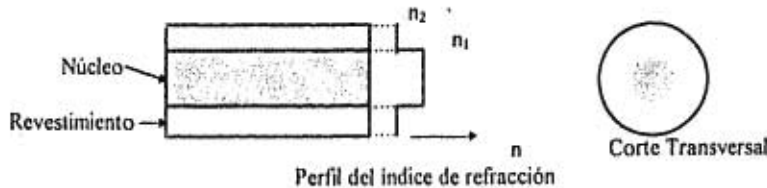


FIGURA 1.4 ESTRUCTURA DE LA FIBRA OPTICA

Teoría de la propagación de la fibra óptica

La conducción de la luz se basa en un parámetro del material que la conduce, conocido como índice de refracción. Este índice se define de la siguiente forma:

$$n = \text{vel. de la luz en el vacío} / \text{vel. de la luz en el material}$$

Las bases para la conducción de la luz en una fibra óptica se ilustran en la figura 1.5. En esta figura se observa la frontera que separa un material con un índice de refracción n_1 de otro con un índice de refracción n_2 , con $n_1 > n_2$.

Considérese primero la geometría de la figura 1.5a donde la luz se dirige del material 1 al material 2. En la frontera parte de la luz se refleja hacia el material 1. La parte restante cruza la frontera como "refractado" que viaja con un ángulo θ_2 . La ley de Snell proporciona una relación entre los ángulos de incidencia y de refracción:

$$n_1 \text{ sen } (\theta_1) = n_2 \text{ sen } (\theta_2)$$

Si el material 1 representa el núcleo de la fibra, entonces, la luz reflejada no se pierde y la luz refractada abandona el material.

Aunque bajo estas condiciones se produce algún tipo de conducción de la luz, la pérdida de potencia óptica es grande.

Si el ángulo θ_1 aumenta, se alcanza un punto en el cual no existe el rayo refractado. Se trata del ángulo crítico θ_c , que define el punto en el cual se produce la reflexión total en la frontera. En la figura 1.5b se ilustra esta condición, con $\theta_2 = 90^\circ$. Todos los rayos de luz con un ángulo de incidencia mayor que el ángulo crítico son totalmente reflejados, como se muestra en la figura 1.5c. Si el material 1 (el núcleo de la fibra) está rodeado por una segunda capa (el revestido), entonces la luz que viaja dentro del cono definido por el ángulo crítico se encuentra atrapada y puede ser conducida por la fibra. Esta es la propiedad que es fundamental para la propagación de la luz por una fibra óptica. Si $n_1 < n_2$ el ángulo crítico no existe, por lo que las pérdidas de la potencia óptica son elevadas.

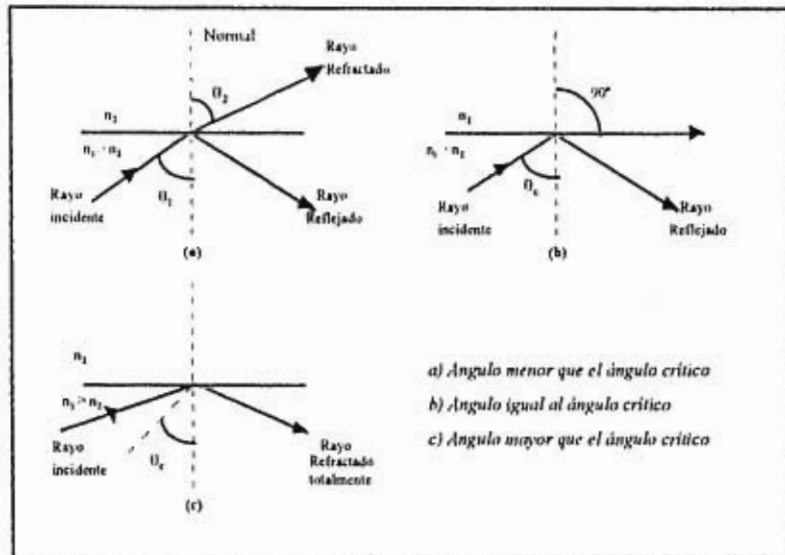


FIGURA 1.5 REFLEXION Y REFRACCION DE LA LUZ EN UNA FRONTERA, SEGUN EL ANGULO DE INCIDENCIA.

La ley de Snell indica que la refracción no puede tener lugar cuando el ángulo de incidencia es muy grande (por ejemplo, cuando la luz viaja de un índice alto a un índice menor). Si el ángulo de incidencia excede el valor crítico, en donde el seno del ángulo es igual a 1, la luz no se refracta. Todo el rayo es reflejado cuando el ángulo de incidencia es más grande que el ángulo crítico. Este fenómeno se llama Reflexión Interna Total y mantiene a la luz confinada dentro de una fibra óptica. El ángulo crítico, con el cual se da lugar a la reflexión interna total se deriva de la ley de Snell:

$$\text{Angulo crítico} = \text{seno}^{-1} (n_2/n_1)$$

Dicho fenómeno puede observarse frecuentemente, por ejemplo en el límite entre el aire y el agua. De esta manera, aquella onda óptica con un reducido ángulo de propagación con respecto al eje de la fibra, queda confinada en el núcleo y se propaga a lo largo de dicho eje.

En general, el ángulo crítico en las fibras ópticas utilizadas para la transmisión varía entre 75° y 85° . Esto significa que pueden transmitirse a través de las fibras aquellas ondas ópticas con ángulos de propagación entre 0° y 15° .

Aún cuando la fibra es doblada, con un radio de curvatura grande, la onda se propaga sin pérdidas apreciables. Sin embargo, a medida que el radio de curvatura es reducido, las pérdidas aumentan considerablemente. Esto se debe a que, cuando el ángulo de propagación es cercano a $\pi/(2-0_c)$, en la porción curvada se excede dicho valor y la onda óptica se interna en la región del revestimiento provocando las pérdidas.

El número de modos que se propagan en la fibra se determinan según: la longitud de onda óptica, la diferencia del índice de refracción entre el núcleo y el revestimiento, perfil del índice de refracción del núcleo, y dimensiones del núcleo. La fibra que admite un solo modo se denomina fibra de modo único (single-mode fiber) y aquella que admite varios modos se llama fibra multimodo (multimode fiber). La tabla 1.2 resume los rasgos característicos de las fibras de modo único y multimodo desde el punto de vista estructural y características de transmisión.

	FIBRAS DE MODO ÚNICO	FIBRAS MULTIMODO	
		INDICE ESCALON	INDICE GRADUAL
DIAMETRO DEL NUCLEO	ALGUNOS μm	40-100 μm	40-100 μm
ANCHO DE BANDA DE LA FRECUENCIA DE BANDA BASE	MAYOR DE 10GHz. Km	10-50 GHz.km	HASTA ALGUNOS GHz.km
FACILIDAD DE EMPALME	DIFÍCIL (0.1 μm)	RELATIVAMENTE SENCILLO (1 μm)	RELATIVAMENTE SENCILLO (1 μm)

TABLA 1.2 COMPARACION DE LAS FIBRAS OPTICAS SEGUN EL MODO DE TRANSMISION

Según el tipo de perfil del índice de refracción del núcleo, la fibra multimodo se clasifica en índice escalón (step-index) figura 1.6 e índice gradual (graded-index) figura 1.7. La fibra de índice gradual, que tiene un perfil casi parabólico, posee características de banda ancha ya que en tal tipo de fibras las diferencias de velocidad de propagación entre modos son pequeñas.

En general los diámetros del revestimiento y del núcleo de la fibra oscilan entre 100 y 300 micrómetros y 5 a 100 micrómetros respectivamente. Para fibra multimodo de índice gradual se ha adoptado en forma internacional 125 micrómetros para el diámetro del revestimiento y 62.5 micrómetros para el diámetro del núcleo.

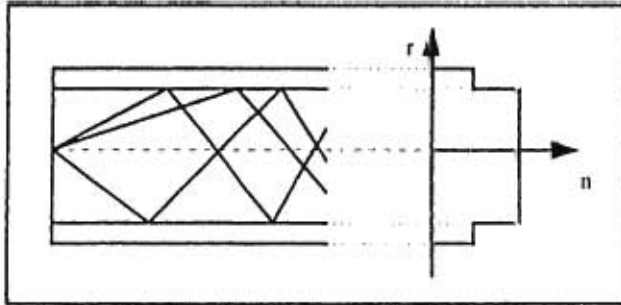


FIGURA 1.6 DIFERENTES TRAYECTORIAS DE PROPAGACION Y PERFIL DEL INDICE DE REFRACCION DE LAS FIBRAS MULTIMODO DE INDICE ABRUPTO

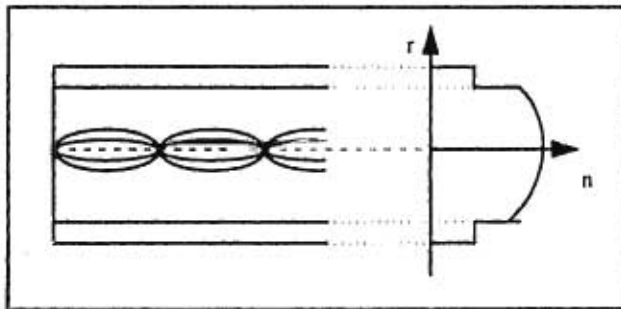


FIGURA 1.7 DIFERENTES TRAYECTORIAS DE PROPAGACION Y PERFIL DE INDICE DE REFRACCION DE FIBRAS MULTIMODO DE INDICE GRADUAL

Características de transmisión en la fibra óptica

Las principales características de transmisión en la fibra óptica son:

(I) pérdida óptica:

- I.a - pérdida óptica intrínseca de la fibra óptica
- I.b - pérdida debido a curvatura de la fibra
- I.c - pérdida de conexión de fibras
- I.d - pérdida de acoplamiento entre fibras y dispositivos ópticos, fuente óptica a la entrada y detector a la salida.

(II) respuesta en frecuencia de la banda base

I.- Pérdidas en la transmisión de la fibra óptica:

Las pérdidas intrínsecas en la fibra son debidas a la dispersión y a la absorción de las ondas ópticas que se propagan en la fibra. Los principales factores son:

1) Dispersión de Rayleigh.- se debe a fluctuaciones microscópicas del índice de refracción en el núcleo, siendo estas pérdidas inversamente proporcionales a λ^4 .

2) absorción debida a impurezas tales como iones OH e iones metálicos de transición. Sin embargo recientes mejoras en la tecnología de fabricación de las fibras, que previenen la introducción de iones OH en la fibra, reducen considerablemente las pérdidas.

3) absorción intrínseca en las regiones infrarroja y ultravioleta.

4) radiación y dispersión debidas a imperfecciones en la estructura de la fibra.

II.- Respuesta en frecuencia de banda base.

La respuesta en frecuencia de banda base es otro de los factores importantes en el diseño de un sistema de transmisión óptico.

Con el objeto de entender claramente las dispersiones de la fibra óptica, se han esquematizado en la figura 1.8 los modos de propagación sujetos a las dispersiones. La limitación de ancho de banda es equivalente a la dispersión de pulsos de señal de transmisión que surgen debido a la diferencia en la velocidad de grupo.

Se observa en la figura 1.8; (a) la señal tal como se inyecta a la fibra; (b) forma del pulso óptico después de que se ha propagado una distancia relativamente corta en la fibra y (c) el ensanchamiento es tan grande que se detecta otra secuencia de bits.

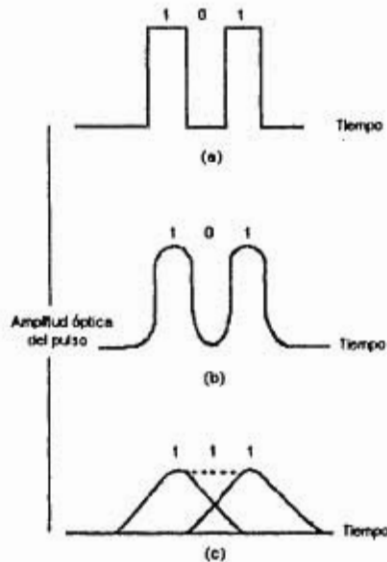


FIGURA 1.8 EFECTO DEL ENSANCHAMIENTO DEL PULSO EN LA DETECTABILIDAD DE UN PATRÓN DE PULSOS ÓPTICOS QUE SE PROPAGA POR UNA FIBRA.

La dispersión de modo es la diferencia de velocidad de grupo entre modos, siendo éste un rasgo característico de las fibras multimodo. Las ondas ópticas correspondientes a cada modo se propagan por diferentes caminos, uno de otro, siendo diferentes los instantes en que llegan a la salida cada una de las ondas. En consecuencia un pulso agudo a la entrada se transforma en un pulso ancho.

Para una fuente luminica que tiene simultáneamente diferentes componentes de longitud de onda, la dispersión del material provoca cambios en la velocidad de grupo. Usando tal fuente luminica, un pulso de entrada agudo se transforma en uno ancho tal como se observa en la figura 1.8. Este fenómeno es el principal limitador de un ancho de banda en una fibra de modo único.

El ensanchamiento del pulso en el dominio del tiempo equivale a una atenuación de las componentes de alta frecuencia en el dominio de las frecuencias. Es de notar que las pérdidas en las componentes de alta frecuencia no arrastran pérdidas de energía en la fibra óptica.

Cable coaxial

El cable coaxial es otro medio típico de transmisión. Hay dos tipos de cable coaxial que se utilizan con frecuencia, uno de ellos es el cable de 50 Ohms, que se utiliza en la transmisión digital y se conoce como coaxial de banda base; en tanto que el otro tipo, el cable de 75 Ohms que se emplea en la transmisión analógica es el coaxial de banda ancha.

El cable coaxial consta de un alambre de cobre duro en su parte central, es decir, que constituye el núcleo, el cual se encuentra rodeado por un material aislante. Este material aislante está rodeado por un conductor cilíndrico que frecuentemente se presenta como malla de tejido trenzado. El conductor externo está cubierto por una capa de plástico protector en la figura 1.9 se muestra un corte de un cable coaxial.

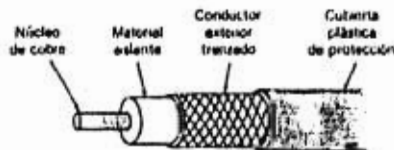


FIGURA 1.9 CORTE DE UN CABLE COAXIAL.

Coaxial de banda base

La construcción del cable coaxial produce una buena combinación de un gran ancho de banda y una excelente inmunidad al ruido. El ancho de banda que se puede obtener depende de la longitud del cable; para cables de 1 km, por ejemplo, es factible obtener velocidades de datos de hasta 10 Mbps, y cables de longitudes menores, es posible obtener velocidades superiores. Se pueden utilizar cables con longitudes mayores, pero se obtienen velocidades más bajas. Los cables coaxiales se emplean ampliamente en redes de área local y para transmisiones de larga distancia del sistema telefónico.

Aunque, algunas veces se utilizan señales binarias, en cables coaxiales, de forma directa (por ejemplo, 1 volt para representar un valor de 1 y, 0 volts para representar el valor de 0), este método no ofrece al receptor un medio para determinar el momento en el que cada bit empieza y termina; por esta razón se prefiere usar una técnica denominada *codificación Manchester*, o una técnica relacionada llamada *codificación diferencial Manchester*. Con la codificación Manchester cada periodo de bit se divide en dos intervalos iguales. Un bit binario con valor 1 se envía con un voltaje alto durante el primer intervalo y bajo durante el segundo. Un bit de valor 0 es precisamente lo contrario: es decir, primero se tiene un voltaje bajo y después uno alto. Con este esquema se asegura que todos los periodos de bit tengan una transición en la parte media, propiciando así un excelente sincronismo entre el transmisor y el receptor.

La codificación diferencial Manchester es una variación de la codificación Manchester básica, pues en ella, un bit con valor 1 se indica con la ausencia de transición al inicio del intervalo, y un bit con valor de cero se indica por la presencia de una transición al inicio del intervalo. En ambos, casos existe una transición en la parte media. El esquema diferencial exige un equipo más sofisticado, pero ofrece una mayor inmunidad al ruido. La figura 1.10 muestra estos tipos de codificación.

Coaxial de banda ancha

El sistema que considera el otro tipo de cable coaxial emplea la transmisión analógica. Los cables pueden emplearse para aplicaciones que necesiten hasta 300 MHz (y en algunos casos hasta los 450 MHz) gracias a la naturaleza analógica de la señal, que es menos crítica que la del tipo digital.

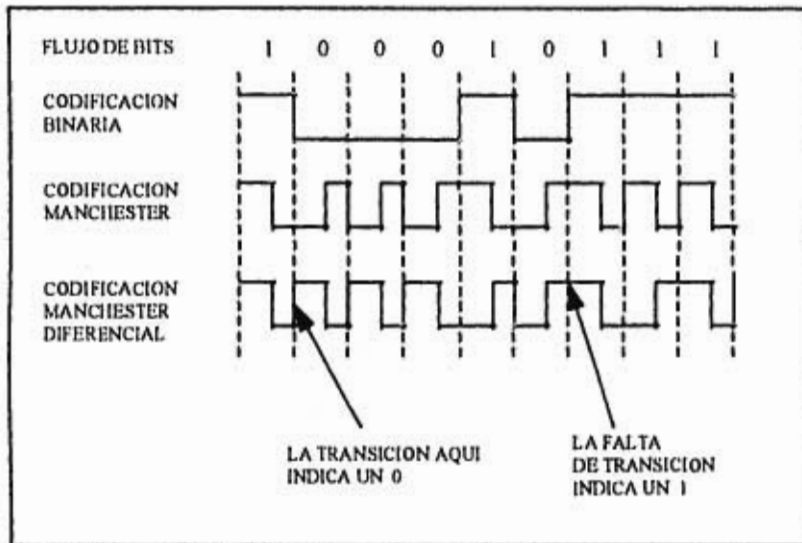


FIGURA 1.10 CODIFICACION MANCHESTER Y MANCHESTER DIFERENCIAL

Para transmitir señales digitales en una red analógica, cada interface debe tener un dispositivo electrónico que convierta en señal analógica el flujo de bits de envío, y otro para convertir la señal analógica que llega en un flujo de bits. En general se pueden citar las siguientes características del cable coaxial de banda ancha:

- Se usa FDM.
- Todas las señales son HDX, pero usando dos canales se obtiene FDX.
- Mejor inmunidad al ruido que el de banda base.
- Es un medio resistente que no necesita conducto.
- Se combina voz, datos y vídeo simultáneamente.
- Su costo es alto, se necesitan modems en cada estación del usuario, lo que aumenta aún más su costo.

Enlaces de microondas

Un enlace de microondas realiza casi las mismas funciones que un cable de fibra óptica, pero en diferente forma, usando transmisión de microondas punto a punto entre repetidores. La mayoría de los enlaces operan en la región entre 4 y 6 GHz, mas sin embargo algunos enlaces operan a frecuencias por debajo de los 2 GHz y otros operan a frecuencias superiores a los 13 GHz. La propagación es por supuesto por medio del aire y por lo tanto esta limitada a que exista línea de vista. Consecuentemente el espaciamiento típico entre repetidores es alrededor de 50 Km, debido a la alta atenuación a grandes distancias a las que las ondas de radio están sujetas.

Una terminal de microondas tiene similitudes con una terminal de cable coaxial. Por ejemplo, el equipo multiplexor es muy similar, mientras que el sistema de cable utiliza un determinado número de pares de cable, el sistema de microondas utiliza un número de portadoras a diferentes frecuencias dependiendo el ancho de banda del sistema. El efecto es muy similar un espacio entre las portadoras se usa como un rango de protección en caso de fallas. Finalmente hay interconexiones en la terminal al otro sistema de cable o de microondas, local o por una troncal.

Como se ve, las similitudes están en lo que se hace, y las diferencias en como se hace. Esencialmente, los repetidores reciben una señal de microondas modulada desde otro repetidor y la transmite al siguiente, se tiene una cadena idéntica para trabajar en la dirección contraria, la única diferencia aquí es que la transmisión en las dos direcciones es la frecuencia para evitar la interferencia; la diferencia en frecuencia es típicamente de unos cuantos cientos de megahertz en las frecuencias que operan entre los 4 y 6 GHz.

Un típico enlace de microondas consiste en varios repetidores entre los puntos terminales, y por supuesto el ruido se adhiere en cada salto por lo que existe una limitante en cuanto a saltos que por recomendación no deben de exceder los 56 saltos. Uno no debe perder de vista el hecho de que el uso de receptores más sensibles permiten reducir la potencia de transmisión, esto permitiría reducir el costo y tamaño de los repetidores.

Las antenas que mas frecuentemente se usan son aquellas que tienen reflectores parabólicos, ya que tienen una alta densidad de enlace y su diseño permite grandes anchos de banda y bajo ruido, además de tener la gran ventaja de utilizar frecuencias iguales con la separación de las señales mediante la polarización vertical y horizontal.

La potencia con la que se transmite varia, dependiendo del ancho de banda, el número de circuitos por portadora y la distancia hacia el siguiente repetidor. En la mayoría de los casos se utilizan potencias entre 0.25 y 10 Watts, siendo las potencias entre 2 y 5 W las más comunes. Para potencias entre 1 y 5 W, a frecuencias que no excedan los 6 GHz, se utilizan amplificadores de salida, mientras que con las potencias de 0.5 W o menores no es necesario un amplificador de salida, en su lugar se puede utilizar un oscilador de potencia.

El número típico de portadoras en un enlace de microondas es por lo menos 4 y algunas veces se llega hasta 12. Normalmente hay entre 600 y 2700 canales por portadora. En lugares difíciles, se utiliza la diversidad, en esos casos la mas común es la diversidad de espacio incorporando pares de antenas en la misma dirección.

Ahora veremos el caso cuando se quiere transmitir datos digitales utilizando señales analógicas, quizás el caso mas conocido es el módem cuando se utiliza en la red telefónica publica, una desventaja de este caso es que se tiene el limitante del ancho de banda de las líneas telefónicas, que están diseñadas para transmitir señales de voz que no pasan de los 4 KHz. Para transmisión de datos a mayores velocidades se utilizan las microondas, por lo que es necesario utilizar técnicas de codificación o modulación digital a altas frecuencias.

• Sabemos que la modulación es la variación de alguna característica de una señal portadora: amplitud, frecuencia o fase. De acuerdo con estas características se tienen tres principales técnicas de modulación digital:

- ASK (Amplitude-Shift Keying)
- FSK (Frequency-Shift Keying)
- PSK (Phase-Shift Keying)

CAPÍTULO I. REDES

En ASK, los dos valores binarios son representados por dos diferentes amplitudes de la señal portadora. Comúnmente, uno de los valores es cero, es decir, uno de los valores está representado por una señal de amplitud constante de la portadora y el otro valor está representado por la ausencia de señal portadora. La señal resultante es:

$$s(t) = \begin{cases} A \cos(2\pi f_c t + \theta_c) & \text{binario 1} \\ 0 & \text{binario 0} \end{cases}$$

ASK es una técnica susceptible a repentinas ganancias y por lo tanto es una técnica de modulación algo ineficiente.

En FSK, los dos valores binarios son representados por dos señales diferentes en frecuencia, la señal resultante es:

$$s(t) = \begin{cases} A \cos(2\pi f_1 t + \theta_c) & \text{binario 1} \\ A \cos(2\pi f_2 t + \theta_c) & \text{binario 0} \end{cases}$$

Donde f_1 y f_2 son frecuencias separadas en magnitudes iguales de la frecuencia portadora f_c .

FSK es menos susceptible a errores que ASK, es comúnmente usada en altas frecuencias (3 a 30 MHz) para transmisión de radiofrecuencias, aunque se puede usar a mayores frecuencias para transmisiones de datos en redes.

En PSK, la fase de la señal portadora es alterada para representar un dato, en este sistema, un 0 binario está representado por una señal de la misma fase que la anterior y un 1 binario está representado por una señal defasada un ángulo π de la señal anterior. Esto es conocido como PSK diferencial, ya que el defasamiento es con relación a la señal anterior y no con una señal de referencia. La señal resultante es:

$$s(t) = \begin{cases} A \cos(2\pi f_c t + \pi) & \text{binario 1} \\ A \cos(2\pi f_c t) & \text{binario 0} \end{cases}$$

Se puede hacer un mejor uso del ancho de banda si cada elemento de la señal representa más de un bit. Por ejemplo, en lugar de un defasamiento de 180 grados, que es el mas común, se puede usar una técnica de codificación conocida como QPSK (*quadrute phase-shift keying*) que utiliza defasamientos múltiples de 90 grados.

$$s(t) = \begin{cases} A \cos(2\pi fct + 45) & 11 \\ A \cos(2\pi fct + 135) & 10 \\ A \cos(2\pi fct + 225) & 00 \\ A \cos(2\pi fct + 315) & 01 \end{cases}$$

De este modo cada elemento de la señal representa dos bits en vez de uno aprovechando mejor el ancho de banda. Este esquema se puede extender, es posible transmitir tres bits al mismo tiempo utilizando ocho diferentes angulos de defasamiento.

Estas son las tres técnicas básicas de codificación digital a analógico, la figura 1.11 muestra los tres tipos.

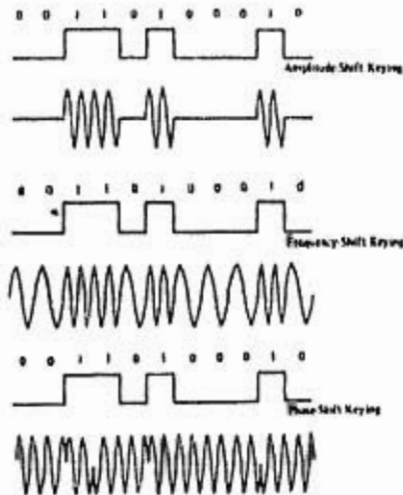


FIGURA 1.11 MODULACION DIGITAL.

1.2.5 ANCHO DE BANDA

Las redes de comunicaciones sólo pueden transportar rangos específicos de frecuencias y esto depende en gran medida del medio de transmisión ya sea par torcido, cable coaxial, microondas, fibra óptica, etc.

El ancho de banda es básicamente la medida de la capacidad de la portadora de un enlace de transmisión, se trata de un elemento de capital importancia en el diseño de redes, puesto que la capacidad de un canal está en relación directa con su ancho de banda, como puede verse en la siguiente ecuación, que es la expresión de capacidad de Shannon.

$$C = W \log_2 \left(1 + \frac{S}{N} \right) bps$$

Donde:

- C : Capacidad de canal
- W: Ancho de banda
- S/N: Relación señal a ruido

En la figura 1.12 se puede ver fácilmente la atenuación que presentan diferentes medios de transmisión para diferentes anchos de banda.

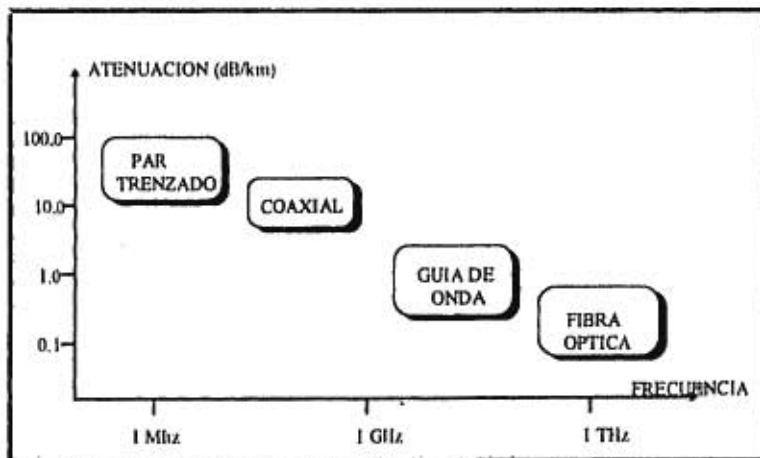


FIGURA 1.12 RELACION ENTRE LOS MEDIOS DE TRANSMISION Y EL ANCHO DE BANDA

La fibra óptica transmite información de tipo digital, cuando un pulso de luz viaja por la fibra, se ensancha por factores propios de la transmisión. Este fenómeno puede verse en la figura 1.13.



FIGURA 1.13 ENSANCHAMIENTO DEL PULSO

Este ensanchamiento es el que limita la velocidad de transmisión, dado que es necesario separar más los pulsos para poder distinguirlos. La siguiente ecuación relaciona el ancho de banda W con el ensanchamiento del pulso (Δt), medido a mitad de altura.

$$W = \frac{0.44}{\Delta t}, \text{ medido en MHz por Km}$$

Las fibras ópticas operan cerca de la región infrarroja del espectro de frecuencias a 10^{14} ciclos por segundo; las frecuencias en esta región son de 30 a 400 THz. El cable telefónico usado en la era predigital, operaba a frecuencias de hasta 4 KHz, por esta razón los enlaces con fibra óptica reemplazaron a los enlaces con cable telefónico, debido a su capacidad de transportar miles de veces más tráfico.

La tabla 1.3 resume las características de estos medios de transmisión, resaltando la enorme diferencia que existe en el ancho de banda.

CARACTERISTICA	PAR TORCIDO	FIBRA OPTICA
PESO (Kg/Km)	50	30-170
COSTO	BAJO	ALTO
INTERFERENCIA	ALTA	NINGUNA
ANCHO DE BANDA	1.5 -100 MHz	>150 MHz
SEGURIDAD	BAJA	ALTA

TABLA 1.3 COMPARACION ENTRE PAR TORCIDO Y FIBRA OPTICA

CAPITULO I. REDES

El cable coaxial opera con anchos de banda de 10 MHz. para cable de banda angosta y hasta 400 MHz. para cable de banda ancha, el cable coaxial presenta mayor inmunidad al ruido que el par torcido, y es más barato que la fibra óptica. La tabla 1.4 compara las principales características de los dos tipos de cable coaxial.

CARACTERISTICA	COAXIAL BANDA BASE	COAXIAL BANDA ANCHA
PESO (Kg/Km)	75 - 750	150 - 500
COSTO	MEDIO	ALTO
INTERFERENCIA	MEDIA	BAJA
ANCHO DE BANDA	10 - 16 MHz	400 MHz
SEGURIDAD	ALTA	ALTA

TABLA 1.4 COMPARACION ENTRE LOS DOS TIPOS DE CABLE COAXIAL.

Las señales de microondas tienen un rango de frecuencias desde 2 hasta 25 GHz, este rango de 20 GHz es usado y dividido para transportar muchos canales a la vez. Los satélites operan básicamente con dos frecuencias, la frecuencia baja, banda C (4 y 6 GHz) y la alta frecuencia, banda Ku (11 y 14 GHz) la cual es digital.

Por último, en la figura 1.14 se presenta para cada tipo de aplicación su ancho de banda.

TIPO	ANCHO DE BANDA
CONEXION CON MODEM	1,200 28,800 bps
TRANSFERENCIA DE ARCHIVOS CON EL PUERTO SERIAL	2,000 bps
ENLACE RED WAN	64,000 bps
PUERTO PARALELO	300,000 bps
T1 DIGITAL	1.544 Mbps
RED LAN ARCNET	2.5 o 20 Mbps
RED TOKEN RING	4 o 16 Mbps
RED ETHERNET	10 o 100 Mbps
T3 DIGITAL ENLACE WAN	44.184 Mbps
INTERFASE SERIAL DE ALTA VELOCIDAD	52 Mbps
FDDI	100 Mbps
SONET	51.9 Mbps A 2.5 Gbps
ATM	HASTA 400 Mbps

FIGURA 1.14 ANCHO DE BANDA PARA DIFERENTES APLICACIONES

CAPITULO II

REDES LAN

2.1 DEFINICION DEL CONCEPTO

2.1.1 INTRODUCCION

En los últimos veinte años, la industria de las comunicaciones ha centrado su atención en sistemas que transportan datos a largas distancias. La industria de las redes de gran cobertura (WAN) ha madurado y es hoy por hoy un sector estable. Las redes locales (LAN), por el contrario constituyen un campo relativamente nuevo.

La tecnología en que se basan empezó a adquirir interés a mediados de los setenta, y es en la actualidad uno de los sectores de más rápido crecimiento dentro de la industria de comunicación de datos. Una red de área local LAN (Local Area Network) parece ser el "mamut" de la conectividad, pero su antigüedad no implica su obsolescencia, por el contrario las redes de área local se han convertido en la base de las redes de área amplia WAN (Wide Area Network), de las redes de área global GAN (Global Area Network), de las redes metropolitanas MAN (Metropolitan Area Network) y de la misma supercarretera que pretende comunicar al mundo a través de una red global.

2.1.2 CONCEPTO DE REDES LAN

Esta red está compuesta por un conjunto de computadoras que se comunican entre sí en una área geográficamente limitada, como puede ser un edificio. La idea básica de una red de área local es facilitar el acceso a todos los equipos terminales de datos y poder compartir recursos de software y hardware. Por ejemplo se pueden adquirir versiones para red de software muy populares, con un ahorro bastante considerable si se compara con su costo al comprar copias con licencia individual. Se pueden compartir recursos de la red, como ejemplos de estos recursos se encuentran impresoras, trazadores de planos (plotters), dispositivos de almacenamiento de datos e incluso otros sistemas informáticos.

Con un sistema de red no es necesario que se adquiera, por ejemplo, varias impresoras ni varios paquetes de software de la misma aplicación; bastará con indicar al sistema cuantas personas podrán hacer uso de los dispositivos y aplicaciones.

Otro fin de las redes LAN es la comunicación sin pérdida de tiempo, en ocasiones se tiene que cazar al personal, en un sistema de red estos problemas desaparecen con el uso de correo electrónico. Otro factor muy importante es la seguridad, los sistemas operativos de red ofrecen elementos de seguridad avanzados que aseguran que los archivos y recursos van a estar protegidos de usuarios sin autorización.

Principales atributos de una red local

- Las conexiones entre las estaciones de Trabajo suelen tener longitudes comprendidas entre algunos metros y varios kilómetros.
- La capacidad de transmisión de una red local suele ser mayor que la de una red extensa.
- Las velocidades de transmisión suelen estar comprendidas entre 1 Mbps hasta 100 Mbps.
- El canal de la red local suele ser propiedad de la misma organización que utiliza la red. Por lo general las compañías telefónicas no intervienen en su propiedad ni en su gestión.
- La tasa de errores de una red local suele ser considerablemente menor que la del canal telefónico orientado a redes extensas (aunque las redes de fibra óptica constituyen la excepción a esta regla).

2.1.3 COMPONENTES DE UNA RED LOCAL

Los componentes principales de una red LAN son:

El servidor (server): es una computadora con gran capacidad de procesamiento que se encarga de administrar y compartir los recursos de la red y en el que reside el sistema operativo con el que se trabaja. La labor principal del servidor es descargar las tareas de las computadoras que se encuentran conectadas en red. Un servidor puede contener programas y datos que todos los usuarios de la red pueden compartir y puede estar dedicado sólo a proveer las necesidades de los usuarios u operar como otra estación de trabajo más, aunque esto no es muy recomendable.

Estación de trabajo: Es una máquina de usuario, que en ocasiones puede funcionar como una computadora personal. Se encuentra interconectada por medio de una tarjeta de interface que permite que se comunique con otras estaciones.

Tarjeta de interface: Va instalada dentro de una micro, y según su especificación, cada tarjeta determina, la topología de cada red.

Canal de comunicación: Por lo general es un cable dedicado a las comunicaciones, este canal de comunicación determina la velocidad máxima de transferencia de información.

Repetidores: En algunos casos por las distancias entre las unidades de la red, son necesarios para reforzar la señal.

Sistema operativo de red: Es el software, base de control bajo el que se trabaja, tal como Netware, LAN Manager, OS/2, LANtastic, etc. Este sistema reside en el servidor y cada estación de trabajo cuenta con un componente del software que permite que una aplicación sea leída y se puedan escribir datos en el servidor desde la máquina local que se esté utilizando.

2.2 DEFINICION DE PARAMETROS

Antes de hablar de parámetros tales como topologías, cableado y ancho de banda para una red LAN, es conveniente hacer una breve descripción sobre algunos tipos de redes LAN existentes en el mercado. A la fecha existen tres tecnologías líderes en la base instalada mexicana; además de otros nombres, que por su poca presencia, no se consideran dentro del estándar que han marcado Ethernet, Token Ring y Arcnet.

Arcnet

Arcnet está aún presente en la pequeña y mediana empresa, Arcnet usa una topología de anillo que corre a 2.5 Mbps. Permite la conexión de 1 a 255 nodos, cumple con la norma IEEE 802.4 y usa el protocolo token passing.

En esta tecnología la información viaja de manera lógica y cíclica, por lo que el tiempo de respuesta no es muy atractivo y el tráfico es común, además de que cada estación o nodo debe esperar su turno para poder ejecutar su proceso, pues se encuentran conectados físicamente en orden y la conexión inicia en la misma estación donde termina. Por ello, cuando una estación deja de funcionar el token de la red se paraliza.

En la actualidad Arcnet, ha perdido popularidad y cede ante una topología de anillo modificado como Token Ring, donde la falla de una estación no implica la caída de la red. Arcnet trabaja en armonía en ambiente de oficina donde la carga de información no es muy grande o donde el procesamiento es similar para los 25 ó 40 usuarios que pueden acceder a esta red.

Es una buena opción para aplicaciones que no requieren un tiempo de respuesta inmediato y por su diseño, es ideal para aquellas estructuras donde se dificulta la instalación de cableado. Pero con todo esto, los conocedores auguran la desaparición de Arcnet del mercado.

Token Ring

Token Ring trabaja en una topología de anillo conectada en forma de estrella, donde las estaciones de trabajo se enlazan alrededor de un concentrador/repetidor o MAU (Multiple Acces Unit); Unidad de acceso Multiple. Esta tecnología corre a una velocidad de 4 y 16 Mbps, velocidades que representan su máximo de transferencia de datos, utiliza el protocolo de comunicación Token Passing al igual que Arcnet y cumple con la norma 802.5 de la IEEE que incluye una capacidad de prioridad, la cual permite que algunas estaciones tengan más prioridad de acceso que otras.

A diferencia de Arcnet, la expansión de redes Token Ring resulta cara pues se necesita incrementar el número de repetidores en el anillo. Un detalle como este, se compensa con la casi nula probabilidad de que la red se paralice; ya que Token Ring utiliza tarjetas controladoras con microprocesadores que minimizan la posibilidad de que la transferencia de información sea incorrecta.

Token Ring se encuentra libre de colisiones. El gran inconveniente de esta tecnología es que no ofrece soluciones distintas a la línea de conectividad que ofrece IBM, lo cual es bastante caro.

Ethernet

Ethernet es un ambiente de comunicación entre computadoras que cumple con la norma IEEE 802.3, la velocidad de transmisión de Ethernet es de 10 Mbps, se puede utilizar con distintas opciones de cableado, permite la conexión de 1 a 1023 nodos y su precio es menor que el de Token Ring. Físicamente Ethernet, se parece a las redes Token Ring o Arcnet pues las estaciones de trabajo se conectan a través de un centro de cableado o concentradores y estos podrán enlazarse, a un bus de cable coaxial, fibra óptica o par torcido.

Ethernet, es atractivo por su precio, estandarización, sencillez en la instalación de cableado, cuenta con el respaldo de diversos fabricantes lo que permite a los usuarios con instalaciones de equipo distinto, implantarlo sin el menor problema.

2.2.1 TOPOLOGIAS DE REDES LAN.

Como se dijo en la sección 1.2.3 del presente trabajo, en redes locales, prácticamente existen tres tipos básicos de topologías, a saber:

Estrella.
Bus.
Anillo.

Para el estudio de la topología se deben considerar dos tipos:

Física.
Lógica.

La topología física es determinada por la disposición de los elementos conectados a la red. La topología lógica la determina el protocolo de comunicación operando en la red, no importando la disposición física de los elementos; en otros términos, se puede implementar un anillo lógico en un bus físico.

Topología de Estrella

En una red en estrella, todas las estaciones de trabajo se comunican entre sí a través de un dispositivo central (figura 2.1). El nodo central asume un papel muy importante, ya que todas las comunicaciones que se llevan a cabo en la red se realizan por medio de éste. Lo usual es que el nodo central ejerza todas las tareas de control y posea los recursos comunes de la red.

La configuración en estrella presenta buena flexibilidad para incrementar o decrementar el número de estaciones de trabajo, ya que las modificaciones necesarias no representan ninguna alteración de la estructura y están localizadas en el nodo central.

La repercusión en el comportamiento global de la red al presentarse alguna falla en uno de los nodos periféricos es muy baja y sólo afectaría al tráfico relacionado con ese nodo. En caso contrario si la falla se presentara en el nodo central, el resultado podría ser catastrófico y afectaría a todas las estaciones de trabajo.

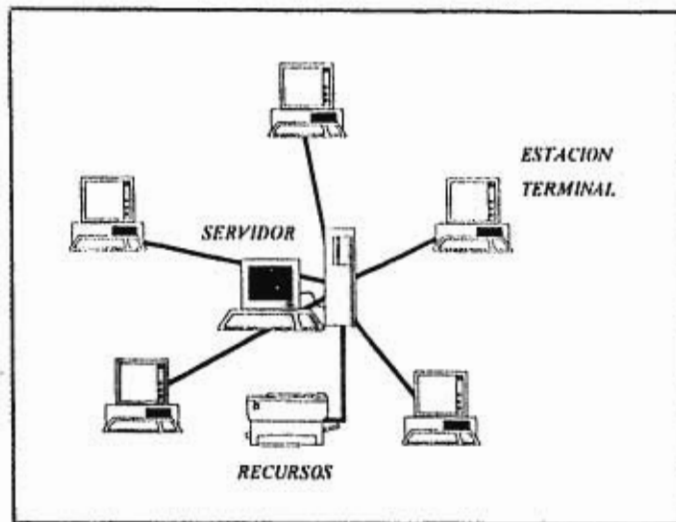


FIGURA 2.1 TOPOLOGIA EN ESTRELLA

El flujo de información puede ser elevado y los retardos introducidos por la red son pequeños si la mayor parte de ese flujo ocurre entre el nodo central y los nodos periféricos. En caso de que las comunicaciones se produzcan entre las estaciones, el sistema se vería restringido por la posible congestión del dispositivo central. En caso de existir una falla en el medio de comunicación, sólo quedaría fuera de servicio la estación de trabajo afectada.

La disposición física de los elementos ocasiona que sea una tecnología "costosa", porque no se puede aprovechar la cercanía de las máquinas para interconectarlas, sino que se deben conectar al centro.

Topología de Bus

Esta conexión se considera que es la más sencilla de todas, donde las micros, incluyendo al server, están enlazadas por un sólo cable (figura 2.2), y la información viaja en ambos sentidos, por lo que es necesario prevenir las colisiones, antes de transmitir un mensaje, cada nodo debe averiguar si el bus está disponible. Para ello el protocolo apropiado es el CSMA/CD (Carrier Sense Multiple Access/Collision Detection).

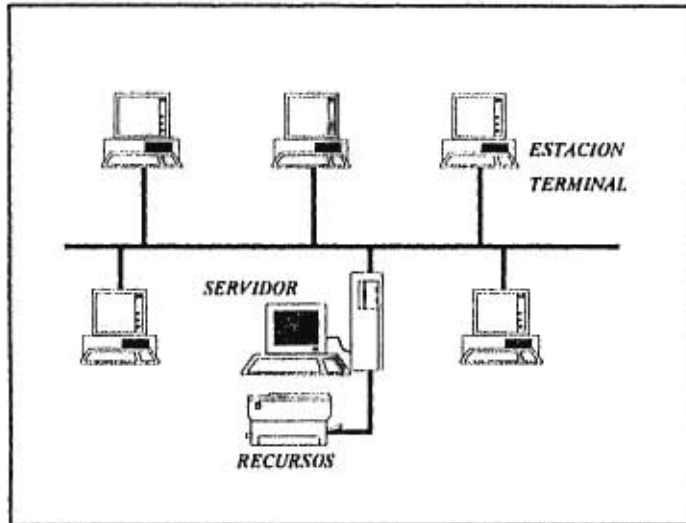


FIGURA 2.2 TOPOLOGIA EN BUS

La conexión en el nivel físico es tan simple, que sólo hay que conectar el dispositivo al medio. Normalmente, el canal se halla en estado "pasivo", esto es el canal no amplifica las señales, por lo tanto, han de tener una longitud limitada, ya que los transmisores deben poder enviar la señal a lo largo de todo el canal. Cuando se coloca un paquete en el canal, lo ven todos los dispositivos conectados a él. Desde el punto de vista de la interconexión de los dispositivos e instalación de la red, los sistemas de línea común suelen ser más sencillos que otras topologías.

Esta configuración además presenta gran flexibilidad en lo referente a incrementar o decrementar el número de estaciones de trabajo. La falla en una de las estaciones de trabajo, sólo repercutirá a esa estación de trabajo en particular, pero una ruptura en el bus dejará a la red dividida en dos o inutilizada totalmente según esté implementado el control. Esta es la topología que usa Ethernet y Arcnet.

Topología en Anillo

En esta configuración de anillo, los nodos de la red están colocados formando un anillo (figura 2.3), de manera que cada estación de trabajo tiene conexión con otras dos estaciones. Los mensajes viajan por el anillo, de nodo en nodo, en una única dirección de manera que toda la información pase por todos los módulos de comunicación de la red.

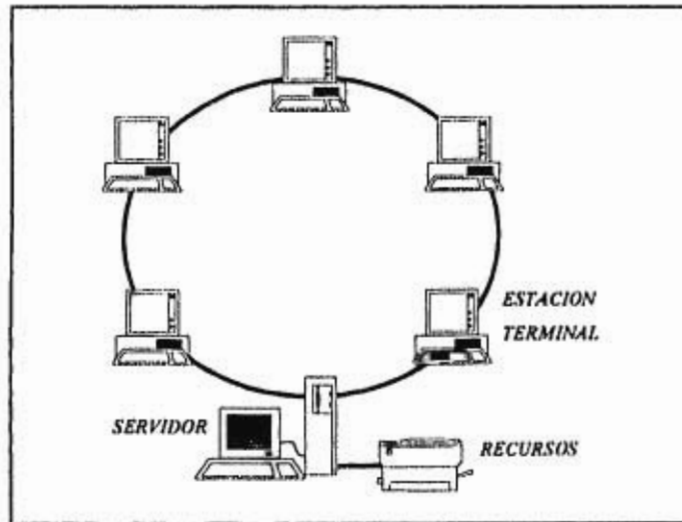


FIGURA 2.3 TOPOLOGIA EN ANILLO

Cada nodo tiene que ser capaz de reconocer los mensajes que van dirigidos a él y actuar como retransmisor de los mensajes que, pasando a través de él van dirigidos a otras estaciones que puedan existir dentro de la red.

El control de la red puede ser centralizado o distribuido entre varios nodos.

En caso de ser centralizado, uno de los nodos actúa como controlador de manera que, como todos los mensajes tienen que pasar a través de él, si no hay averías, puede verificarse el correcto funcionamiento de la red y en caso de una falla, adoptar las correspondientes medidas para solucionar el problema.

En caso de ser distribuido, el control se ejerce de manera conjunta entre diversos nodos. El flujo de información se verá limitado por el ancho de banda del medio de comunicación. Ya que cada estación de trabajo esta obligada a retransmitir cada mensaje, en caso de existir un número elevado de estaciones, el retardo introducido por la red puede ser demasiado grande para ciertas aplicaciones.

En la estructura de anillo, una falla en cualquier parte del medio de comunicación, deja bloqueada a la red en su totalidad. Si la falla se da en una de las estaciones de trabajo, la repercusión en el resto de la red dependerá de si la avería se encuentra o no en el módulo de retransmisión. En caso de que el módulo de retransmisión continúe funcionando de manera adecuada, la avería no se propaga a la red, sino que solamente deshabilita a esa estación de trabajo en particular. En caso contrario, donde la falla también involucra al módulo de comunicaciones, el anillo se "corta" y la red queda bloqueada.

Una manera de evitar estos riesgos consiste en el uso de concentradores. El concentrador es un dispositivo, fabricado con una alta confiabilidad, al que se conectan las estaciones de trabajo de la red (figura 2.4).

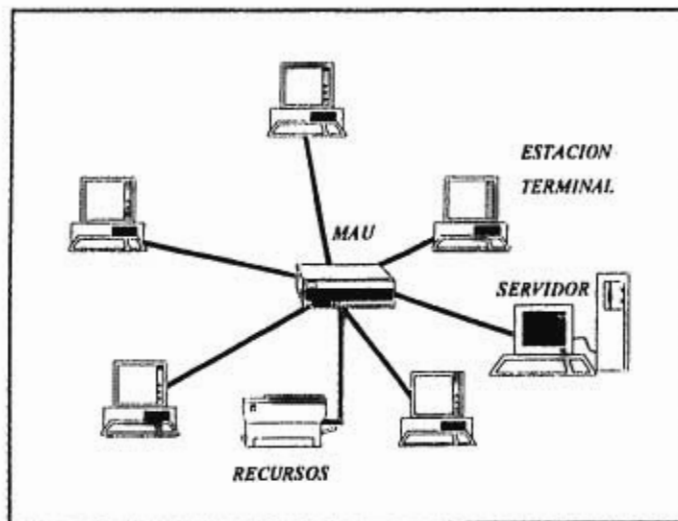


FIGURA 2.4 TOPOLOGIA EN ANILLO UTILIZANDO UN MAU

El anillo lógico ocurre dentro del concentrador y cuando un nodo deja de funcionar, se hace corto circuito con la entrada hacia la estación en el propio concentrador, reestableciéndose el anillo. A simple vista, la topología física parecerá en estrella, más la topología lógica continua siendo en anillo.

El concentrador acepta un número limitado de estaciones de trabajo, por lo que en el caso de necesitar añadir alguna otra estación una vez agotado el espacio disponible para la conexión, se puede recurrir a concatenar varios concentradores para ampliar la red. En el ámbito comercial, a estos concentradores se les llama MAU (Multiple Acces Unit).

Cabe señalar que dentro del mercado se reconoce una topología conocida como árbol o estrella distribuida, pero en términos técnicos es un anillo lógico.

2.2.2 CABLEADO DE REDES LAN.

En las Redes Arcnet el cable que comúnmente se utiliza se conoce como cable coaxial delgado RG/62, el cual tiene una impedancia de 90 ohms, un diámetro de 0.2 pulgadas, permite desplazar una señal sin necesidad de repetidores hasta una distancia efectiva de 600 metros. La máxima distancia que puede alcanzar este tipo de red a través de repetidores es de 6000 metros.

Este tipo de red Arcnet existe tanto en cableado coaxial como en par torcido, siendo el primero el más utilizado. Físicamente sería conflictivo tender una red de este tipo ya que se tendría que cerrar el anillo y agregar o eliminar un nodo sería muy complicado. En la actualidad, este tipo de red se maneja por centros de alambrado o repetidores (hubs), los que se encargan de hacer ese anillo.

Las redes Ethernet de tipo bus se pueden implantar con dos tipos de cable coaxial. Una de ellas opera con cable coaxial delgado RG/58 AU de 50 ohms, 0.2 pulgadas de diámetro y permite transportar una señal hasta 200 metros, también sin el uso de repetidores. La figura 2.5 muestra como se ve una conexión usando este tipo de cable.

La segunda alternativa es mediante la implantación del cable coaxial grueso RG/11 de 50 ohms, de 0.4 pulgadas de diámetro, que permite manejar señales hasta 500 metros sin presentar algún tipo de atenuación que produzca errores en la comunicación.

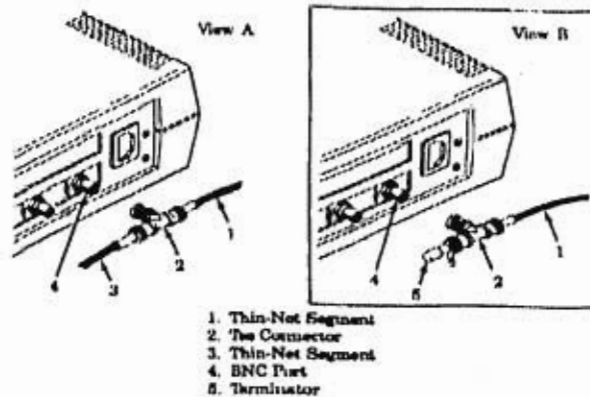


FIGURA 2.5 CONEXION DE UN CABLE COAXIAL DELGADO RG/58

La IEEE ha definido especificaciones para el cable coaxial de banda base de 10 Mbps, para una red con topología en Bus, las principales características se muestran en la tabla 2.1.

PARAMETRO	10base5	10base2
Velocidad de datos	10 Mbps	10 Mbps
Máxima longitud del cable	500 m	200 m
Nº. De Nodos	100	30
Separación del Nodo	2.5 m	0.5 m
Diámetro del cable	0.4 in	0.25 in
Extensión de la Red	2500 m	1000 m

TABLA 2.1 CARACTERISTICAS DEL CABLE COAXIAL

Tomando en cuenta las características descritas en la sección 1.2.4 del presente trabajo la alternativa de colocar cables coaxiales en redes locales tiene una relación de costo beneficio muy buena.

Como se mencionó en la sección 1.2.4 de esta tesis, el par torcido es uno de los medios más utilizado, esto se debe a su bajo precio y fácil instalación. Los cables con los conductores de cobre más delgados y menos protegidos por un jacket están dentro de la clasificación de cables tipo UTP, son sumamente baratos, flexibles y permiten manipular una señal a una distancia máxima de 110 metros sin el uso de regeneradores.

Los cables conductores más gruesos y muy bien cubiertos por un jacket son denominados del tipo STP, estos son más caros y menos flexibles que los UTP, pero permiten un rango de operación de hasta 500 metros, como en el caso de las instalaciones del tipo Token Ring STP cuando se instalan redes con un número máximo de 15 unidades MAU con tarjetas de 4 Mbps.

En general, el par torcido viene en conjuntos típicos de 2, 3, 4, 6, 16 y 25 pares de cables torcidos, sin embargo para redes locales del tipo UTP sólo se necesitan dos pares de cable para conectar a cada nodo de la red. La figura 2.6 muestra la utilización de este tipo de cable con un conector RJ-45.

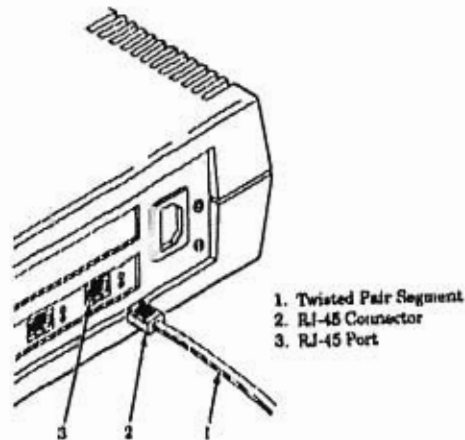


FIGURA 2.6 CONEXION DE UN CABLE DE PAR TORCIDO USANDO UN RJ-45

Los cables UTP y STP para redes de tipo Ethernet y Token Ring deben cumplir con las siguientes especificaciones:

- Tener una impedancia entre 85 y 115 Ohms a 10 Mhz.
- Presentar una atenuación máxima de 11 dB/110 metros a 10 Mhz. o una atenuación máxima de 7.2 dB/110 metros a 5 Mhz.

Algunos ejemplos del cable UTP comercial son:

- TIPO 3 ANSI/ICEA S-80-576-1983
- AT&T DIW 24/4 (D-Inside Wire)
- BellSystems 48007
- #22 AWG ó #24 AWG (American Wire Gauge)
- Systimax 2061

y del STP:

- Tipo I de IBM
- AT&T 1105 002AW1000
- AT&T 1105 012AR9800
- AT&T 1261 004A
- PrestoLite D0424PA-GY02

En resumen, el cable de par torcido tiene compatibilidad con Ethernet y Token Ring, facilidad y rapidez de instalación, Tecnología conocida, excelente relación de precio rendimiento y buena tolerancia a interferencias debido a factores ambientales.

La tercera tecnología de cables que se utiliza en las redes LAN es la fibra óptica. Normalmente se emplea por tres razones básicas: Para aquellos casos en donde las grandes distancias son un factor determinante para la implantación de una red local; cuando se requiere una alta capacidad de aplicaciones de comunicación y cuando el ruido o cualquier tipo de interferencia son factores a considerar.

Los enlaces de fibra óptica son hechos comúnmente con uno de los siguientes tipos de cable:

Cable de fibra óptica de 50/125 μm .

Cable de fibra óptica de 62.5/125 μm .

Cable de fibra óptica de 100/140 μm .

La atenuación máxima permitida para cada uno de estos cables debe ser de:

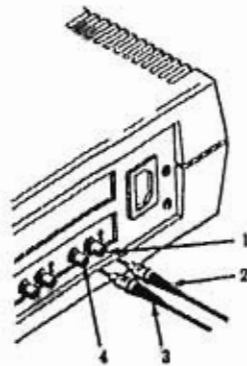
13.0 dB de atenuación para una fibra de 50/125 μm .

16.0 dB de atenuación para una fibra de 62.5/125 μm .

19.0 dB de atenuación para una fibra de 100/140 μm .

La longitud máxima permitida para redes LAN es de 2 km. de nodo a nodo sin el uso de repetidores. No obstante el estándar IEEE 802.3 permite un máximo de 1 km.

En resumen el cable de fibra óptica tiene compatibilidad con Ethernet, Token Ring y FDDI. La figura 2.7 muestra un ejemplo de conexión con fibra óptica y conectores ST.



1,4: Puertos TX y RX
2,3: Patch con conector tipo ST

FIGURA 2.7 CONEXION DE CABLE DE FIBRA OPTICA

Para terminar con esta sección, la tabla 2.2 muestra una estimación del porcentaje del tipo de cable usado en redes LAN.

TIPO DE MEDIO	1992	1993	1994	1995	1996
COAXIAL GRUESO	21.5%	20.1%	18.6%	17.1%	15.5%
COAXIAL DELGADO	13.3%	12.8%	12.1%	10.5%	8.7%
FIBRA OPTICA	5.9%	6.2%	6.6%	7.1%	7.6%
STP	28.7%	26.5%	23.6%	21.1%	18.0%
UTP	23.7%	28.8%	32.4%	36.5%	41.1%
SIN CABLE	0.7%	1.6%	2.9%	4.2%	6.1%

TABLA 2.2 PORCENTAJE DEL TIPO DE CABLE USADO EN REDES LAN

2.2.3 ANCHO DE BANDA DE REDES LAN

Las velocidades de transferencia de datos de las redes LAN actuales son muy variadas, la transferencia de datos más rápida en redes LAN llega hasta 100 Mbps.

La velocidad de transferencia de datos de una red no es suficiente para clasificarla como LAN; también se deben considerar otras características relacionadas con la velocidad. La capacidad nominal de un enlace de comunicación depende de:

1. El medio usado para transmitir la información.
2. La distancia que recorrerá la señal.
3. El esquema de codificación.

El ancho de banda que soporta el medio de transmisión ha sido descrito en la sección anterior, explicando con detalle para cada medio de transmisión, la distancia, atenuación y el ancho de banda.

La distancia sobre la cual trabajan las redes LAN, comparándola con otros tipos de redes, está resumida en la tabla 2.3.

RED	VELOCIDAD	DISTANCIA TOTAL CUBIERTA POR LA RED
LAN (IEEE 802)	1-20 Mbps	<25 Km.
FDDI	100 Mbps	< 100 Km.
MAN	30 Mbps-1Gbps	< 160 Km.
WAN	10 Kbps-1.5 Mbps	ILIMITADO
WAN ALTA VELOCIDAD	50 Mbps-1Gbps	ILIMITADO

TABLA 2.3 DISTANCIA SOBRE LA CUAL TRABAJAN LAS REDES LAN

La actual capacidad de las redes LAN, depende en gran medida de las técnicas de codificación. La codificación se refiere al mecanismo o procedimiento de la capa física que crea las señales, representando los bits que pueden ser transportados por un medio físico.

Mecanismos simples codifican un bit por baudio; mecanismos multinivel más sofisticados codifican múltiples bits por baudio. Así por ejemplo redes tipo Ethernet emplean una codificación tipo manchester, operando a una velocidad de 10 Mbps, con una frecuencia de 20 MHz y por lo tanto una eficiencia del 50%. Las redes tipo Token Ring también emplean una codificación manchester obteniendo una velocidad de 16 Mbps con una frecuencia de 32 MHz y una eficiencia del 50 %. Como un ejemplo de una codificación multinivel se tienen las redes FDDI las cuales emplean una codificación 4B5B obteniendo una velocidad de 100 Mbps para una frecuencia de 125 Mhz y por lo tanto una eficiencia de 80 %.

2.3 PROTOCOLOS

2.3.1 INTRODUCCION

El protocolo de comunicación es el conjunto de normas y regulaciones que gobiernan la transmisión y recepción de datos en la red. Análogamente el protocolo es el idioma que habla el equipo de cómputo y a través del cual puede comunicarse con otros sistemas y así como existen diversos idiomas, también existen diversos protocolos. Para entender mejor su aplicación es necesario comprender el modelo OSI (Open System Interconnection; Interconexión de sistemas abiertos) que es la base del protocolo de comunicación.

MODELO OSI

El modelo de interconexión de sistemas abiertos, es un modelo de referencia definido por la ISO (International Standards Organization; Organización internacional de estándares) como un estándar a nivel mundial del que parten los fabricantes y desarrolladores para lograr que sus productos se comuniquen.

El modelo OSI tiene el objetivo de brindar al usuario final transparencia total para que pueda comunicar los diferentes tipos de computadoras y equipo de redes que existen actualmente en el mercado.

Este modelo define una estructura para la implantación de protocolos en siete capas o niveles (figura 2.8). Cada capa comprende una serie de funciones necesarias para la comunicación entre computadoras de diferentes marcas y utiliza las capas inferiores para comunicarse con su mismo nivel pero en otro equipo. Las siete capas son las siguientes:

1) **nivel físico** es en el que se lleva a cabo el intercambio de señales eléctricas que representan los datos y la información de control. Este nivel incluye la especificación de las características mecánicas y eléctricas de la conexión física. También se definen los procedimientos para establecer, mantener y liberar las conexiones entre los circuitos eléctricos que están enlazados por medio de la comunicación.

2) nivel de enlace de datos toma el sistema de comunicaciones a partir de los bits que da el nivel físico y le superpone un medio de transmisión de datos e información de control. En este nivel se realiza el reconocimiento de la recepción de datos, así como el control de errores, con la posibilidad de retransmisión si es necesario. También puede estar presente en este nivel el control de flujo para evitar que los dispositivos más rápidos saturan a los más lentos.

3) nivel de red toma bloques de datos del tamaño de paquetes del nivel de transporte y les añade información de dirección y encaminamiento que complementan el paquete.

4) nivel de transporte proporciona un servicio de transmisión y recepción de datos fiable al nivel de sesión. Los datos se transmiten de la manera más eficiente posible para las necesidades del nivel de sesión. El nivel de transporte toma los datos del nivel de sesión y los divide en partes del tamaño del campo de datos del paquete. Después pasa los bloques de datos al nivel de red.

5) nivel de sesión establece, mantiene y termina una conexión con un proceso en un computador remoto. Este nivel debe dar un servicio fiable al nivel de presentación y tener la capacidad de restablecer una conexión en caso de que falle uno de los niveles más bajos. Mientras se establece una conexión, el nivel de sesión debe poder negociar con la máquina remota ciertos parámetros de la conexión. Estos pueden incluir el tipo de comunicación que se empleará (dúplex o semidúplex), cómo se va a controlar la integridad de la conexión, etc.

6) nivel de presentación proporciona un conjunto de servicios que se pueden usar en el proceso de intercambio de datos a través de la conexión de la sesión. Los servicios pueden incluir, por ejemplo, compresión, traducción y cifrado de los datos.

7) nivel de aplicación este nivel interactúa directamente con el software de aplicación que quiere transferir datos a través de la red. Los demás niveles existen con el único propósito de satisfacer las necesidades de este nivel.

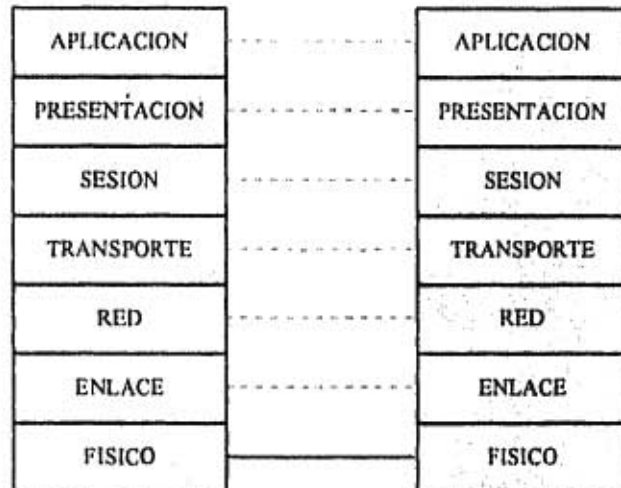


FIGURA 2.8 REPRESENTACION DE LAS 7 CAPAS DEL MODELO OSI

2.3.2 SDLC

SDLC son las siglas en inglés de Control de Enlace de Datos Síncrono que fue desarrollado por IBM para su modelo de interconexión de sistemas abiertos en su modelo SNA en su capa de control de enlace de datos que es equivalente a la capa de enlace en el modelo OSI. SDLC es equivalente a la capa de MAC de el modelo de IEEE 802. Entonces SDLC es equivalente a los protocolos 802.3 y 802.5 que se verán posteriormente.

Este protocolo maneja gran cantidad de información de control en cada trama, debido a que no sólo se necesita que sea recibida correctamente la trama, sino que también se necesita saber el número de secuencia de cada trama para que con esto una transmisión de multitrama no tenga problemas y que se pueda detectar una posible trama perdida.

El formato general de una trama SDLC se muestra en la figura 2.9

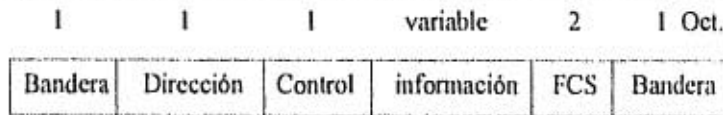


FIGURA 2.9 FORMATO DE TRAMA SDLC

Bandera de inicio.- Este campo es el inicio de cada trama de transmisión. Una bandera consiste de un sólo byte que tiene la combinación 01111110. Para asegurar que sólo será este campo el que contenga esta combinación. En donde se encuentren 6 unos consecutivos se utiliza una técnica de violación de código llamada bit stuffing.

Campo de dirección.- Este campo esta presente en todas las tramas SDLC y consiste normalmente de un sólo byte. Este campo contiene la dirección de la estación secundaria que recibirá el mensaje, entendiéndose en este caso que la estación secundaria puede ser una sólo estación, un grupo de ellas o todas las estaciones de la red (Broadcast). Cuando se tiene una transmisión punto a punto esta campo lleva puros ceros binarios. Cuando la estación secundaria esta transmitiendo el campo de dirección lleva la dirección de la estación que origino el mensaje. En este caso la dirección esta implícita ya que la estación destino del mensaje originado por la estación secundaria es siempre la estación primaria. Existe una extensión de este campo para que se haga multibyte, cuando esta arquitectura es utilizada se coloca un 1 en la posición 7 de un byte de este campo para indicar que sigue otro byte, de este modo el último byte tendrá en su posición 7 un 0, Esto permite un campo de longitud variable.

Campo de control.- Este campo es de un sólo byte de longitud y define que tipo de información contiene la trama. Existen tres tipos básicos de tramas SDLC, cada uno tiene diferente campo de control, los tres tipos de tramas que existen son:

Tramas de información: La función principal de la trama de información es transportar datos de usuario y su formato se muestra en la figura 2.10

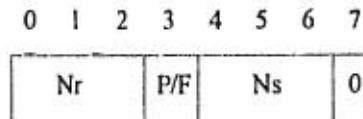


FIGURA 2.10 CAMPO DE CONTROL EN TRAMAS TIPO I

La posición 6 y 7 del campo de control identifican el tipo de trama, en una trama de información, en la posición 7 de este campo se coloca un cero binario, los tres primeros bits de este campo indican el número de trama recibida el bit en la posición 3 es un bit de poll o final, mientras que los bits en las posiciones 4, 5 y 6 indican el número de trama de transmisión, con esta arquitectura se pueden tener una transmisión máxima de 7 tramas entre reconocimientos. El bit de poll/final tiene dos propósitos dependiendo cual sea la estación que transmite, la primaria o la secundaria, cuando es la estación primaria la que transmite enciende este bit para indicar que esta haciendo el poleo de la dirección de la estación secundaria. Una estación secundaria enciende este bit sólo cuando ha enviado su última trama y regresa la transmisión a la estación primaria.

Tramas de supervisión: Estas tramas son usadas para transportar la información necesaria para funciones de control de información que es transparente para el usuario. Estas funciones incluyen el requerimiento de transmisión, requerimiento de suspensión temporal de transmisión, reporte de estado etc. El formato de un campo de control en una trama de supervisión se muestra en la figura 2.11.

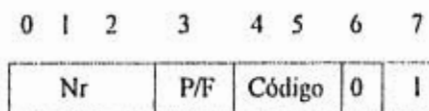


FIGURA 2.11 CAMPO DE CONTROL EN TRAMAS TIPO S

Es de notar que estas tramas no contienen campo de información ya que son sólo para fines de mantenimiento del enlace, como se ve en este caso el bit en la posición 7 se coloca en 1, luego entonces el bit que se encuentra en la posición 6 es el que define que tipo de trama está en curso, las opciones pueden ser que sea una trama de supervisión o una trama no numerada que se vera más adelante.

Los tres primeros bits de el campo de control en tramas de supervisión indican el número de conteo de la trama de recepción, el bit en la posición 3 es un bit de poll/final, y los bits 4 y 5 son dos bits de código. La función de este código es identificar el tipo de comando o respuesta que la trama representa. Las combinaciones del código son:

RR (Receiver Ready). Es utilizado como un comando de la estación primaria para el poleo y como una respuesta de la estación secundaria para indicar que esta lista para recibir las tramas 1.

RNR (Receiver Not Ready). Es usado por la estación secundaria para indicar que no esta lista para aceptar las tramas de la estación primaria.

REJ (Rejected). Es usado para indicar ciertos tipos de errores en el campo de conteo Ns.

Tramas no numeradas: Son utilizadas algunas veces para transportar datos pero son mas frecuentemente usadas para funciones especiales como para el proceso de inicialización, el control de enlace de datos y la invocación de secuencias de diagnóstico. La figura 2.12 muestra el formato de un campo de control en una trama no numerada.

Algunos comandos y respuestas de las tramas no numeradas tienen campo de información y otras no. En esta trama las posiciones 6 y 7 identifican que se trata de una trama no numerada cuando tienen una configuración de 11 en estas posiciones. El bit en la posición 3 es el bit de poll/final, el resto de los bits son interpretados como bits de código, estos bits en un trama no numerada identifican el tipo de comando que la trama representa.

Una función particular de la configuración de bits de código pueden tener diferentes interpretaciones dependiendo si la trama contiene un comando que es enviado por la estación primaria hacia la estación secundaria o una respuesta que es enviada desde la estación secundaria hacia la estación primaria, debido a que son 5 bits de código se tienen 32 combinaciones diferentes y debido a la dirección de la trama estos bits pueden representar arriba de 64 funciones diferentes, aunque solo algunas de ellas se utilizan actualmente en SDLC.

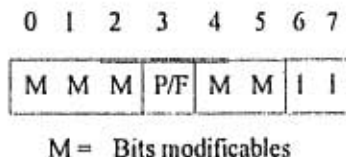


FIGURA 2.12 CAMPO DE CONTROL EN TRAMAS TIPO U

Campo de información.- El campo de información en una transmisión es usado para transportar datos de usuario, este campo puede ser de longitud variable pero siempre de múltiplos de ocho bits. A pesar de que la arquitectura no define una longitud máxima, un dispositivo particular debe de poner un límite en la longitud del campo de información basado en la capacidad del buffer que esta disponible, el contenido del campo de información no tiene significado para SDLC ya que SDLC es para la capa de control de enlace de datos de SNA y el campo de información pertenece a capas superiores.

Campo de FCS.- Este campo contiene 16 bits de chequeo de redundancia que es usado para detecciones de errores cíclica, estos dos bytes son generados por la estación que transmite. El campo de dirección, el de control y el de información están incluidos en el cómputo del CRC.

Bandera de final.- El fin de una trama de SDLC es una bandera de final que tiene la misma configuración que la bandera de inicio de trama (01111110).

2.3.3 HDLC

HDLC es una norma publicada por ISO que ha conseguido afianzarse en todo el mundo. Proporciona una amplia variedad de funciones y cubre un amplio espectro de comunicaciones. Está considerado en realidad como un ámbito que engloba a muchos otros protocolos. El protocolo HDLC puede instalarse de muchas maneras. Admite transmisiones dúplex y semidúplex, configuraciones punto a punto o multipunto, y canales conmutados o no conmutados. Una estación HDLC puede funcionar de tres formas:

- La estación principal controla el enlace de datos. Esta estación envía tramas de comando a las estaciones secundarias del canal, de las cuales, a su vez, recibe tramas de respuesta. Si el enlace es multipunto, la estación principal es responsable además de mantener una sesión independiente con cada una de las estaciones conectadas al canal.
- La estación secundaria funciona como esclava de la principal. Envía mensajes de respuesta a los comandos procedentes de la estación controladora. Sólo mantiene la sesión en curso con la estación principal, y no interviene en el control de enlace.

- La estación combinada transmite comandos y respuestas, y también recibe comandos y respuestas de otras estaciones combinadas. Mantiene una sesión con otra estación combinada.

El Formato de trama del protocolo HDLC es igual al de SDLC excepto en el campo de control que se explicará más adelante. El formato se muestra en la figura 2.13.

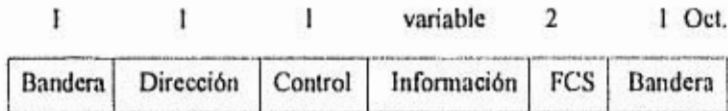


FIGURA 2.13 FORMATO DE TRAMA HDLC

Los campos de bandera, dirección y FCS son idénticos a los que se explicaron en SDLC. El campo de información también depende de capas superiores.

Campo de control: Define los comandos y respuestas para controlar el flujo de tráfico del enlace. En este campo se definen también tres diferentes tipos de trama que son los mismos que se vieron con SDLC:

- Tramas de Información
- Tramas de supervisión
- Tramas no numeradas

La trama de información tiene el mismo formato que su contraparte en SDLC y también sirve para transmitir información de usuario.

La trama de supervisión también presenta el mismo formato que en la trama SDLC explicado en la sección anterior. También presenta los mismos comandos y respuestas.

El formato de tramas no numeradas es prácticamente idéntico al formato de tramas no numeradas de SDLC, la diferencia recae en los comandos y respuestas que manejan cada protocolo, los comandos no numerados se agrupan según la función que realizan:

- Comandos de activación de modo: SABM, SNRM, SABME, SIM, DISC.
- Comandos de transferencia de información: UI, UP.
- Comandos diversos: XID, TEST.

Algunos de los comandos y respuestas más importantes se listan a continuación:

UI: (Información no numerada). Este comando permite transmitir datos de usuario dentro de una trama no numerada (no sometida a secuenciamiento).

SIM: (Activar modo de inicialización). Sirve para inicializar una sesión primaria/secundaria. La respuesta esperada es un UA.

SNRM: (Activar modo de respuesta normal). Coloca a la estación secundaria en modo de respuesta normal, no puede transmitir tramas sin recibir autorización para ello, lo que significa que todo el control de flujo de tráfico recae en la estación principal.

DM: (Modo de desconexión). Una estación transmite esta trama para indicar que desconecta el modo actual.

DISC: (Desconectar). Cuando una estación principal envía este comando a una secundaria, esta queda en modo de desconexión, se trata de un comando muy útil en líneas conmutadas. Se espera una respuesta UA.

UA: (Reconocimiento no numerado). Esta es la confirmación que se devuelve al recibir comandos de activación de modo. También sirve para informar que ha concluido el estado de ocupado de una estación.

FRMR: (Rechazo de una trama): Una estación secundaria entrega esta trama cuando detecta una trama errónea.

RD: (Solicitud de desconexión). Solicitud que envía la estación secundaria para ser desconectada y ser colocada en estado de desconexión lógica.

XID: (Identificación de la estación de intercambio). Este comando pide a una estación secundaria que se identifique. En sistemas conmutados sirve para determinar cual es la estación que llama.

TEST: Sirve para solicitar de la estación secundaria una respuesta a determinadas pruebas y comprobaciones.

SABM: (activar modo asíncrono equilibrado). Activa el modo Arm en el cual las dos estaciones tienen la misma jerarquía.

SABME: (activar modo asíncrono equilibrado extendido). Entra en modo SABM reservando dos octetos mas para el campo de control.

UP (sondeo no numerado). Sondea una estación sin tomar en cuenta el secuenciamiento ni el acuse de recibo.

La codificación de los bits en el campo de control dependiendo de su comando o respuesta se muestra en la tabla 2.4.

Las diferencias en los protocolos SDLC y HDLC recaen básicamente en la cantidad de comandos que utiliza SDLC que no aparece en ninguna norma de HDLC. Se puede decir que SDLC es la versión de IBM de HDLC. Puede operar en topologías de bucle y puede realizar un sondeo en anillo y en bucle. En consecuencia SDLC es capaz de manejar configuraciones punto a punto, multipunto o en anillo, otras diferencias son:

HDLC permite extender el campo de control. Los sistemas HDLC que emplean la opción de formato extendido pueden ampliar su campo de control hasta 16 bits, lo cual permite manejar números de secuencia mayores dentro de los campos N(R) y N(S). IBM sólo admite el formato básico de 8 bits. Este hecho adquiere una especial importancia cuando se opera con enlaces vía satélite.

Los sistemas SDLC obligan a que el campo de información esté formado por un número par de octetos. HDLC no impone esa restricción.

Formato	Código	Comandos	Respuestas
	0 1 2 3 4 5 6 7		
Información	0 N(S) - N(R)	Información	Información
Supervisión	1 0 0 0 - N(R) 1 0 0 1 - N(R) 1 0 1 0 - N(R) 1 0 1 1 - N(R)	RR REJ RNR SREJ	RR REJ RNR SREJ
No Numerado	1 1 0 0 - 0 0 0 1 1 0 0 - 0 0 1 1 1 0 0 - 0 1 0 1 1 0 0 - 1 0 0 1 1 0 0 - 1 1 0 1 1 0 0 - 1 1 1 1 1 1 0 - 0 0 0 1 1 1 0 - 0 0 1 1 1 1 1 - 0 0 0 1 1 1 1 - 0 0 1 1 1 1 1 - 0 1 0 1 1 1 1 - 0 1 1 1 1 1 1 - 1 0 0 1 1 1 1 - 1 0 1 1 1 1 1 - 1 1 0	UI SNRM DISC UP TEST SIM SARM RSET SARME SNRME SABM XID SABME	UI RD UA TEST RIM FRMR DM XID

El bit en la posición 4 puede ser 1 o 0 dependiendo si es poll o final.

TABLA 2.4 CODIFICACIÓN DE LOS BITS EN EL CAMPO DE CONTROL

2.3.4 ESTANDARES IEEE 802

2.3.4.1 INTRODUCCION

Debido a las necesidades de estandarización para redes, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) desarrolló la recomendación 802, la cual está dirigida a las capas física y de enlace del modelo OSI. La figura 2.14 muestra la relación entre el modelo OSI y la recomendación 802 de IEEE.



FIGURA 2.14 RELACION ENTRE OSI Y IEEE 802

La capa física del modelo de IEEE es muy similar a su contraparte de OSI. Es responsable de la codificación y decodificación de la señal, de la transmisión y recepción serial de bits, y también del medio de transmisión (Par trenzado, cable coaxial, fibra óptica, etc.).

Traslapando las capas física y de enlace del modelo OSI se encuentra la capa de Control de acceso al medio (MAC) de 802 de IEEE, esta capa como su nombre lo indica se encarga de controlar el acceso al medio de transmisión, y además está dividida en otros estándares:

- 802.3 Carrier Sense Multiple Access Bus with Collision Detection (CSMA/CD)
- 802.4 Token Passing Ring
- 802.5 Token Passing Bus

2.3.4.2 IEEE 802.2 (LLC)

La capa más alta del modelo de IEEE definido para LAN es la de Control de enlace lógico (LLC) definida por el estándar 802.2. La principal diferencia entre la capa de enlace de OSI y la capa de LLC de IEEE es que en el modelo de IEEE pueden existir varios puntos terminales.

Hay dos tipos de operación del LLC:

Tipo 1 Soporta servicios sin acuse de recibo.

Tipo 2 Soporta servicios con acuse de recibo.

El formato básico del protocolo LLC se muestra en la figura 2.15

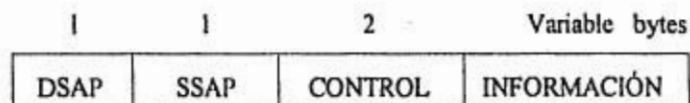


FIGURA 2.15 FORMATO BASICO LLC

Los dos primeros campos son las direcciones DSAP (Punto de acceso a servicio destino) y SSAP (Punto de acceso a servicio fuente), las cuales tienen una longitud de un octeto cada uno, el bit menos significativo (LSB) del DSAP indica si la dirección es un grupo o un punto individual, mientras que el LSB del SSAP indica si la trama es un comando o una respuesta.

El campo de control es el siguiente: esta formado por uno o dos octetos. Existen tres tipos diferentes de campos de control: de información (I), de supervisión (S) y no numerado (U).

El formato de información (figura 2.16) es usado para la transmisión de datos secuenciales incluyendo un número de secuencia, N(S), de la trama transmitida, además del reconocimiento, N(R), que indica la trama I esperada de la estación remota, el formato I es usado solamente en el tipo 2.

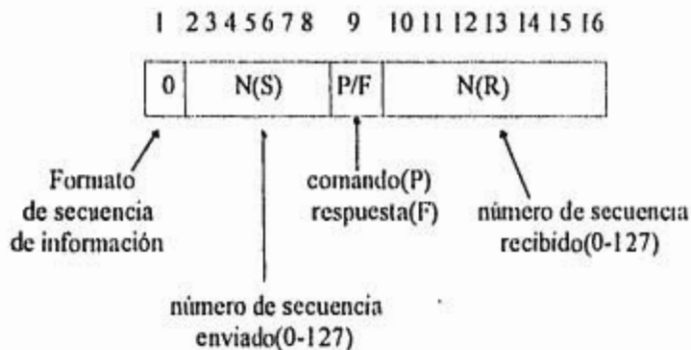


FIGURA 2.16 FORMATO DEL CAMPO DE CONTROL EN TRAMAS I

El formato de supervisión (S) que se muestra en la figura 2.17 se usa para supervisar el intercambio de tramas de información, incluye N(R), el contador de secuencia de recepción, el formato S es usado solamente en el tipo 2.

El formato no numerado es usado para establecer y desconectar el enlace lógico. El formato U puede ser usado en el tipo 2 o en el tipo 1 operando acorde a su aplicación. Su formato se indica en la figura 2.18.

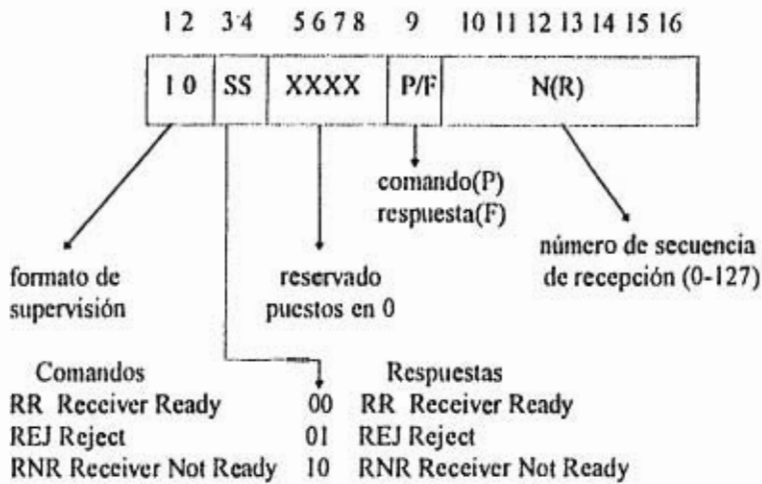


FIGURA 2.17 FORMATO DEL CAMPO DE CONTROL EN TRAMAS TIPO S

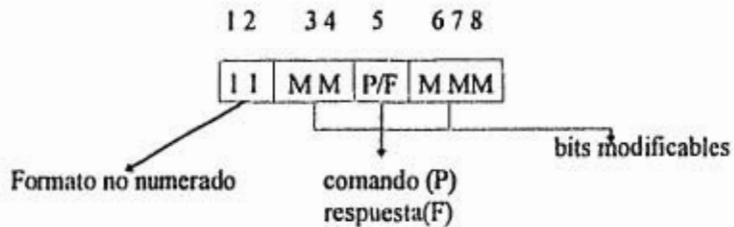


FIGURA 2.18 FORMATO DEL CAMPO DE CONTROL EN TRAMAS TIPO U

Los bits M pueden variar, las posibles combinaciones de este campo son:

1	2	3	4	5	6	7	8	Bits	
1	1	0	0	P	0	0	0	UI Comando	} Tipo de operación 1
1	1	1	1	P	1	0	1	XID Comando	
1	1	0	0	P	1	1	1	Test Comando	
1	1	1	1	F	1	0	1	XID Respuesta	
1	1	0	0	F	1	1	1	Test Respuesta	
1	1	1	1	P	1	1	0	SABME Comando	} Tipo de operación 2
1	1	0	0	P	0	1	0	Disconnect Comando	
1	1	0	0	F	1	1	0	UA Respuesta	
1	1	1	1	F	0	0	0	DM Respuesta	
1	1	1	0	F	0	0	1	FRMR Respuesta	

Por último el campo de información lleva la información de capas superiores, y tiene una longitud de $M \cdot 8$ bits, donde M es un valor entero igual o mayor que 0.

El contenido de esta capa (LLC) se deposita en la capa MAC. Existen diferentes estándares para esta capa, los cuales se describen a continuación.

2.3.4.3 IEEE 802.3

El protocolo MAC IEEE 802.3 usa el protocolo CSMA/CD (Carrier Sense Multiple Access with Collision Detection). La versión original fue desarrollada por Xerox como parte de la red Ethernet.

Con CSMA/CD, una estación que desea transmitir primero ve el medio de transmisión para determinar si existe una transmisión en progreso (Carrier Sense). Si el medio está libre la estación puede transmitir. Puede suceder que dos o más estaciones intenten transmitir al mismo tiempo. Si esto ocurre existirá lo que se conoce como colisión; los datos que envían las estaciones se dañan y por lo tanto no son recibidos exitosamente.

CAPITULO II. REDES LAN

De este modo, se necesita un procedimiento que especifique que es lo que debe de hacer una estación si el medio esta ocupado y que se debe de hacer si ocurre una colisión:

1. Si el medio esta libre, transmite, de otro modo, ve al paso 2.
2. Si el medio esta ocupado, continua escuchando hasta que el medio se desocupe, después transmite inmediatamente.
3. Si se detecta una colisión durante la transmisión, transmite una pequeña señal jamming para asegurar que todas las estaciones sepan que ha ocurrido una colisión.
4. Después de transmitir la señal jamming, espera un tiempo aleatorio y después intenta transmitir una vez más.

La figura 2.18a describe el formato de una trama para el protocolo 802.3.

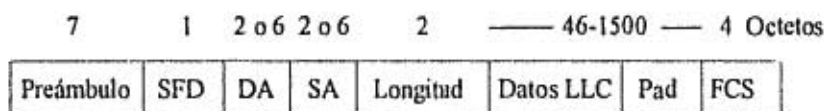


FIGURA 2.18a FORMATO DE TRAMA IEEE 802.3

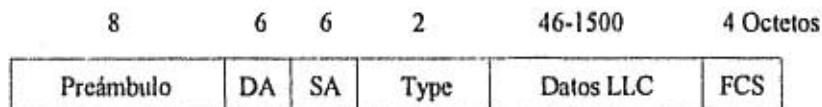


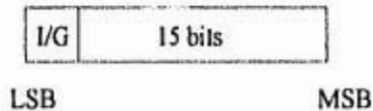
FIGURA 2.18b FORMATO DE TRAMA ETHERNET

El primer campo es el **preámbulo**, el cual consta de 7 octetos que siguen un patrón de combinación de bits, alternando 1s y 0s (10101010....10) y es utilizado para establecer sincronización de bits.

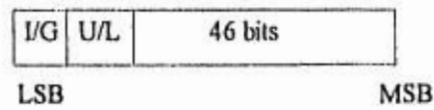
SFD (Delimitador de inicio de trama). Indica el inicio de la trama y permite al receptor localizar el primer bit del resto de la trama, este campo tiene un octeto de longitud y una combinación de bits fija: 10101011.

DA (Dirección destino). Especifica la estación a la cual va dirigida la trama, puede ser una dirección física única, una dirección de grupo o una dirección global. La elección de 2 o 6 octetos de longitud es una decisión que debe de ser la misma para todas las estaciones de la LAN, lo mas común es el uso de 6 octetos. El formato de este campo se muestra en la figura 2.19.

Para 2 octetos:



Para 6 octetos:



LSB = Bit menos significativo
I/G = Campo Individual/Grupo

MSB = Bit mas significativo
U/L = Campo Universal/Local

FIGURA 2.19 FORMATO DE CAMPO DE DIRECCION

SA (Dirección origen). Especifica la estación que origina la trama y tiene el mismo formato que el DA. Si el DA es de dos octetos el SA también debe de ser de dos octetos, lo mismo ocurre cuando el DA es de 6 octetos, es decir, estos dos campos son de igual longitud, 2 o 6.

Longitud. Especifica la longitud del campo de datos LLC.

Datos LLC. En este campo se deposita el formato LLC que ya se describió anteriormente.

Pad. Son octetos que se utilizan para asegurar que la trama es suficientemente grande para una operación correcta, Cuando el campo LLC es menor a 46 octetos se usa el campo Pad. Se tiene como máximo una longitud de 1500 octetos entre el campo de datos y el Pad.

FCS. Es un CRC de 32 bits aplicable a los campos DA, SA, Longitud, Datos LLC y Pad.

TRAMA ETHERNET

La versión original desarrollada por Xerox Ethernet-LAN difiere un poco de la versión de IEEE 802.3, esta versión se muestra en la figura 3.18b

En esta versión el preámbulo consta de 8 octetos que tienen la combinación de 101010.... 10101011 y también sirve para establecer sincronización, el DA y El SA tienen una longitud de 6 octetos y tienen el mismo formato que en el caso de 6 octetos de la versión de IEEE 802.3.

El campo de type tiene una longitud de 6 octetos y se utiliza para especificar el protocolo de capas superiores que se deposita en el campo de datos. Algunos de los tipos más conocidos son el 0800h (TCP/IP), 0600h (XNS) y 0806h (ARP).

El campo de datos es igual que en la versión de IEEE, lo mismo que el campo de FCS.

2.3.4.4 IEEE 802.5 (TOKEN RING)

La técnica de Token Ring está basada en el uso de una pequeña trama llamada *Token* que circula cuando todas las estaciones están sin transmitir (Se debe tener en cuenta que Token Ring presupone una topología de anillo). Una estación que desea transmitir debe esperar hasta que detecta que el token pasa por ella, entonces toma el token y le cambia un bit, con esto el token se convierte en una secuencia de inicio de una trama de datos. Después la estación construye los campos necesarios restantes para completar la trama de datos.

Cuando una estación toma el token y comienza a transmitir una trama de datos, no existe token en el anillo, así es que otras estaciones que desean transmitir deberán de esperar. La trama en el anillo dará una vuelta entera hasta que sea absorbida por la estación transmisora, con esto se entiende que la estación receptora toma una copia de la trama y la vuelve a transmitir. La estación transmisora inserta un nuevo token cuando se cumplen las siguientes condiciones:

- La estación ha completado la transmisión de su trama.
- La trama ha regresado a la estación origen.
- La estación origen ya no desea transmitir otra trama.

Debido a la operación de Token Ring se requiere de tres formatos diferentes:

- formato de Token
 - formato de trama MAC
 - formato de secuencia de aborto
- El formato de Token esta formado por tres octetos como se muestra en la figura 2.20

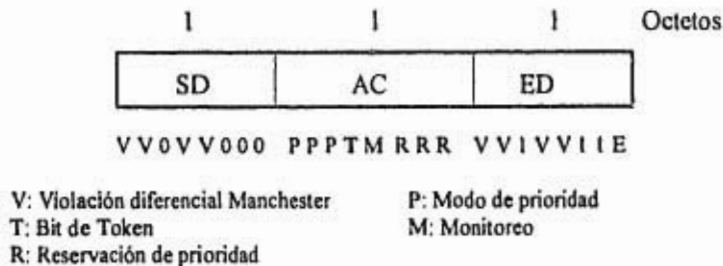


FIGURA 2.20 FORMATO DE TOKEN

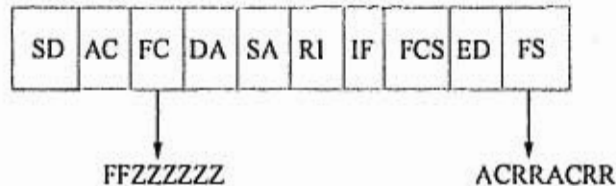
SD (Delimitador de inicio). Contiene bits de violación Manchester diferencial, además de los 0's binarios.

AC (Control de acceso). Comienza con tres bits de prioridad. Cada estación tiene asignada una prioridad para su transmisión, 000 es la prioridad más baja y 111 es la más alta.

Los bits R (reservación) pueden ser usados por una estación que requiere reservar el siguiente token para su transmisión. Para que una estación pueda transmitir su prioridad debe ser mayor o igual a la del token. El bit T hace la diferencia entre un token (T=0) y una trama (T=1). El bit M es usado para evitar que una trama este circulando continuamente en el anillo, este bit es puesto en 0 por la estación transmisora y es puesto en 1 por un estación de monitoreo activa.

ED (Delimitador de fin). Incluye bits de violación Manchester diferencial, un bit intermedio que cuando es puesto indica que es parte de una multitrama, bits binarios puestos en 1 y un bit E que es puesto cuando la trama tiene un error de FCS.

- El formato de trama es de longitud variable, y este es transmitido después de la exitosa captura del token. Este formato se muestra en la figura 2.21.



- F = Formato de trama
 - 00 =MAC(Datos del anillo)
 - 01 =LLC(Datos de usuario)
 - IX=Uso futuro
- Z = Bits de control
- A = Dirección reconocida
- C = Trama recibida
- R = Bits reservados

FIGURA 2.21FORMATO DE TRAMA TOKEN RING

Los primeros dos octetos de la trama, el SD y AC son tomados del formato del token descrito anteriormente.

FC (Control de trama). Define dos tipos de tramas, la trama LLC que contiene datos de usuario, o la trama MAC que contiene datos para mantenimiento del anillo. Este campo tiene un octeto de longitud

Los campos **DA** y **SA** de dos o seis octetos de longitud están regidos por el mismo formato que la recomendación IEEE 802.3 en sus campos de dirección.

RI (Información de ruteo). este campo es opcional (Agregado por IBM), aparece cuando la trama transmitida tiene que pasar por diferentes anillos a través de bridges. Es un campo de longitud variable de 0 a 30 octetos.

IF (Campo de Información). Contiene los datos de usuario en el caso de LLC, en este caso se depositan los campos de LLC que se analizaron previamente. En el caso de una trama MAC este campo contiene comandos y parámetros para el mantenimiento del anillo.

FCS. Es igual al FCS de la recomendación IEEE 802.3.

ED (Delimitador de fin). Este campo es tomado del formato de token.

FS (Estado de trama). Este campo es el último de la trama, incluye los bits de reconocimiento de dirección (A) y de trama recibida (C) que verifican que la estación receptora ha procesado propiamente la trama.

- El formato de aborto consta de solamente dos octetos como se muestra en la figura 2.22.

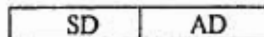


FIGURA 2.22 FORMATO DE ABORTO

Este formato se usa cuando ocurren condiciones erróneas, como pueden ser errores graves en la estación de trabajo. Los campos **SD** y **ED** son idénticos a los campos correspondientes en el formato de token.

2.3.5 TCP/IP

TCP/IP (Transmission Control Protocol / Internet Protocol), fue desarrollado a mediados de los años 70's por el departamento de defensa, por la administración de investigación de proyectos avanzados de redes de defensa (ARPANET).

TCP/IP es un conjunto de protocolos no relacionados con las capas física y de enlace de datos, según se describe en el modelo de referencia OSI. TCP/IP se puede implementar en casi cualquier medio físico de comunicaciones de datos y protocolos de las capas físicas y de enlace de datos.

Descripción general de protocolos TCP/IP

Aunque no existe una relación uno a uno entre el modelo OSI de siete capas y TCP/IP, se puede considerar que este ocuparía de la capa 3 a la 7. Sin embargo, en su definición únicamente utiliza tres capas: aplicación, transporte y red (figura 2.23).

<i>TCP/IP</i>	<i>OSI</i>
APLICACION (TELNET, FTP, MAIL)	APLICACION
TRANSPORTE (TCP)	PRESENTACION
	SESION
	TRANSPORTE
INTERNETWORK (IP)	RED
SUBNETWORK (ETHERNET, ARCNET)	ENLACE
	FISICA

FIGURA 2.23 RELACION ENTRE TCP/IP Y OSI

APLICACION

En esta capa se encuentran todos los protocolos que definen las diferentes aplicaciones dentro de la red, como el correo electrónico, la transferencia de archivos, etc. Los servicios de TCP/IP son soportados por los protocolos adecuados que se describen a continuación:

Transferencia de archivos

El protocolo de transferencia FTP permite a un usuario o a cualquier computadora transferir archivos de otra computadora o enviar archivos a otra computadora. Existen tres utilerías que permiten la transferencia de archivos entre un PC un Host¹ remoto. Este Host puede localizarse en la red local o en una red remota, estas utilerías son las siguientes:

- FTP (File Transfer Protocol). Permite el acceso a directorios y archivos de un Host realizando las operaciones comunes sobre ellos.
- RCP (Remote Copy) Permite copiar archivos, directorios y estructuras de directorios.
- TFTP (Trivial File Transfer Protocol) Permite realizar copias sin necesidad de identificarse como un usuario.

Login remoto

El protocolo de terminal de red permite conectarse a un Host remoto que soporte el protocolo Telnet y en el cual se tenga una cuenta de usuario válido. Una vez dentro de la sesión se puede ejecutar cualquier comando que el Host remoto entienda además de los comandos existentes en el modo de comando del Telnet.

- TELNET: Permite conectarse a un Host remoto que soporte Telnet identificándose como un usuario válido.

¹ Host: Sistema informático que tiene una relación jerárquica superior con respecto a los otros elementos.

- RLOGIN: (Remote Login) Permite realizar una conexión virtual a un sistema remoto que soporte el protocolo telnet.

Correo por computadora

Este correo permite mandar mensajes a usuarios en otras computadoras.

- MAIL: Es una extensión de la utilería de correo de los ambientes UNIX que permite enviar y recibir mensajes con el protocolo SMTP (protocolo simple de transferencia de correspondencia). utiliza el nombre de la cuenta del usuario como dirección destino.

Ejecución remota

Permite que un programa se ejecute en otra computadora. Se pueden ejecutar comandos, programas o realizar llamadas a procedimientos remotos.

TRANSPORTE

Esta capa se encarga de la comunicación *end-to-end*, es decir, sólo entre la comunicación entre la máquina origen y la destinataria, no importando por que máquinas pase dentro de su viaje por la red.

Protocolo TCP

El protocolo TCP es el responsable de que los comandos y mensajes, proporcionados por las aplicaciones, se transmitan a través de la red hasta alcanzar su destino; lleva un registro de lo que se envía y se transmite debido a errores o pérdida de los paquetes. Se encarga también de dividir los paquetes demasiado grandes en paquetes del tipo *datagrama*¹ y de ensamblarlos posteriormente en el lado destino colocándolos en orden de acuerdo a su secuencia. TCP es un conjunto de rutinas que las aplicaciones utilizan cuando requieren una comunicación confiable a través de la red con otra computadora.

¹ Un datagrama puede definirse como un paquete de longitud finita con información suficiente para ser enviado en forma independiente de la fuente al destino sin apoyarse de transmisiones anteriores.

En forma similar, TCP hace llamadas a los servicios de IP, que en términos generales, hará las veces de ruteador. Sin embargo, IP no tiene la capacidad para saber que relación existe entre un datagrama y el siguiente datagrama que envíe.

Supóngase que se desea transmitir un mensaje, TCP divide los datos en datagramas, el siguiente paso es que TCP ponga un encabezado al inicio de cada datagrama; este encabezado se muestra en la figura 2.24

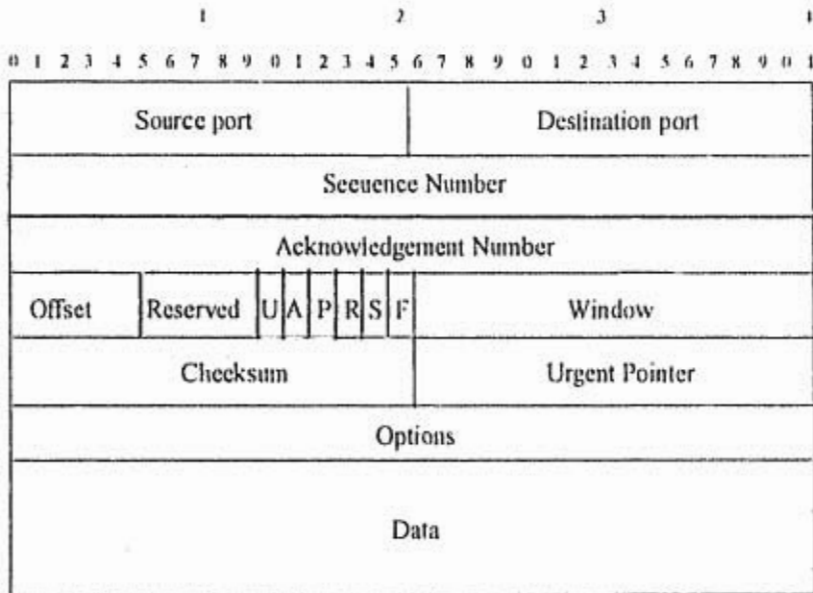


FIGURA 2.24 HEADER DEL PROTOCOLO TCP

Los campos más importantes de este formato son: "puerto origen", "puerto destino", "número de secuencia" y "Checksum".

CAPITULO II. REDES LAN

El número de secuencia sirve para que el puerto destino verifique que todos los datagramas enviados por el puerto origen hayan llegado correctamente y que puede ensamblarlos de acuerdo con esta secuencia.

El Checksum contiene un número que se obtiene de la suma de todos los octetos del datagrama. En el puerto destino, se vuelve a calcular el valor del Checksum y se le compara con el valor original. Si existe diferencia significa que el paquete sufrió algún daño durante la transmisión y se le desecha.

Para asegurar que el destino recibió el datagrama envía al origen el "Acknowledgement number". Si el origen no recibe este ACK después de un tiempo razonable, el dato se transmite otra vez.

El campo de "Window" se utiliza como mecanismo de control de flujo de datos en tránsito que el origen puede enviar al destino. No es práctico que el origen espere por el ACK de cada datagrama que envía al destino, antes de transmitir el siguiente porque esto provocaría que la transmisión de datos fuera en extremo lenta. Tampoco se pueden transmitir datos sin un control, porque se podría sobrepasar la capacidad de procesamiento de datos del lado destino. Para evitar cualquiera de estas situaciones, el lado destino escribe en el campo Window la cantidad de datos que está preparado para recibir. Cuando el valor de Window se incrementa, el origen comienza a enviar datos al destino.

INTERNETWORK

Provee las funciones necesarias para conectar redes y gateways. Esta capa es responsable de la entrega de datos de su origen hasta su destino final.

Protocolo IP

El IP agrega un encabezado (figura 2.25) que se relaciona principalmente con las direcciones de internet origen y destino. En general, la función principal de IP es informar quien llama al lado destino y encontrar la mejor ruta a través de la red para que el datagrama encuentre su destino.

A continuación se describen los campos del header IP.

- **Ver (4 bits):** Identifica la versión de IP que genero el datagrama. La versión de IP actual es 4. Un datagrama que tenga un número de versión diferente a 4 es descartado.
- **HL (4bits):** La longitud en octetos del header IP en palabras de 32 bits (mínimo 5 palabras o 20 octetos).
- **Type of service (8 bits):** Especifica prioridad, confiabilidad y retardo.
- **Total length (16 bits):** Longitud total del datagrama IP, dado en octetos, incluyendo el encabezado IP.
- **Identification (16 bits):** Provee un identificador único para este datagrama. Cuando el datagrama sufre fragmentación al ser encapsulado el host emisor genera un identificador único para identificar a todos los fragmentos que se generaron.
- **Flags (3bits):** Controlan el manejo de los datagramas en caso de fragmentación. El bit llamado DF (Don't Fragment) al estar encendido especifica que el datagrama no puede ser fragmentado bajo ninguna circunstancia. El bit MF (More Fragments) al estar encendido indica que le siguen a este datagrama más fragmentos.

XX	DF	MF
----	----	----

- **Fragment offset (13 bits):** Está expresado en unidades de 8 bytes e indica el corrimiento del fragmento, relativo al inicio del datagrama completo.
- **Time to live (8 bits):** Este valor indica que tanto tiempo puede permanecer el datagrama recorriendo la red antes de ser descartado. Este valor es decrementado por cada ruteador que procesa el datagrama. Si el valor llega a cero antes de que el datagrama llegue a su destino, el datagrama será descartado.
- **Protocol (8 bits):** Identifica el próximo protocolo que sigue al encabezado IP, por ejemplo TCP, cuyo valor es 6.
- **Header checksum (16 bits):** Usado para checar los datos del header de IP.
- **Source address (32 bits):** Indica la dirección Internet del host origen.
- **Destination address (32 bits):** Indica la dirección Internet del host destino.
- **Options (variable):** opciones del remitente; por ejemplo, especificación de ruta.
- **Padding (variable):** Se asegura de que el header termine en 32 bits.
- **Data (variable):** En múltiplos de 8 bits, no exceden a 65 535 octetos para el encabezado IP más datos (Datos y header de TCP, etc).

Nótese que los límites de un datagrama IP son 576 octetos como mínimo y 65, 535 octetos como máximo.

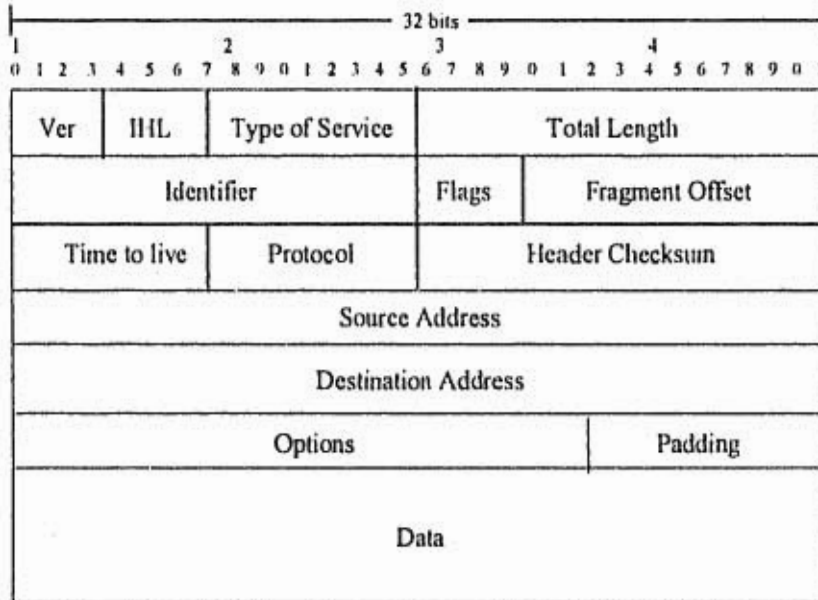


FIGURA 2.25 HEADER DEL PROTOCOLO IP

Dirección Internet

Las direcciones en Internet constan de cuatro números (32 bits), cada uno menor que 256. Cuando dichos números se escriben, se separan por puntos, como se muestra a continuación:

132.248.10.3

Los primeros números de la dirección indican a los ruteadores cual es la red a la que pertenece esta dirección. Los últimos números indican que computadora personal o host (equipo anfitrión) de la red debe recibir el paquete.

Cada dirección se divide en dos partes: la red y el host local. Esta división se puede realizar de tres formas llamadas clase A, B y C (figura 2.26).



FIGURA 2.26 DIRECCIONES DE INTERNET

Clase A

En esta clase el primer número (byte) representa el número de la red y los tres restantes el número de host local. Como el primer bit del byte utilizado para el número de la red se pone en cero se pueden tener un total en total, 128 (2^7) redes de clase A con 16 777 216 (2^{24}) host cada una.

Clase B

Esta clase consiste en utilizar los dos primeros bytes para indicar la red y los dos siguientes para el host local. Los primeros bits del número de red se ponen en 10 de manera que puede haber 16 384 (2^{14}) redes de clase B con 65 536 (2^{16}) host cada una.

Clase C

En este tipo los tres primeros bytes se utilizan para el número de red y el último para el número del host local. Los primeros bits se ponen como 110, de manera que podemos tener 2 097 152 (2^{21}) redes de clase C con 256 (2^8) host cada una.

ESTA TESIS NO DEBE
SALIR DE LA BIBLIOTECA

Nombre del Host

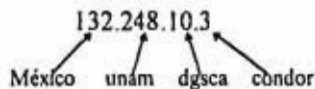
Para facilitar a los usuarios la identificación de los host de una red se asigna un nombre a cada uno de ellos. El nombre del host es un conjunto de caracteres alfanuméricos que comienza con una letra y se utiliza en los comandos de línea y en archivos de administración de la red. A nivel del sistema, el nombre se traduce a su correspondiente dirección de Internet antes de enviar los paquetes de información.

En la conversión del nombre del host a la dirección Internet se utiliza el DNS (Domain Name System) que provee un método estándar para el establecimiento, mantenimiento y distribución de la información acerca de la red, host y nodos. Generalmente utiliza una tabla de nombres de host y sus correspondientes dirección de Internet, de manera que puede servir para rutear correo o para determinar el nombre del host que corresponde a cierta dirección de Internet.

En el DNS, en nombre del host es la porción izquierda del nombre del dominio. Cada porción (label) del nombre del dominio se separa por puntos con una longitud máxima de 63 caracteres por porción; por ejemplo.

Condor.dgsca.unam.mx

en este caso el nombre del host es condor y su dirección será:



cada número ocupa una posición que determina su nivel dentro de la red. (Figura 2.27)

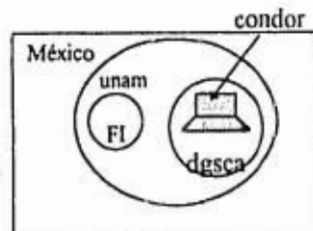


FIGURA 2.27 AUTORIDAD SOBRE DOMINIOS

SUBNETWORK

Capa que no se encuentra definida por TCP/IP, simplemente hace referencia a los protocolos de comunicación específicos empleados en cada tecnología de red en particular.

Aunque la mayoría de las redes que utiliza TCP/IP funcionan con 802.3 con el protocolo CSMA/CD, esto no significa que es la única topología que puede usar o el único protocolo con el que puede convivir. De hecho TCP/IP es independiente del medio de transmisión, de la topología y del protocolo de acceso al medio. Por lo tanto, es posible tener redes Arcnet (usando protocolo token passing), Token Ring, Ethernet, X.25 o enlaces satélites usando TCP/IP.

Los datagramas de IP pueden ser encapsulados dentro de tramas 802.3, 802.4 o 802.5. Una trama Ethernet que dentro de su campo de datos utiliza los protocolos TCP/IP se muestra en la figura 2.28.

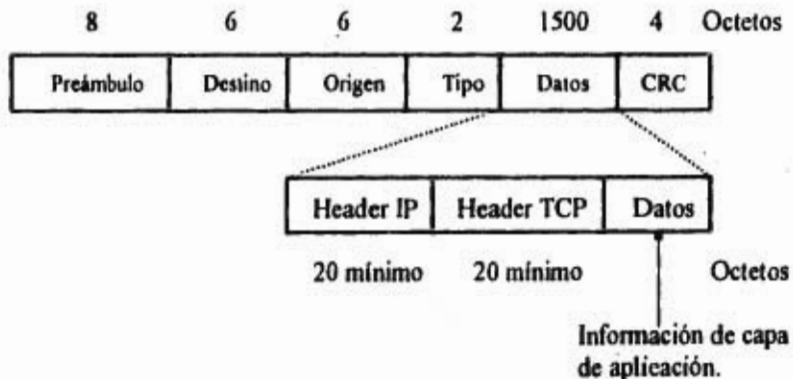


FIGURA 2.28 HEADERS TCP/IP DENTRO DE UNA TRAMA ETHERNET

2.3.6 SONET

SONET (Synchronous Optical Fiber) es un estándar basado en el trabajo desarrollado en Bellcore y estandarizado por ANSI (American National Standard Institute) T1-E1.2/92-020. Es compatible a SDH (Synchronous Digital Hierarchy) publicado por las recomendaciones del CCITT G.707, G708 y G.709. SONET intenta proveer una especificación para aprovechar todas las ventajas de transmisión digital de alta velocidad que ofrece la fibra óptica.

La principal razón para la creación de SONET fue proporcionar una solución a largo plazo para estandarizar los accesos a redes ópticas entre proveedores, es decir, permitir que el equipo de diferentes proveedores puedan comunicarse entre sí.

La segunda ventaja de SONET es que es síncrono, en la actualidad la mayoría de las redes con fibra y de los sistemas de multiplexaje son plesiosíncronos. Es decir, no existe un reloj de red al cual todos los elementos de la red se encuentren sincronizados. Por tanto la temporización puede variar de un equipo a otro. En las redes plesiosíncronas, una señal completa tenía que ser demultiplexada para ocupar un canal particular, por lo que los canales vacíos tenían que ser multiplexados de nuevo para ser enviados a través de la red hacia su propio destino. En un formato SONET, sólo aquellos canales que son requeridos en un punto particular son demultiplexados, debido a eso, se elimina la necesidad de un multiplexaje tras otro.

El estándar SONET contiene los siguientes puntos específicos:

1. Establece un formato de multiplexaje síncrono estándar usando cualquier número de señales de 51.84 Mbps con bloques estructurados.
2. Establece una señal óptica estándar para interconectar equipo de diferentes proveedores.
3. Establece capacidades de operaciones extensivas, administración y mantenimiento (OAM, Operations, Administration and Maintenance), como parte del estándar.

4. Define un formato de multiplexaje síncrono para llevar señales digitales de bajo nivel (DS-1, DS-2 y estándares CCITT).
5. Establece una arquitectura flexible capaz de soportar futuras aplicaciones tales como ISDN-B, con una variedad de tasas de transmisión.

Existen tres requerimientos claves que han dirigido el desarrollo de SONET

Primero fue la necesidad de empujar los estándares existentes al límite del nivel DS-3 (44.736 Mbps). Con el crecimiento de los sistemas de fibra óptica, un gran número de vendedores introdujeron sus propios esquemas de comunicación desde 2 hasta 12 DS-3 en una señal óptica. Además los esquemas europeos, basados en la jerarquía CCITT, son incompatibles con los sistemas norteamericanos.

SONET provee una jerarquía estandarizada de tasas de transmisión digital multiplexadas compatibles con las tasas Norteamericanas y CCITT compatibles.

El segundo requerimiento fue proveer acceso económico a pequeños montos de tráfico, dentro del volumen de una señal óptica. Para este propósito SONET introdujo una nueva aproximación al multiplexaje por división de tiempo.

El tercer requerimiento es prepararse para un servicio futuro sofisticado que se ofrecerá, tal como una red virtual privada. Y permitiendo las técnicas de transmisión ATM/ISDN-B, para reunir estos requerimientos, se necesitó un mayor incremento en las necesidades de manejo de la red dentro de una señal con división de tiempo síncrona.

Jerarquía de señales

La especificación SONET define una jerarquía de señales estandarizada, la cual se muestra en la tabla 2.5.

CAPITULO II. REDES LAN

DESIGNACION SONET	DESIGNACION CCITT	VELOCIDAD DATOS (MBPS)
STS-1/OC-1	-	51.84
STS-3/OC-3	STM-1	155.52
STS-9/OC-9	STM-3	466.66
STS-12/OC-12	STM-4	622.08
STS-18/OC-18	STM-6	933.12
STS-24/OC-24	STM-8	1,244.16
STS-36/OC-36	STM-12	1,866.24
STS-48/OC-48	STM-16	2,488.32

TABLA 2.5 JERARQUIA DE SEÑALES

A la señal de más bajo nivel de la jerarquía SONET se le llama STS-1 (Synchronous Transport Signal level-1) y las señales de niveles más altos se les llama señales STS-N. Una señal STS-N se compone de N señales STS-1. La contraparte óptica de cada señal STS-N es una señal OC-N (Optical Carrier level-N). Para el estándar SDH, la velocidad más baja es 155.52 Mbps, la cual es designada como STM-1 (Synchronous Transfer Mode level-1), esta corresponde a una señal STS-3 de SONET.

JERARQUIA DEL SISTEMA SONET

El estándar SONET sigue una jerarquía de cuatro capas la cual se muestra en la figura 2.29.

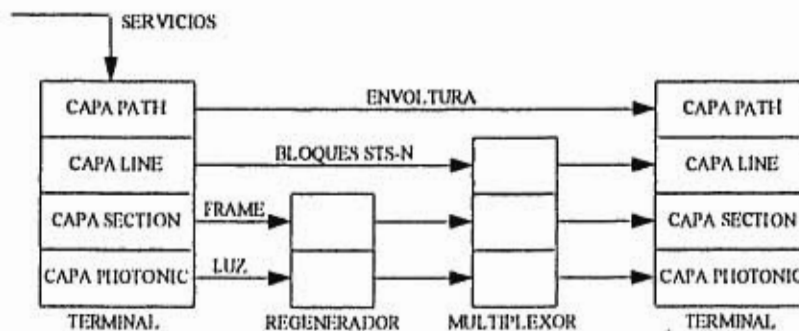


FIGURA 2.29 JERARQUIA LOGICA DEL ESTANDAR SONET

1. **Photonic.** Esta es la capa física, incluye una especificación del tipo de fibra óptica que puede ser usado y detalles tales como requerimientos mínimos de potencia y características de dispersión de los láseres de transmisión y requerimientos de sensibilidad de los dispositivos receptores. Esta capa es también responsable de convertir señales STS (eléctricas) a señales OC (ópticas).
2. **Section.** Esta capa crea las tramas básicas SONET, también incluye funciones de transmisión tales como monitoreo de errores.
3. **Line.** Esta capa es responsable de la sincronización, multiplexaje de datos dentro de tramas SONET y protección de la conmutación.
4. **Path.** Esta capa es responsable del transporte de fin a fin (end-to-end) de datos a una apropiada velocidad.

Una sección es el bloque básico estructurado físicamente y representa un recorrido único del cable entre dos transmisores y receptores de fibra óptica. Para distancias cortas, el cable puede ir directamente entre dos unidades terminales. Para distancias más largas, son necesarios repetidores/regeneradores.

El repetidor es un aparato simple que acepta un flujo digital de datos de un lado, regenera y repite cada bit del otro. Aspectos de sincronización y tiempo necesitan ser añadidos.

Una line es una secuencia de una o más sections tal que la señal interna o estructura de canal se mantiene constante. Puntos finales o intermedios multiplexores pueden añadir o tirar canales terminando una line. Finalmente un path conecta dos puntos finales, esto corresponde a un circuito end-to-end.

Los datos son montados en el comienzo de un path y no son accedidos o modificados hasta ser desmontados en el otro extremo del path. La figura 2.30 muestra la relación física de las capas lógicas.

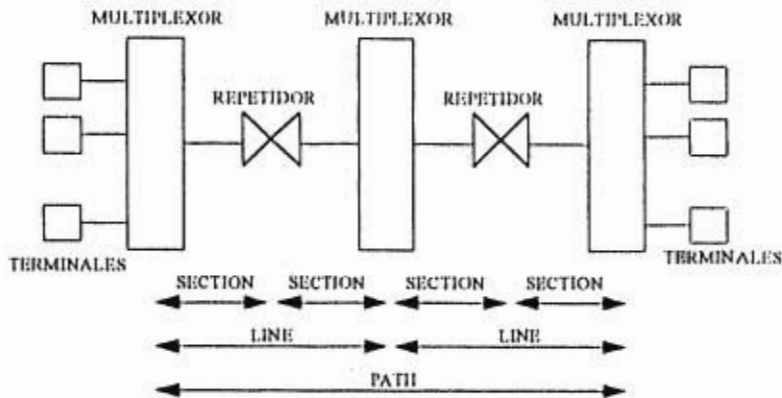


FIGURA 2.30 JERARQUIA FISICA DEL ESTANDAR SONET

FORMATO DE TRAMA

La estructura básica de un bloque SONET es la trama STS-1, la cual consiste de 810 octetos, y es transmitida una vez cada 125 μ s. La trama puede ser vista lógicamente como una matriz de nueve renglones de 90 octetos cada uno, como se muestra en la figura 2.31, comenzando la transmisión un renglón a la vez, de izquierda a derecha y de arriba hacia abajo.

Los tres primeros bytes de cada renglón son asignados para el encabezado de transporte. El encabezado de transporte está compuesto por el encabezado de sección y el encabezado de línea. El encabezado de ruta está contenido dentro del payload (carga de información), tal como se muestra en la figura 2.31.

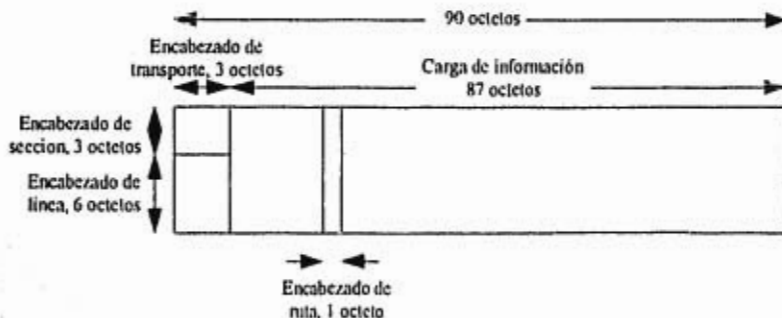


FIGURA 2.31 ESTRUCTURA BASICA DE UN BLOQUE SONET

La figura 2.32 muestra la ubicación de cada byte de los encabezados del estándar SONET. Estos bytes se describen a continuación.

Encabezado de sección

A1, A2: Bytes de alineación de trama, son usados para sincronizar el comienzo de la trama y tienen valores de F6 y 28 HEX, respectivamente.

C1: Número de identificación de STS-1 (1 a N).

B1: Supervisión del error de sección.

E1: Es un canal de voz opcional a nivel sección de 64 kbps PCM para transferencia de ordenes.

F1: Canal de 64 kbps para propósitos de usuarios.

D1-D3: Canales de comunicación de datos 192 kbps, para alarmas, control de mantenimiento y administración entre secciones.

Encabezado de línea

H1-H3: Bytes punteros, usados en el alineamiento de trama y ajuste de frecuencia de datos.

B2: bit intercalado de paridad para monitoreo de errores en el nivel de línea.

K1, K2: Estos dos bytes están asignados para señalización de conmutación de protección automática entre equipos.

D4-D12: Canales de comunicación de datos para alarmas, mantenimiento, monitoreo y administración a nivel de línea.

Z1, Z2: Reservado para uso futuro.

E2: Canal de voz 64 kbps PCM para transferencia de ordenes a nivel de línea.

Encabezado de trayectoria

J1: Canal de 64 kbps el cual transmite repetidamente una cadena con formato de 64 octetos. Esto permite a la terminal receptora dentro de la ruta verificar su conexión continúa a la terminal emisora.

B3: Byte de código de paridad intercalado de nivel de trayectoria.

C2: Etiqueta de señal de ruta, este byte es utilizado para indicar si el STS no ha sido equipado (valor = 0) o equipado (valor = 1).

G1: Byte de estado de ruta. Este byte es utilizado para indicar el estatus de la terminación de la ruta y el desempeño del equipo de terminación de la ruta que lo originó.

F2: 64 kbps, Canal de usuario de ruta. Este byte es utilizado para la comunicación del usuario con el resto de los elementos de la ruta.

H4: Byte indicador de multitrama, para cargas de información que necesitan más de una trama.

Z3-Z5: Reservado para uso futuro.

	Encabezado de transporte			STS-1 Carga de información	
Encabezado de sección	A1	A2	C1	J1	
	B1	E1	F1	B3	
	D1	D2	D3	C2	
Encabezado de línea	H1	H2	H3	G1 Encabezado de ruta	
	B2	K1	K2	F2	
	D4	D5	D6	H4	
	D7	D8	D9	Z3	
	D10	D11	D12	Z4	
	Z1	Z2	E2	Z5	
	3 columnas			87 columnas	

FIGURA 2.32 FORMATO DE TRAMA SONET

CAPITULO III

FDDI

3.1 PRINCIPIOS BASICOS DE OPERACION DE FDDI

3.1.1 INTRODUCCION

El estándar ISO 9314 (ANSI X3T9.5) describe una red que permite cubrir una área geográfica grande (100 km.) y una velocidad de datos de 100 Mbps. FDDI corre alrededor de un anillo al cual se conectan las estaciones (máximo 500).

El soporte físico generalmente consiste de fibras multimodo, en tal caso las estaciones pueden estar espaciadas una distancia de 2 km. proyectos recientes proponen el uso de par torcido a una distancia entre nodos limitada alrededor de 100 m.

Características relevantes del estándar FDDI

- 2 km. como distancia máxima entre dos estaciones.
- Es una red basada en fibra óptica multimodo 65.5/125 μ m.
- Usa el código 4B5B.
- 100 km. como circunferencia total del anillo.
- Permite un máximo de 500 estaciones enlazadas en el anillo.
- Velocidad de datos 100 Mbps.
- Topología en anillo doble.
- Baja tasa de error, en el peor de los casos una en un billón.
- Conmutadores ópticos opcionales.
- Tamaño de paquete variable, máximo 4500 bytes.
- Eficiencia del 80 %, con una frecuencia de 125 MHz.

3.1.2 COMPONENTES DEL PROTOCOLO FDDI

Como se vió en la sección 2.4 de esta tesis, los protocolos se dividen en capas o componentes para su mejor análisis, el protocolo FDDI no es la excepción. El estándar FDDI subdivide las capas física y de enlace de datos del modelo de referencia OSI en cinco componentes¹ como se muestra en la figura 3.1.

¹ Sólo los cuatro primeros componentes son capas o niveles, el quinto componente no es una capa pues este se comunica con todas las capas y no tiene una relación jerárquica con estos componentes.

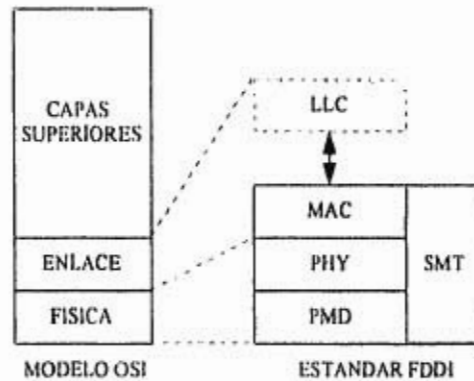


FIGURA 3.1 COMPONENTES DEL PROTOCOLO FDDI.

- 1) **PMD** (*Physical Layer Medium Dependent*). La capa PMD especifica las señales ópticas y la forma de onda en el cable de la fibra óptica. Además especifica un máximo de distancia de 2 km. entre estaciones. La máxima atenuación del anillo FDDI está establecido como 11 dB de fin a fin , este referido típicamente como 2.5 dB por km.
- 2) **PHY** (*Physical Layer Medium Independent*). La función de esta capa es la sincronización, codificación y decodificación de señales. FDDI usa una codificación 4B5B la cual provee una eficiencia del 80 % para 125 MHz de velocidad de señalización, el tamaño máximo de trama FDDI es de 4500 bytes el cual se especifica en esta capa.
- 3) **MAC** (*Media Access Control*). La función de la capa del MAC es transferir datos al anillo y sacarlos de este, formar la tramas, reconocer la dirección de las estaciones y la generación y verificación de trama (FCS).
- 4) **LLC** (*logical Link Control*). Este componente multiplexa/demultiplexa los paquetes recibidos de los diversos niveles de protocolos de red. FDDI usa LLC como es especificado por el estándar IEEE 802.2.
- 5) **SMT** (*Station Management*). Este componente del estándar FDDI tiene como funciones principales: iniciar la configuración del anillo, monitoreo de bit de errores, localizar y aislar fallas automáticamente, administración del anillo y reconfiguración de la red.

De estos cinco componentes sólo cuatro son especificados por el estándar FDDI, el componente LLC es especificado por el estándar IEEE 802.2.

3.1.3 CONFIGURACIONES DE REDES FDDI

TIPOS DE NODOS

La topología física de una red FDDI puede ser, un anillo, una estrella o una malla, pero la configuración lógica de la topología es un anillo doble. Un anillo llamado el principal es el que transporta los datos, el anillo secundario actúa como respaldo en caso de una falla en el anillo primario. La topología permite dos tipos de conexión (figura 3.2):

- Acceso al doble anillo (nodos tipo A)
- Acceso a un sólo anillo (nodos tipo B)

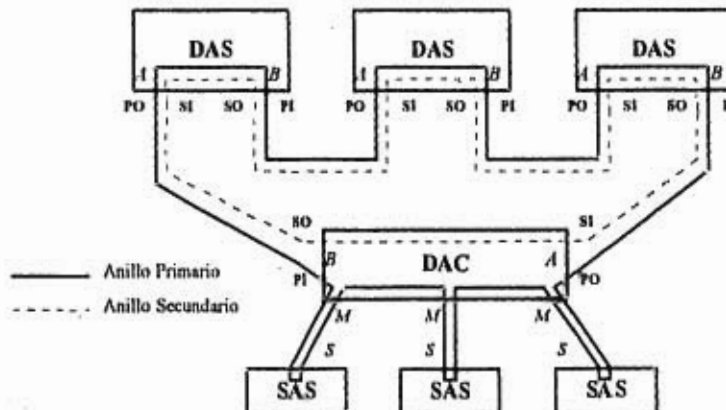


FIGURA 3.2 ESTRUCTURA GENERAL DE UNA RED FDDI

Existen cuatro tipos de nodos:

DAS (Dual Attachment Stations). Las estaciones con doble enlace tienen dos puertos conocidos simplemente como puerto *A* y puerto *B* (figura 3.2). Cada puerto puede transportar datos en dos direcciones; aunque en operación normal, sólo una dirección es usada. En un anillo doble, el puerto *A* conecta al puerto *B* de una estación vecina y viceversa. Con el anillo primario funcionando el puerto *A* recibe datos de la entrada primaria (PI), entonces el puerto *B* transmite en la salida primaria (PO). Cuando el anillo secundario, por alguna razón, entra en operación, el puerto *A* transmite en la salida secundaria (SO) y el puerto *B* recibe en la entrada secundaria (SI).

DAC (Dual Attachment Concentrators). La función primaria de un concentrador es extender el anillo primario y algunas veces el secundario bajo un árbol. Esto se hace vía *M* o puertos maestros, los cuales proveen un enlace único para una única estación, esta estación puede ser incluso otro concentrador. El anillo primario es extendido para cada uno de los puertos *M*, vía una ruta interna.

SAS (Single Attachment Stations): La forma más simple de una estación, es la estación con enlace único o SAS como comúnmente se le conoce. Un sólo par de fibras permite la transmisión y recepción de datos vía un puerto llamado esclavo o *S*. Este tipo de conexión es el que más se usa por estaciones de trabajo (*workstations*) o computadoras personales. Un puerto *S* siempre está conectado a un puerto *M* de un concentrador.

SAC (Single Attachment Concentrators): Los concentradores con enlace único son internamente muy similares a la arquitectura de los DAC's excepto que los puertos *A* y *B* son reemplazados por un único puerto llamado puerto *S*.

APLICACIONES DE ANILLOS FDDI

FDDI es una red versátil que puede ser usada en una variedad de aplicaciones. Existen tres tipos de redes de computadoras en las cuales puede ser usada FDDI (figura 3.3). Redes *Back-end*, *Front-end* y *Backbone*. A continuación se describen las características de estas aplicaciones.

- **Back-End:** La red usada para conectar un procesador con aparatos de almacenamiento es llamada red *back-end*. Estas redes generalmente están localizadas en un sólo local y se caracterizan por tener enlaces cortos de menos de 30 m. pero un intenso tráfico.
- **Front-End:** Las redes usadas para conectar servidores a estaciones de trabajo son llamadas redes front-end. Estas redes típicamente son usadas en edificios de oficinas, abarcando uno o más pisos, y se caracterizan por tener un gran número de estaciones de trabajo y computadoras personales conectadas.
- **Backbone:** Las redes usadas para conectar muchas redes son llamadas redes backbone. Esta configuración puede ser usada para conectar redes FDDI, redes IEEE 802.3/ETHERNET, y/o redes 802.5/TOKEN RING en diferentes edificios. Una red de Backbone consiste en un pequeño número de enlaces de larga distancia.

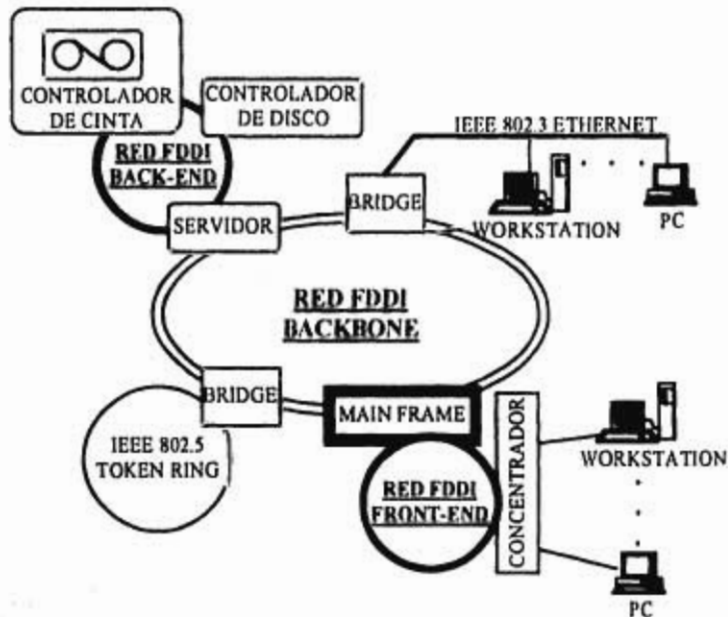


FIGURA 3.3 APLICACIONES DE ANILLOS FDDI

3.1.4 MECANISMOS PARA SUPERAR FALLAS EN EL ANILLO

El principal problema en el desarrollo de redes con topología en anillo es la tolerancia a las fallas. Estrictamente hablando un anillo consiste en muchas estaciones conectadas en serie, la probabilidad de que falle la red se incrementa exponencialmente con el número de estaciones. Para soportar fallas en redes de anillo se han desarrollado varias técnicas en los últimos años. De estas técnicas, las siguientes son relevantes dentro del concepto de FDDI.

Estación bypass: Una correcta aproximación para tolerar fallas en las estaciones, es el uso de los *bypass* ópticos que automáticamente aíslan una estación y permiten la operación continúa del anillo.

Un *bypass* permite que una estación sea desconectada del anillo. En el modo de paso, la señal óptica que entra es pasada directamente a la siguiente estación como se muestra en la figura 3.4, ya que una estación SAS está siempre conectada a un concentrador, estos pueden ser fácilmente puenteados por el concentrador y no necesitarán usar *bypasses* ópticos.

Cuando una estación es puesta en estado de paso, esta estación se encuentra en *loop* de tal manera que el transmisor y receptor de un puerto son conectados al receptor y transmisor, respectivamente, del otro puerto.

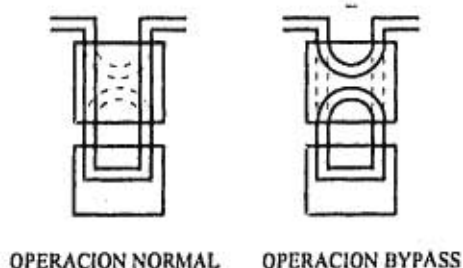


FIGURA 3.4 ESTADOS DEL BYPASS OPTICO.

Características de funcionamiento de los bypass

- a) **Baja atenuación:** Cuando una estación es puenteada, dos enlaces de fibra son unidos como se muestra en la figura 3.5. Este nuevo enlace combinado debe satisfacer todos los requerimientos de un único enlace. En particular la longitud total debe ser menos de 2 km; la atenuación total del enlace debe ser menos de 11 dB, la máxima atenuación permitida para bypass en 2.5 dB.
- b) **Alto aislamiento de canales:** Puesto que las señales de luz de ambos anillos, primario y secundario, viajan hacia el bypass, existe una posibilidad de interferencia, por esto es deseable que la señal óptica de un anillo tenga un mínimo efecto sobre el otro anillo. Esto es llamado aislamiento de canal. El estándar requiere que el aislamiento sea por lo menos de 40 dB.

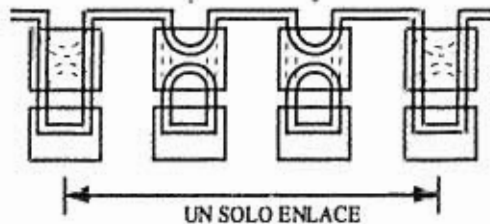


FIGURA 3.5 DESPUES DEL PUENTE SE FORMA UN SOLO ENLACE

- c) **Rápida conmutación:** Después de que el bypass es instruido para quitar o insertar una estación del anillo, debe realizarlo rápidamente. El máximo tiempo de conmutación permitido son 15 ms.
- d) **Mínima interrupción:** Cuando una estación es puenteada los anillos son interrumpidos brevemente. Este tiempo de interrupción del medio debe ser el mínimo posible. El máximo tiempo permitido son 15 ms.

Anillo doble: Mientras un *bypass* permite mantener el anillo en caso de que falle una estación, el anillo es aún susceptible a fallas en el cable. Una falla en cualquier cable puede detener la operación del anillo. Para resolver este problema se propuso el uso de un cable de respaldo en espera, para cada cable de la red. Esto da lugar a una configuración de anillo doble tal como se muestra en la figura 3.6.

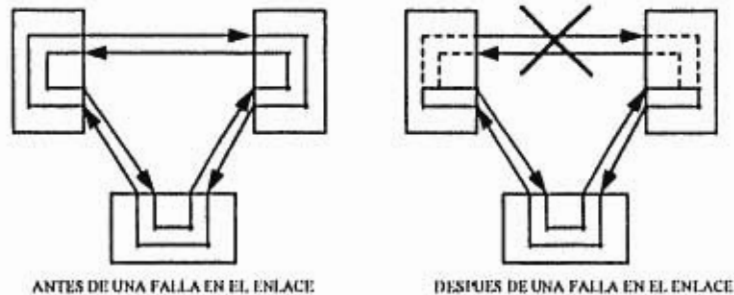


FIGURA 3.6 EN UNA TOPOLOGIA DE ANILLO DOBLE

Esta técnica fue propuesta para permitir que continúe la operación del anillo, aún cuando ambos cables entre un par de estaciones vecinas se rompan. Cuando ocurre un falla las estaciones que están conectadas a las terminales del cable roto reconfiguran sus rutas internas manteniendo el anillo y conectando todas las estaciones. Este tipo de configuración es llamada *wrapping*.

FDDI fue el primer estándar de Token Ring que adoptó una topología de anillo doble para cubrir fallas. Ahora esta técnica es usada por otros estándares que usan token ring, incluyendo IEEE 802.5/Token Ring.

Anillo en forma de estrella: Saltzer and Program del instituto tecnológico de Massachusetts propusieron el uso de un anillo en forma de estrella en el cual todos los cables de las estaciones están conectados a un concentrador. La idea de tener todos los cables conectados a este concentrador puede hacer más fácil el monitoreo del estado de todas las conexiones y así aislar las estaciones o cables que no están operando correctamente. Figura 3.7

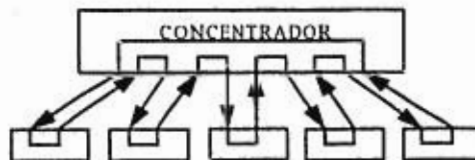


FIGURA 3.7 TECNICA DE ANILLO EN FORMA DE ESTRELLA

El uso de concentradores, anillos dobles y *hypasses* hace a FDDI extremadamente tolerante a fallas.

3.2 TRAMA DE FDDI

3.2.1 FORMATO DE TRAMA FDDI

La figura 3.8 describe el formato de trama para el protocolo FDDI. El estándar define el contenido de este formato en términos de símbolos. Con cada símbolo correspondiente a 4 bits. Los símbolos son usados porque la capa física de datos codifica y transmite partes en un código llamado 4B5B, el cual se vera en la sección 3.2.2.

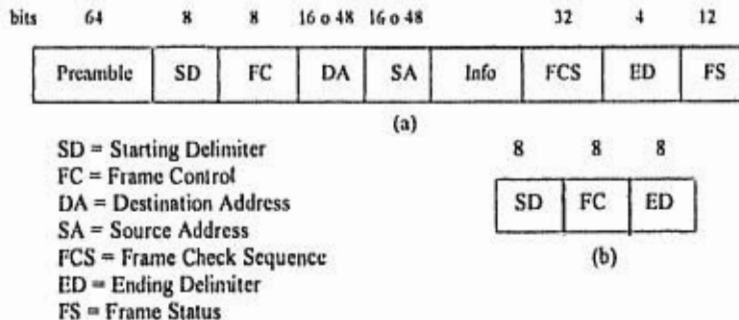


FIGURA 3.8 (a) FORMATO GENERAL DE TRAMA (b) FORMATO DE TOKEN

El formato de trama general de FDDI consiste en los siguientes campos:

Preamble

Sincroniza la trama con el reloj de cada estación. El originador de la trama usa un campo de 16 símbolos "1" ociosos, este símbolo "1" se codifica como 11111 según se muestra en la tabla 3.2; subsecuentemente puede cambiar la longitud del campo siguiendo los requerimientos de sincronía. Estos símbolos ociosos no son datos. El preámbulo le da a una estación un tiempo de respiro entre recepción de tramas sucesivas. Durante este tiempo, la estación puede reiniciar la tabla de estados y la ruta de datos. La estación puede no tener suficiente tiempo de hacer esto si el preámbulo es muy corto.

Starting Delimiter (SD)

El delimitador de inicio indica el comienzo de la trama. Esta formado por los simbolos J-K, los cuales se codifican en el código 4B5B como 11000 y 10001, respectivamente. Este es un patrón de bits único que puede ser identificado por un nodo FDDI a cualquier hora en el flujo de recepción de datos.

Frame Control (FC)

El campo de control de trama indica la clase de servicio, la longitud del campo de dirección y el tipo de trama. El formato del campo de control se muestra en la figura 3.9.

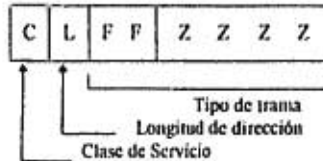


FIGURA 3.9 FORMATO DEL CAMPO DE CONTROL DE TRAMA

El primer bit denotado como C indica la clase de servicio. Un 0 indica una clase de servicio asincrono y un 1 indica una clase de servicio síncrono. El segundo bit denotado por L indica la longitud de la dirección fuente y destino. Un 0 indica direcciones de longitud corta (16 bits), mientras que un 1 indica direcciones de longitud larga (48 bits). Los siguientes 6 bits indican el tipo de trama. La tabla 3.1 muestra las posibles combinaciones en el campo de control de trama.

C	L	F	F	Z	Z	Z	Z	
0	X	0	0	0	0	0	0	Trama vacía
1	0	0	0	0	0	0	0	Token no restringido
1	1	0	0	0	0	0	0	Token restringido
1	L	0	0	0	0	1	1	Trama MAC de petición de token
1	L	0	0	0	0	1	0	Trama MAC de errores
0	L	0	0	1	1	1	1	Tramas SMT
0	L	0	1	0	P	P	P	Tramas asincronas LLC
1	L	0	1	0	0	0	0	Tramas síncronas LLC
C	L	1	0	0	X	X	X	Reservado para implementaciones
C	L	1	1	0	0	0	0	Reservado para estandarización futura

TABLA 3.1 TIPOS DE TRAMA FDDI

A continuación se describen con más detalle los tipos de trama señalados en la tabla 3.1.

1. *Tramas LLC*: Este es el tipo de tramas que más comúnmente se ven sobre un anillo FDDI. Los bits FF en el campo de control de trama de tramas LLC son 01. Para tramas asíncronas los últimos tres bits indican la prioridad de la trama. Cero es la más baja prioridad y siete es la más alta. El cuarto bit marcado como "r" es reservado y debe ser puesto a 0. Para tramas sincronicas no existen prioridades. Todos los bits Z son reservados y puestos a 0000.
2. *Tokens*: El valor del campo de control de trama 1000-0000 y 1100-0000 indican un token no restringido o token restringido, respectivamente.
3. *Tramas MAC*: Las tramas MAC son indicadas por 1L00-ZZZZ en el campo de control de trama. Los bits ZZZZ definen el tipo de trama MAC. Dos tipos de tramas MAC que son usadas para la inicialización del anillo y la reparación de una falla son la trama de petición de inicio de token (*claim frame*) y tramas de aviso y detección de una falla (*beacon frame*) cuyos valores son indicados como 1L00-0011 y 1L00-0010, respectivamente.
4. *Tramas SMT*: Las tramas de administración de estación están indicadas por 0L00-ZZZZ en el campo de control de trama. Los últimos cuatro bits fueron originalmente pensados para indicar el tipo de tramas SMT. No obstante sólo se han definido dos tipos de valores. Un valor de 0100-0001 es usado por la mayoría de las tramas SMT y el valor 0100-1111 es usado para indicar la dirección de la estación siguiente (NSA). En este caso la dirección destino especificada es generalmente un grupo o una dirección de *broadcast*.
5. *Tramas vacías*: El valor en el campo de control de este tipo de tramas es puesto como 0X00 0000. Este tipo de tramas son usadas como marcadores en muchos algoritmos de asociación de acceso al medio. Por ejemplo, algunos puentes las usan para marcar el fin de una secuencia de transmisión.

6. *Tramas de implementación:* El valor CL10-0XXX en el campo de control de trama es reservado para implementaciones en la red. Los vendedores pueden usarles en la forma que les parezca. El bit r está reservado y debe ser puesto a 0. El uso de los otros bits es dejado a los implemetadores. La presencia del campo de información es opcional. Debido a que no es muy claro como diferentes vendedores pueden coordinarse para usar estas tramas, tales tramas no han sido usadas por nadie.
7. *Tramas reservadas:* El valor de CL11-0000 en el campo de control de trama es reservado para futura estandarización.

Destination Address (DA)

Especifica la dirección de la estación o estaciones a la cual está dirigida la trama. El campo DA puede contener la dirección de una única estación, de un grupo de estaciones (*multicast*) o de todas las estaciones (*broadcast*) El estándar FDDI usa el mismo formato de direcciones que los estándares IEEE 802.3 o Ethernet de Xerox, tal como se muestra en la figura 3.10.

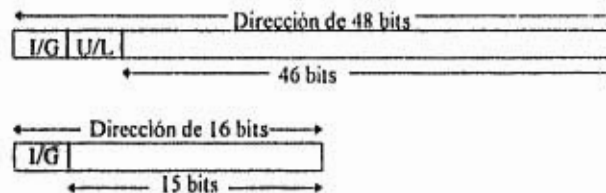


FIGURA 3.10 FORMATO DE DIRECCION DESTINO DE 16 Y 48 BITS

El primer bit transmitido es el bit I/G (Individual/Group). El bit I/G es puesto a 0 para indicar que la dirección es de una estación individual. Y el bit I/G es puesto a 1 para indicar que la dirección esta asociada con un grupo de estaciones. El siguiente bit en la dirección de 48 bits es el bit U/L (Universal/Local). El bit U/L es puesto a 0 para indicar el uso de un plan de direcciones universal administrado por una autoridad central, como el IEEE. Y es puesto a 1 para indicar el uso de un plan de direcciones administrado localmente.

Los restantes 15 o 46 bits contienen la dirección actual, si todos los bits son puestos a 1, esta es una dirección de difusión (*broadcast*) y el mensaje será enviado a todas las estaciones. En el caso de un plan de direcciones administrado universalmente, los primeros 22 bits son típicamente una organización o una red y los restantes 24 bits son asignados localmente. En el caso de un grupo de direcciones, es responsabilidad de las estaciones que están sobre la red entender como interpretar apropiadamente las direcciones. Una dirección nula, en la cual todos los bits son 0, no es interpretada por las estaciones como dirección.

Source Address (SA)

Especifica la dirección de la estación que envía la trama. El formato de la dirección origen es el mismo que el estándar 802.3 o Ethernet de Xerox, este se muestra en la figura 3.11.

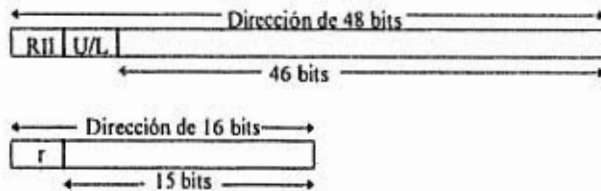


FIGURA 3.11 FORMATO DE DIRECCION ORIGEN DE 16 Y 48 BITS

El primer bit del campo SA de 48 bits es el bit RII (bit indicador de información de ruteo). El bit RII es puesto a 1 para indicar la presencia del campo de información de ruteo en esta trama; de otra manera el bit RII es puesto a 0. El segundo bit es el bit U/L. El primer bit del campo SA de 16 bits está actualmente reservado y puesto a 0.

Information

El campo de información es usado para transmitir la carga de información por la trama y puede consistir de cualquier número de símbolos desde 0 hasta un máximo limitado por el número total de símbolos permitidos en la trama del estándar FDDI (9000 símbolos o 4500 bytes).

Además habrá que tomar en cuenta los símbolos que definen los otros campos de la trama. En tramas con direcciones de 16 bits son permitidos 4488 bytes de carga, mientras que en tramas con direcciones de 48 bits esta carga se reduce a 4480 bytes.

El contenido del campo de información depende del tipo de trama de que se trate. Por ejemplo, cuando se están transportando datos de control de una trama tipo MAC un total de 4 bytes son usados para transportar la información de control tal como se ilustra en la figura 3.12. Para una trama de tipo LLC la cual es usada para transportar datos y protocolos de capas superiores, el campo de información puede transportar la capacidad máxima. Por ejemplo 4488 bytes.

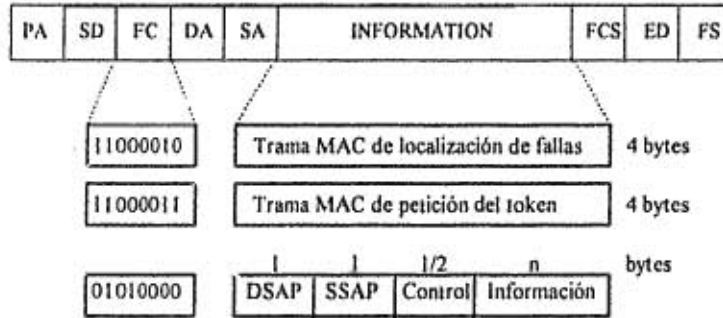


FIGURA 3.12 EJEMPLO DEL CONTENIDO DEL CAMPO DE INFORMACION

Frame Check (FCS)

FDDI usa un chequeo de redundancia cíclica de 32 bits para asegurar que el contenido de la trama está libre de errores. El polinomio CRC es el mismo que se usa en Ethernet, Token Ring y otros protocolos IEEE 802. Este polinomio es:

$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$$

Este chequeo es aplicado a los campos de FC, DA, SA, y de información.

El procedimiento puede ser explicado como sigue. Teniendo una trama o un mensaje M de k bits, el transmisor con ayuda de un polinomio G de $n+1$ bit, genera una secuencia de n bits conocido como el FCS (Secuencia de chequeo de trama). Entonces se añade el FCS a la trama a transmitir obteniendo T de $k+n$ bits.

$$T = M + \text{FCS}$$

El lado receptor llega T y es dividido entre el polinomio $G(x)$ que origino a FCS. Si no existe residuo en esta división, quiere decir que no hay errores en la transmisión y recepción de datos.

Procedimiento del calculo del CRC:

Un mensaje puede ser representado como un polinomio, los bits del mensaje son numerados secuencialmente de derecha a izquierda, el bit más a la derecha es llamado el bit cero. En esta representación polinomial, el bit i es usado como coeficiente de x^i . por ejemplo :

el número de 5 bits 10011 es representado por el polinomio :

$$1x^4 + 0x^3 + 0x^2 + 1x^1 + 1 = x^4 + x + 1$$

El calculo del CRC de n bits sigue los siguientes pasos :

1. Los primeros n bits del mensaje son complementados.
2. Se multiplica el polinomio obtenido en el paso anterior por x^n .
3. El resultado del paso anterior es dividido entre el polinomio CRC original.
4. El residuo de la división es complementado y colocado en los bits más a la derecha.

Ejemplo : considere el mensaje de 10 bits 1100110111_2 . Supóngase que se quiere calcular el CRC de 4 bits usando 10011 como el polinomio CRC. El polinomio del mensaje es :

$$x^9 + x^8 + x^5 + x^4 + x^2 + x + 1$$

siguiendo los pasos para el calculo del CRC tenemos :

1. Los primeros 4 bits del mensaje son complementados, entonces obtenemos 001111011_2 . El resultado de este número se representa por el polinomio

$$x^7 + x^6 + x^5 + x^4 + x^2 + x + 1$$

2. Multiplicado este por x^4 obtenemos

$$x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x^4$$

3. El resultado es dividido por el polinomio $x^4 + x + 1$, El residuo de esta división es $x^3 + x^2 + x + 1$, el cual corresponde a 1111_2 .

4. Complementado el residuo obtenemos 0000_2 el cual lo añadimos al mensaje que deseamos transmitir 11001101110000_2 .

Ending Delimiter (ED)

Contiene uno o dos símbolos y marca el final de la trama, excepto por el campo FS. El delimitador ED tiene una longitud de 8 bits para el token y una longitud de 4 bits para todas las demás tramas. El delimitador ED coloca dos símbolos T (01101) en el token y un sólo símbolo T en las demás tramas

Frame Status (FS)

Una trama FDDI contiene tres o más campos indicadores del estado de la trama. De estos los tres primeros son definidos como indicadores E, A y C. Estos reflejan un error, reconocimiento de dirección y el copiado de una trama. Si el indicador E es puesto quiere decir que un error fue detectado en la trama. La estación que transmite pone el indicador E como una "R". cada estación checa la trama y si un error es detectado el indicador E se pone como "S". El indicador A como otros indicadores es puesto como "R" por la estación que transmite, si alguna estación reconoce la dirección destino pone el indicador A como una "S" y la estación transmisora se percata que la dirección esta en el anillo. El indicador C es también puesto como "R" y si alguna estación copia la trama deberá poner el indicador C como una "S".

Comparando este formato de trama con el de IEEE 802.3 puede notarse que ambos formatos son muy similares. La trama de FDDI incluye un campo llamado preámbulo el cual ayuda a la sincronización, este es necesario debido a una más alta velocidad de datos. Ambas direcciones de 16 y 48 bits son permitidas en la misma red en el estándar FDDI ; esta es una estructura más flexible que la usada por todos los estándares IEEE 802.

3.2.2 CODIFICACION DE BITS EN FDDI

Para alcanzar una gran eficiencia, el estándar FDDI especifica el uso de una codificación llamada 4B5B. En esta estructura cada cuatro bits de datos son codificados a un símbolo con cinco celdas, tales que cada celda contiene un único elemento de señal (presencia o ausencia de luz). En efecto cada cuatro bits son codificados a cinco bits, logrando una eficiencia del 80 % con 125 MHz.

Para entender como el código 4B5B logra la sincronización necesitamos saber que existe una segunda etapa de codificación : cada celda del código 4B5B es tratada como un valor binario y codificada usando la técnica NRZI como se muestra en la figura 3.13. En este código un 1 binario es representado con una transición en el comienzo del intervalo de bit y un 0 es representado con la ausencia de esta transición. Un beneficio de este código es que generalmente es más confiable detectar una transición en presencia de ruido y distorsión.

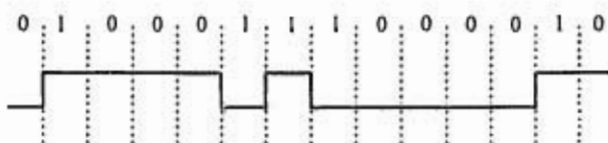


FIGURA 3.13 CODIFICACION NRZI

La tabla 3.2 muestra como se codifican los símbolos en FDDI. Cada posible combinación con cinco celdas es mostrada, aunque sólo 16 de 32 posibles combinaciones son necesarias para codificar datos.

CAPITULO III. FDDI

Código de bits	Símbolo	Asignación
Símbolos de Datos		
11110	0	0000
01001	1	0001
10100	2	0010
10101	3	0011
01010	4	0100
01011	5	0101
01110	6	0110
01111	7	0111
10010	8	1000
10011	9	1001
10110	A	1010
10111	B	1011
11010	C	1100
11011	D	1101
11100	E	1110
11101	F	1111
Símbolos del estado de línea		
00000	Q	Callado
11111	I	Ocioso
00100	H	Interrumpido
11000	J	Primer símbolo del delimitador de inicio
10001	K	Segundo símbolo del delimitador de inicio
00101	L	Fija Delimitador
01101	T	Usado para terminar el flujo de datos
00111	R	Indica un cero lógico (reset)
11001	S	Indica un uno lógico (set)
Asignación de códigos inválida		
00001	VH	Violación o paro
00010	VH	Violación o paro
00011	V	Violación
00110	V	Violación
01000	VH	Violación o paro
01100	V	Violación
10000	VH	Violación o paro

TABLA 3.2 CODIGO 4B5B

3.3 CONTROL DE ACCESO AL MEDIO

3.3.1 PROTOCOLO MAC DE FDDI

El MAC (Control de Acceso al Medio) de FDDI usa un protocolo de token calculado (Timed-Token Protocol, TTP) para ofrecer clases de servicio síncrono y asíncrono a todas las estaciones del anillo. El TTP preasigna una cantidad fija de ancho de banda a cada estación para transmisiones síncronas. Para transmisiones asíncronas el ancho de banda no es preasignado, sino que se asigna dinámicamente según las necesidades de transmisión asíncrona.

En algunos casos, el anillo de FDDI trabaja como un anillo de token regular. La información se transmite en forma serial de una estación a la siguiente. Cada estación regenera y repite los bits. La estación que tiene acceso al medio coloca bits sobre el anillo, y la estación que reconoce su dirección, en el campo de dirección destino, copia la trama y la vuelve a transmitir. La estación que transmite es responsable de quitar la trama que colocó sobre el anillo.

Una estación tiene el derecho de transmitir cuando esta detecta el token. La estación puede capturar el token quitándolo del anillo y entonces puede transmitir una o más tramas, cuando se ha terminado de colocar la información, la estación coloca un nuevo token sobre el anillo, permitiendo a otra estación acceder al medio. Un ejemplo de operación de un anillo de FDDI se muestra en la figura 3.13.

Muchos parámetros de medida de tiempo afectan la operación de una red FDDI. A diferencia de un anillo con token regular, una variable medida en tiempo indica a una estación FDDI cuanto tiempo esperar al siguiente token. Si el token llega temprano (antes de que el tiempo expire) la estación transmite datos síncronos y entonces, opcionalmente puede transmitir datos asíncronos. Si el token llega tarde (después de que el tiempo ha expirado), la estación sólo podrá mandar datos síncronos.

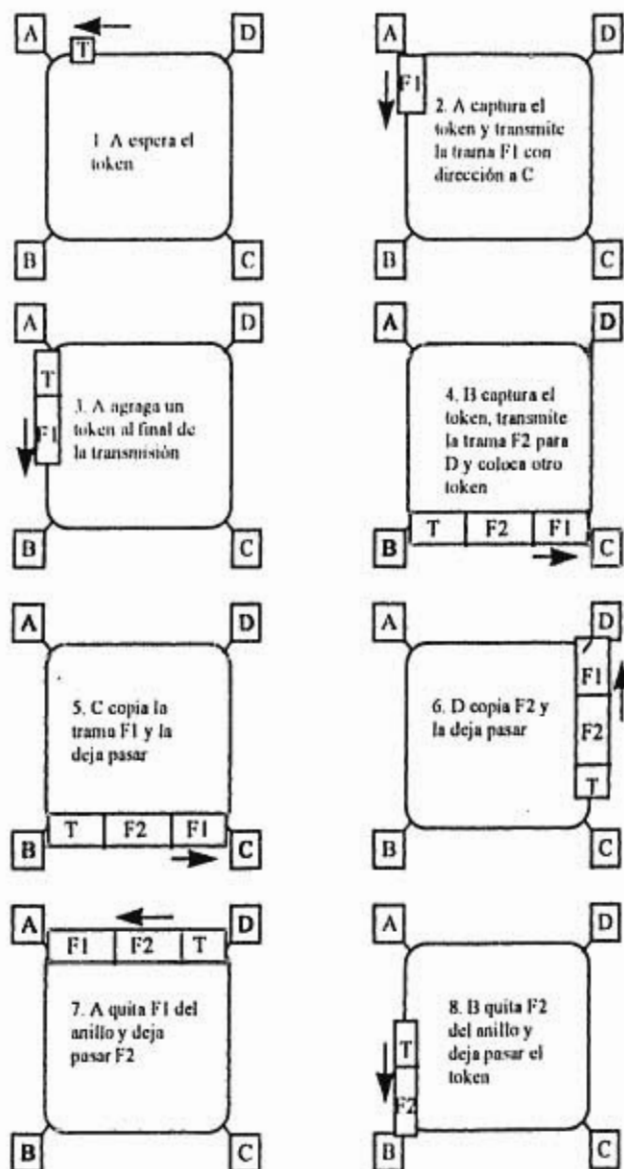


FIGURA 3.13 EJEMPLO DE OPERACIÓN DE UN ANILLO FDDI

3.3.2 PARAMETROS DE TIEMPO EN UN ANILLO FDDI

El MAC de una estación FDDI debe mantener tres tiempos para el control de la operación del anillo, estos parámetros se describen a continuación :

Token-Rotation Timer (TRT, tiempo de rotación del token). El propósito del TRT es controlar el tiempo que le toma al token atravesar el anillo completamente y regresar a una estación en particular. También controla el acceso asíncrono al anillo durante la operación normal. Durante la inicialización del anillo, todas las estaciones acuerdan un *Target Token Rotation Time* (TTRT, tiempo de rotación del token como objetivo o meta), el cual es el promedio esperado de tiempo entre llegadas de token a cada estación. El TRT es inicializado al valor de TTRT y comienza a contar hacia abajo, si el token es recibido antes de que expire TRT, se dice que el token llegó temprano. En este caso la estación puede mandar tramas asíncronas durante un tiempo equivalente a la llegada temprana del token. Si TRT expira antes de que llegue el token, éste se considera como retardado y la estación no podrá mandar ninguna trama asíncrona.

Token-Holdin Timer (THT, Tiempo de sostenimiento del token). Es usado para determinar cuanto tiempo puede transmitir una estación tramas asíncronas una vez capturado el token. Si el token llega temprano, la estación puede transmitir tramas asíncronas por un periodo de tiempo igual a

$$THT = TTRT - TRT$$

hasta que THT llegue a cero segundos.

Para mantener la estructura de prioridades asíncronas, son definidos 8 diferentes umbrales de tiempo, denotados como $T_Pri[i]$ donde i se refiere al nivel de prioridad. Las tramas asíncronas de prioridad i pueden ser transmitidas sólo si

$$T_Pri[i] < THT$$

El valor de $T_Pri[i]$ decrece hasta los niveles más bajos de prioridad, esto garantiza que las tramas con más prioridad sean transmitidas.

Valid-Transmission Timer (TVX, tiempo de transmisión valido). Cada estación sobre el anillo de FDDI continuamente monitorea la correcta operación del anillo. Si una condición invalida, tal como presencia de ruido por un periodo largo de tiempo, es detectada, entonces comienza el proceso de recuperación de la falla. Este monitoreo es hecho usando un temporizador llamado TVX. Cada estación tiene este temporizador o alarma que es reinicializado cada vez que la estación recibe un token o una trama. Si la estación no ve el token o un trama durante el tiempo TVX entonces indica una condición de error en el anillo.

El TVX es un parámetro de la estación y puede ser fijado por el administrador de la red o de la estación. El valor de TVX debe ser fijado tal que, un error de una o dos tramas, no ocasione la reinicialización del anillo. El valor por default del TVX a sido fijado a 2.5 ms. para el modo básico y 3.6 ms. para el modo híbrido. Si durante este periodo la estación no ve tokens o tramas, el tiempo expira y el anillo es reinicializado.

3.3.3 OPERACIÓN DEL ANILLO FDDI

El MAC de FDDI usa una estructura de control distribuido, tal que todas las estaciones participan de igual manera en el control y operación de la red. El token circula en el anillo de tal manera que sólo una estación puede capturar el token a la vez, después de conseguir el token la estación puede enviar datos y entonces generar un nuevo token.

Durante la inicialización del anillo el TTRT es establecido. Cada estación sobre la red espera ver el token cada TTRT segundos. El valor TTRT es determinado tal que el tiempo promedio de rotación del token (o tiempo de respuesta sincrónico promedio) no sea más grande que TTRT, y el máximo tiempo de rotación del token (o máximo tiempo de respuesta sincrónico) no sea mayor que $2 \times \text{TTRT}$.

La figura 3.14 describe en forma sencilla la operación del MAC de FDDI, así como la transmisión de tramas y la relación entre las variables de tiempo.

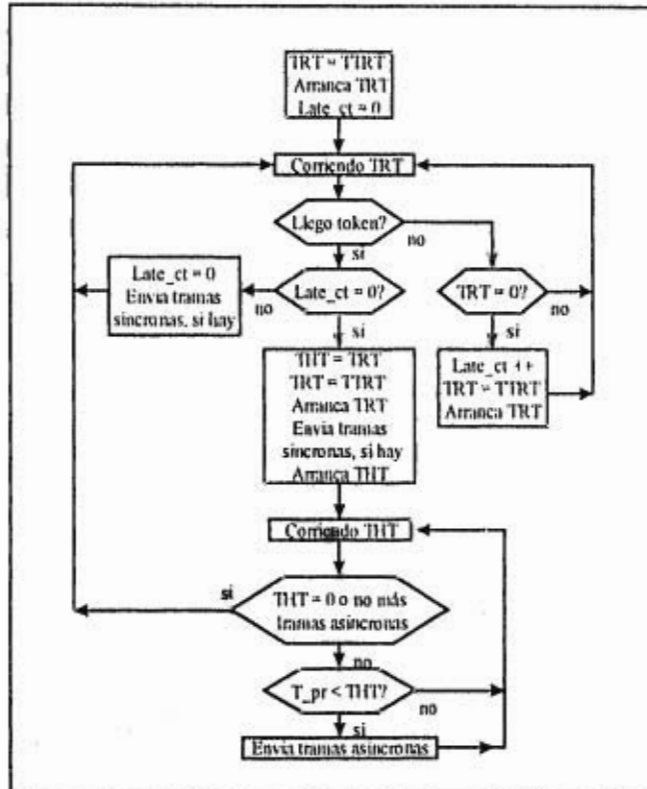


FIGURA 3.14 OPERACIÓN Y RELACION DE VARIABLES EN EL MAC DE FDDI

Cada estación mantiene un TRT para monitorear la cantidad de tiempo que transcurre entre llegadas del token. El TRT es inicializado y puesto al valor de TTRT, cuando empieza a correr este disminuye a cero. Si el token no llega a la estación antes de que el TRT expire, una variable llamada *late-counter* (Late_ct) o contador de retardo es incrementada. La variable Late_ct es inicializada y puesta a cero, y es reinicializada siempre que llega un nuevo token.

Si Late_ct no es cero cuando llega el token, el token es considerado como retrasado; si Late_ct es cero y TRT está aún corriendo cuando el token llega, entonces se dice que el token llegó temprano. La acción tomada por el MAC en la recepción del token está sujeta a la situación de llegada temprana o tardía del token.

Si el token llega temprano (Late-ct = 0 y TRT aún está corriendo) quiere decir que se tiene algún tiempo extra para que la estación envíe tramas asíncronas, si las tiene, cuando el token llega, el valor actual de TRT es asignado a la variable THT, entonces el TRT es reasignado al valor de TTRT y entonces TRT es inicializado y comienza otra vez a contar hasta cero.

Cada estación tiene una asignación conocida de ancho de banda síncrono, definido durante la inicialización del anillo. La suma de la asignación síncrona del ancho de banda de todas las estaciones no puede exceder el máximo ancho de banda síncrono utilizable de la red, el cual es expresado por:

$$TTRT = (D_Max + F_Max + Token_time)$$

donde:

- D_Max: Máximo estado de latencia o retardo de circulación, para que un delimitador de inicio atraviese el anillo.
- F_Max: El tiempo requerido para transmitir una trama de máximo tamaño. En el modo básico, una trama puede contener 9000 símbolos más 16 símbolos de preámbulo. En el modo híbrido las tramas pueden estar compuestas por 17200 símbolos más cuatro símbolos de preámbulo.
- Token_time: El tiempo necesario para enviar un token y el preámbulo.

Los valores característicos de estos parámetros se muestran en la tabla 3.3

PARAMETRO	MODO BASICO	MODO HIBRIDO
D_Max	2.661 ms	2.833 ms
F_Max	0.361 ms	0.6945 a 89.604 ms
Token_time	0.88 µs	0.40 a 52.08 µs

TABLA 3.3

La ecuación anterior define la máxima cantidad de tiempo que una estación puede sostener el token sin que el temporizador THT este corriendo. Después de la transmisión de tramas síncronas (si las hay), el THT comienza a correr y la estación puede enviar tramas asíncronas hasta que THT expire.

La situación con las tramas asíncronas es un poco más complejo de explicar. Recordando que FDDI soporta 8 diferentes prioridades, asociando cada clase de prioridad a un valor de umbral, $T_Pri[i]$, las tramas asíncronas de prioridad i , pueden ser transmitidas sólo si $THT > T_Pri[i]$.

Si la llegada del token es tardía ($Late_ct > 0$), la estación simplemente reinicia $Late_ct$ a 0. La estación puede enviar cualquier trama síncrona pendiente y colocar un token al final de ésta.

EJEMPLO DE OPERACION DEL ANILLO

El siguiente ejemplo ayudará a explicar la operación de un anillo de FDDI y el protocolo de token calculado. Asumiendo que las estaciones de la red acuerdan un TTRT de 100 ms, y cada estación puede enviar tramas síncronas por 20 ms (estos valores no están dentro de la realidad, pero sirven para demostrar la operación del protocolo).

La figura 3.15 muestra la relación del THT, TRT y el contador de retardo $Late_ct$, analizándolo desde una única estación. Para 0 ms. (evento A), el token llega a la estación. El TRT es reinicializado y toma el valor de TTRT (100 ms.) y continua corriendo. Como la estación no tiene tramas que enviar en este momento, el token es pasado a la siguiente estación.

El token regresa a esta estación 60 ms. después (evento B), entonces se considera que el token llegó temprano porque el TRT aún continúa corriendo y $Late_ct = 0$. En este momento la estación si tiene tramas para enviar y muchas acciones se toman en este momento. Primero, el THT toma el valor actual del TRT (40 ms. la diferencia entre TTRT y TRT) y el TRT es reinicializado al valor de TTRT; note que el TRT continúa corriendo.

Después la estación envía tramas síncronas por 20 ms. (evento C). finalmente la estación comienza a contar THT y puede enviar tramas asíncronas hasta que THT expire (evento D). a los 120 ms. un nuevo token debe ser generado.

A los 160 ms. (evento E), el TRT expira, entonces Late_ct es incrementado y el TRT toma una vez más el valor de TTRT (100 ms.). a los 200 ms. (evento F) el token llega y el Late_ct es puesto a 0, pero el TRT no es reinicializado, de esta forma el TRT acumula los retrasos. En este momento esta estación no tiene tramas síncronas para enviar.

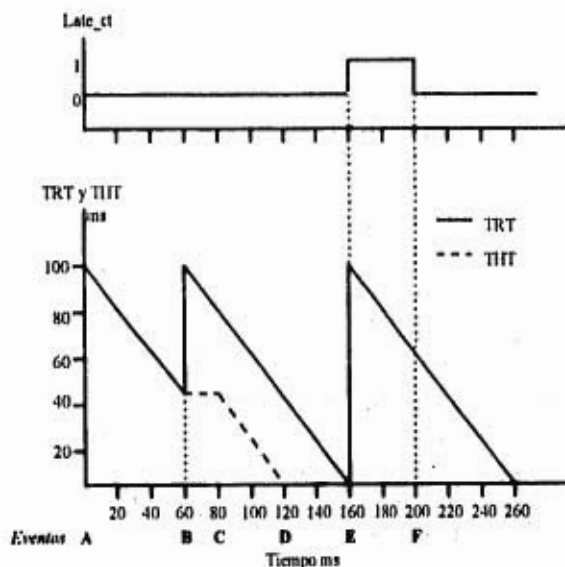


FIGURA 3.15 OPERACION DE TRT, THT Y Late_ct

3.4 RUTEO EN FDDI

3.4.1 ENRUTAMIENTO

El enrutamiento se refiere a la transmisión de un paquete de información de una máquina a través de otra. Cada máquina en la cual entra el paquete analizará el contenido del encabezado del paquete y decidirá su acción, con base en la información dentro del encabezado. Si la dirección destino del paquete coincide con la dirección destino de la máquina, los protocolos de nivel superior retendrán y procesarán el paquete. Si la dirección destino no concuerda con la de la máquina el paquete se envía hacia adelante sobre la red.

DIRECCIONAMIENTO

El esquema de direccionamiento de FDDI es similar al de las redes Ethernet, que requieren un mapeo sencillo. Tanto IP como ARP se pueden usar en FDDI. El protocolo IP ya fue analizado en la sección 2.4.5 de este trabajo, mientras que el protocolo ARP se analizará en la siguiente sección.

Direccionamiento físico: Una dirección física es aquella asignada al dispositivo físico de la red, por ejemplo, en una red Ethernet, tenemos a la dirección MAC. Esta dirección identifica de manera única a la interfaz de la red conectada al equipo y es a través de ella que los protocolos de las capas bajas hacen llegar la información de un equipo a otro. Sin embargo, cuando hablamos de la interconexión de redes de distinta naturaleza, el formato de esta dirección física cambia. Por lo que no podemos hacer un direccionamiento directo entre dos equipos conectados a esas redes.

Direccionamiento lógico (IP): Con el objeto de identificar de manera única a cada una de las máquinas dentro de una red, se definió un identificador universal conocido como dirección IP. El formato de esta dirección IP fue discutido en la sección 2.4.5 del presente trabajo de tesis.

MAPEO DE DIRECCIONES

Para que dos máquinas dentro de una red puedan identificarse deben conocer sus respectivas direcciones físicas. Las direcciones IP nos sirven para identificar una máquina dentro de la red virtual TCP/IP. Pero cuando la información es enviada a través de la red física debemos conocer la dirección física de la máquina destino.

Como puede verse es necesario implementar un método que permita determinar la dirección física asignada a una máquina, a partir de una dirección IP. Para el caso de redes FDDI se usa un protocolo llamado ARP (Address Resolution Protocol) el cual permite localizar una dirección física dentro de la red a partir de una dirección IP.

3.4.2 PROTOCOLO DE RESOLUCION DE DIRECCIONES (ARP)

Este protocolo sirve para localizar una dirección física a partir de una dirección IP, y opera enviando un *broadcast*, es decir, un paquete dirigido a todas la máquinas dentro de la red física en el cual pregunta *¿quién es la máquina con la dirección IP especificada?*. A este mensaje de broadcast sólo va a responder la máquina con la dirección IP dada y le va a contestar a la máquina que originó el broadcast con su dirección física.

Como el tráfico a través de la red se saturaría mucho con los broadcasts, se implementó que cada máquina tuviera una área de almacenamiento denominada *cache broadcast* donde se encontraría una tabla de direcciones IP y sus correspondientes direcciones físicas, de esta manera, antes de enviar un *broadcast* verifica en su cache si ya la conoce y si lo tiene registrado toma la dirección física y envía el paquete. De no ser así, envía el broadcast y la máquina destino le responde a la vez que actualiza su cache con la dirección física de la máquina que envía el broadcast.

En la figura 3.16 aparece la organización de una solicitud ARP, cuando se envía una solicitud ARP, todos los campos del diseño se utilizarán, a excepción de la dirección del hardware del receptor (misma que la solicitud trata de identificar). En una respuesta ARP se utilizan todos los campos.

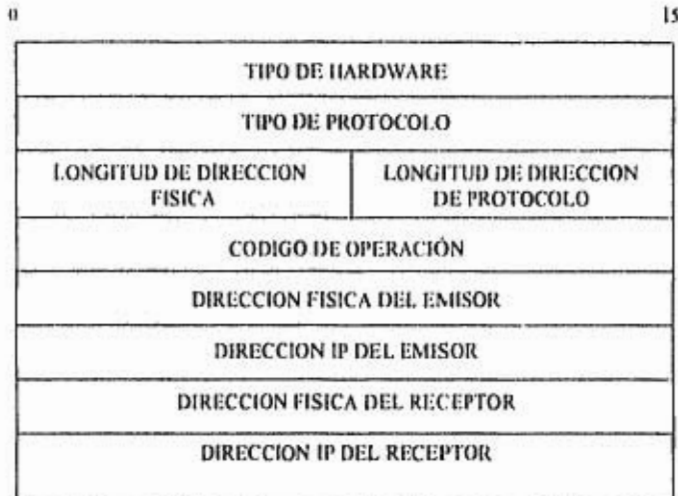


FIGURA 3.16 DISEÑO DE UNA SOLICITUD Y RESPUESTA ARP

TIPO DE HARDWARE (16 bits): Especifica la interfaz de hardware sobre la cual la máquina que envía busca una respuesta.

TIPO DE PROTOCOLO (16 bits): Contiene el tipo de protocolo de la capa superior que envía dicha petición de ARP, por ejemplo contiene 0800h para IP. Esto significa que ARP puede ser utilizado con otros protocolos diferentes a TCP/IP.

LONGITUD DE DIRECCION FISICA (8 bits): Es la longitud de cada una de las direcciones físicas incluidas en el datagrama, expresadas en bytes.

LONGITUD DE LA DIRECCION DE PROTOCOLO (8 bits): Especifica la longitud de la dirección del protocolo utilizado, por ejemplo para IP la longitud es de 32 bits.

CODIGO DE OPERACION (8 bits): Se especifica si es una petición de ARP (1), una respuesta de ARP (2), una petición de RARP (3) o una respuesta de RARP (4).

DIRECCION FISICA DEL EMISOR (48 bits): Se especifica la dirección física de la máquina que envía el paquete.

DIRECCION IP DEL EMISOR (32 bits): Se especifica la dirección IP de la máquina que envía el paquete.

DIRECCION FISICA DEL RECEPTOR (48 bits): Se especifica la dirección física de la máquina a donde se envía el paquete, si es una petición de ARP este campo esta vacío y en la respuesta es donde la máquina que responde pone su dirección física del destinatario.

DIRECCION IP DEL RECEPTOR (32 bits): En este campo se pone la dirección IP del destinatario.

Una falla obvia en el sistema ARP es que si un dispositivo no supiera cuál es su propia dirección IP, no existiría manera de emitir solicitudes y respuestas. Esto puede ocurrir cuando un dispositivo nuevo se añade a la red (típicamente una estación de trabajo sin disco). La única dirección de la cual está consciente el dispositivo es la dirección física establecida. Una solución sencilla es el Protocolo de Resolución de Direcciones Contraria (**Reverse Address Resolution Protocol, RARP**), que funciona en forma inversa al ARP, enviando la dirección física y esperando el regreso de una dirección IP. Se utiliza el mismo formato que ARP, sólo que el campo de operación se pone como una petición de RARP o una respuesta RARP.

Se emite un *broadcast* a todas las máquinas de la red, y le va a responder la máquina o las máquinas configuradas para responder a estas peticiones, llamadas servidores RARP o servidores de *booteo*. Las reglas de RARP estipulan que solamente el servidor RARP podrá generar una respuesta. Muchas redes asignan más de un servidor RARP, tanto para distribuir la carga de procesamiento, como para que actúen como respaldo en caso de que haya algún problema.

Encapsulación del protocolo IP Y ARP en FDDI

Tanto IP como ARP se pueden usar sobre FDDI, estos protocolos son encapsulados dentro de la trama LLC usando el formato LLC-SNAP, tal como se muestra en la figura 3.17

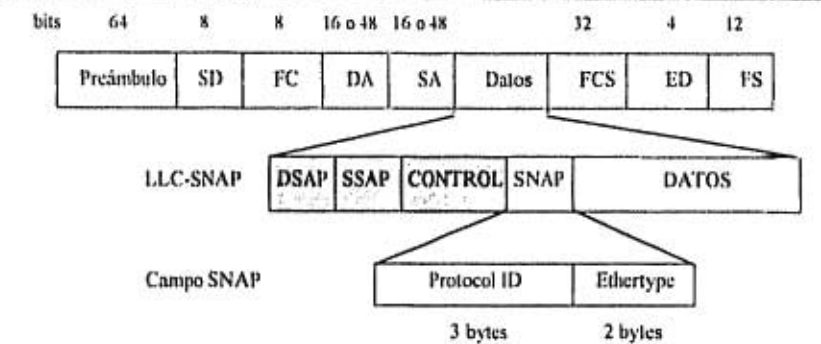


FIGURA 3.17 CAMPO SNAP EN UNA TRAMA LLC

El protocolo de acceso a la subred SNAP, es una extensión del encabezado IEEE 802.2 LLC. Esta extensión fue hecha a fin de encapsular datagramas IP e información del protocolo de resolución de direcciones (ARP). El encabezado SNAP sigue inmediatamente después del encabezado LLC y es encapsulado en el campo de datos, tal como se muestra en la figura 3.17

Para el encabezado LLC-SNAP, ambos campos DSAP y SSAP toman un valor de AAh y el campo de control es puesto con el valor de 03h. Los del campo de identificación de protocolo o código de organización toman todos el valor de 0. El campo Ethertype el cual consta de dos bytes es puesto como 0800h para IP, y 0806h para ARP. La tabla 3.4 contiene otros ejemplos de los posibles valores que puede tomar Ethertype.

Ethertype	valor (hex)
Reservado para el campo de longitud LLC	0000-05DC
IP	0800
X.75 Internet	0801
X.25 Nivel 3	0805
ARP	0806
Sistemas Banyan	0BAD
3-COM Corp	6010-6014
DEC LAN	8038
Appletalk	809B
Appletalk ARP	80F3

TABLA 3.4 VALORES ETHERTYPE USADOS EN EL FORMATO LLC-SNAP

3.4.3 PROTOCOLOS DE RUTEO

Los protocolos de ruteo se utilizan para intercambiar información con otras computas de una forma rápida y confiable. Si hay más de una compuerta (Gateway) dentro de la red local y pueden comunicarse una con otra, se consideran vecinas interiores. Si las computas pertenecen a diferentes sistemas autónomos², se trata de computas exteriores, el enrutamiento de mensajes entre sistemas autónomos queda a criterio de las computas exteriores. Las computas interiores se usan para transferir información dentro de un sistema autónomo.

En el interior de una red, el método de transferencia de información de ruteo entre computas interiores es usualmente RIP, HELLO y más recientemente OSPF, estos son protocolos de compuerta interior (IGP's). Los mensajes entre computas exteriores pasan a través del protocolo de compuerta exterior (EGP).

Los detalles de ruta están contenidos en una tabla de ruteo. Existen unos cuantos métodos comunes para la elaboración de una tabla de ruteo:

- Se crea una tabla fija con un mapa de la red, mismo que se deberá modificar y volver a leer cada vez que exista un cambio físico en cualquier parte de la red.
- Se utiliza una tabla dinámica que evalúa la carga de tráfico y los mensajes provenientes de otros nodos para refinar una tabla interna.
- Se utiliza una tabla de ruteo central fija, que se carga por los nodos de la red a intervalos regulares o cuando es requerida, proveniente del depósito central.

²Sistema Autónomo: Es aquel en el cual la estructura de la red a la que está conectado no es visible para el resto de las redes

Método de ruteo por saltos mínimos

La mayor parte de las redes y compuertas a interredes funcionan bajo el supuesto de que la ruta más corta es la mejor forma de enrutar mensajes. Cada máquina por la cual pasa un mensaje se conoce como salto, por ello este método de ruta se conoce como de saltos mínimos. Aunque la experimentación ha demostrado que los saltos mínimos no son necesariamente el método más rápido, es uno de los métodos más fáciles de implementar. La figura 3.18a muestra una tabla de saltos mínimos obtenida en base a una sencilla red esquematizada en la figura 3.18b.

		DESTINO						
		A	B	C	D	E	F	G
ORIGEN	A	0	1	3	2	4	5	5
	B	1	0	2	1	3	4	4
	C	3	2	0	1	1	2	2
	D	2	1	1	0	2	3	3
	E	4	3	1	2	0	1	1
	F	5	4	2	3	1	0	2
	G	5	4	2	3	1	2	0

FIGURA 3.18a

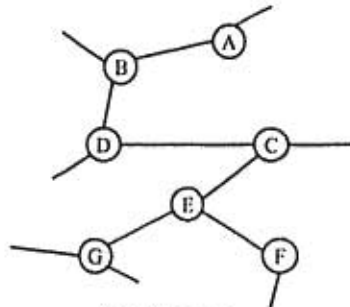


FIGURA 3.18b

La desventaja de este método consiste en que no toma en consideración las velocidades de transferencia, las fallas en líneas y otros factores que podrían afectar el tiempo total de viaje hacia el destino, porque simplemente se preocupa de la distancia más corta aparente, suponiendo que todas las conexiones son iguales.

Enrutamiento por tipo de servicio

Este enrutamiento depende del tipo de servicio de enrutamiento disponible de una compuerta a otra. Este método se conoce como enrutamiento por tipo de servicio (TOS). TOS toma en cuenta la velocidad y la confiabilidad de las conexiones, así como factores de seguridad y ruta específica.

Para llevar a cabo el enrutamiento TOS, la mayor parte de los sistemas utilizan la actualización dinámica de las tablas, reflejando el estado del tráfico. TOS también toma en cuenta las longitudes actuales de las colas de espera en cada compuerta, porque quizá no tenga ninguna importancia la ruta teórica más rápida, si el mensaje se queda esperando en una cola. Esta información se obtiene a través de transferencias frecuentes de mensajes de estado entre compuertas.

Protocolo de información de Ruteo (RIP)

RIP utiliza una tecnología de difusión. Esto significa que a intervalos regulares las compuertas difunden sus tablas de enrutamiento a otras compuertas en la red. Ese es también uno de los problemas de RIP, debido a que el tráfico aumenta en la red y mensajes poco eficientes pueden reducir la velocidad de las redes, en comparación con otros protocolos de ruteo. RIP es un sistema de vector-distancia, enviando en sus mensajes la dirección de la red y la distancia a la dirección. El formato de los mensajes RIP aparece en la figura 3.19.



FIGURA 3.19 FORMATO DEL MENSAJE RIP

El encabezado del mensaje está compuesto por tres campos. El de comando (establecido en 1 si es una solicitud y en dos si es una respuesta), el número de versión del protocolo RIP y un campo reservado sin utilizar. El resto del mensaje contiene información de dirección. Cada conjunto empieza con un identificador de la familia de protocolos utilizados (RIP no es específicamente para protocolos internet, pero si se utiliza en internet, su valor se establece en 2) y un conjunto de identificadores de red. Existen 96 bits disponibles para la dirección de la red, de los cuales máximo 32 son necesarios para una dirección internet. El último campo es el valor "métrico" que por lo general identifica el número de saltos en la red.

Un mensaje de solicitud por lo general se envía a otra compuerta cuando se requiere una actualización de enrutamiento. Cuando se recibe una solicitud, el sistema examina el mensaje para verificar cada una de las direcciones de la red incluidas. Si su tabla de enrutamiento tiene una distancia a esa dirección de la red, en la respuesta se coloca en el campo correspondiente a métrico. Si no se tiene la dirección en la tabla de ruteo no se envía nada.

El protocolo RIP pertenece a una serie de protocolos de enrutamiento basados en el algoritmo de vector distancia, también conocido con el nombre de Bellman-ford. Estos algoritmos obligan a todo ruteador a intercambiar sus tablas de ruteo (o parte de ellas) solamente con sus vecinos. Por lo tanto RIP es usado como un protocolo de compuerta interno IGP, para campos y redes regionales que utilizan líneas seriales, donde sus velocidades son muy variadas. Dentro de las principales limitantes de RIP tenemos las siguientes:

- El protocolo RIP está limitado a redes en las cuales la ruta más grande contiene 15 saltos.
- El protocolo RIP utiliza métricas fijas para comparar rutas alternativas. Esto no es apropiado para situaciones donde las rutas necesitan escoger parámetros de tiempo real tales como un retardo, fiabilidad o carga.

Cada ruteador que implementa RIP contiene una tabla de ruteo. Esta tabla contiene una entrada para cada uno de los destinos. Cada entrada tiene al menos la siguiente información.

- La dirección IP del destino
- Una métrica, la cual representa el costo total de obtener un datagrama del anfitrión al destino. Esta métrica es la suma del costo asociado con la redes por las cuales pasará para llegar al destino
- La dirección IP de la siguiente compuerta de la ruta al destino. Si el destino es uno de los que están conectados directamente, esta información no es necesaria.
- Una bandera que indica que la información acerca de la ruta se ha modificado recientemente.
- Varios timers asociados con la ruta

Timers para el protocolo RIP

Cada 30 segundos el proceso de salida está capacitado para generar una actualización completa hacia todas las compuertas cercanas. Cuando existen varias compuertas en una sola red, se tiende a sincronizarlas unas con otras, de tal manera que todas las emisiones ocurran al mismo tiempo.

Existen dos timers asociados con cada ruta, un "tiempo de expiración" y un "tiempo de colecta de basura" o de "flushing". Cuando un tiempo de expiración se cumple la ruta ya no es válida. Sin embargo, permanece en la tabla por algún tiempo, dando lugar a que las compuertas cercanas se den cuenta de que la ruta ya no es válida. Cuando expira el "timer de colecta de basura", la ruta se elimina de la tabla.

El tiempo de expiración es inicializado cuando se establece la ruta, y a cualquier tiempo se reciben mensajes para la ruta. Si pasan 180 segundos después la inicialización del tiempo agotado se considera que la ruta ha expirado y en seguida comienza el proceso de desecho (tiempo de colecta de basura).

Protocolo HELLO

Este protocolo es distinto de RIP en que HELLO utiliza el tiempo en lugar de la distancia como factor de enrutamiento. El formato de un mensaje HELLO aparece en la figura 3.20, los campos principales del encabezado son:

- Una suma de verificación de la totalidad del mensaje
- La fecha actual de la máquina emisora
- La hora actual de la máquina emisora
- Una marca de tiempo utilizada para calcular retrasos de ida y vuelta
- Un desplazamiento que apunta a las entradas siguientes
- El número de anfitriones que siguen como lista

A continuación del encabezado existe un número de entradas con estimación de retraso de la máquina y un desplazamiento que es una estimación de la diferencia entre los relojes emisor y receptor. Los desplazamientos son importantes porque HELLO es un protocolo crítico en el tiempo, por lo que el desplazamiento permite la corrección entre tiempos de distintas máquinas.

La marca de tiempo en los mensajes es utilizada por las máquinas a través de las cuales pasa dicho mensaje, para calcular retrasos en la red. De esta forma, se puede construir una tabla de enrutamiento basada en tiempos reales de entrega.



FIGURA 3.20 FORMATO DE MENSAJE HELLO

Protocolo de Abrir Primero la Ruta más Corta (OSPF)

El nombre "ruta más corta" no es exacto en la descripción del proceso de enrutamiento de este protocolo (tanto RIP como HELLO utilizan un método de ruta más corta, RIP con base a distancia y HELLO con base a tiempo). Una mejor descripción del sistema sería "ruta óptima" en el cual varios criterios son evaluados a fin de determinar la mejor ruta hacia el destino.

A partir de una tabla de enrutamiento que contiene información sobre la topología de la red, una compuerta OSPF determinará la ruta más corta utilizando métrica de costos, velocidad de ruta, tráfico, confiabilidad, seguridad y otros varios aspectos de la conexión.

OSPF utiliza a IP para la capa de red. La especificación OSPF prevé dos direcciones reservadas de multidifusión, una para todos los ruteadores que soportan OSPF (224.0.0.5), y otra para un ruteador designado y un ruteador de respaldo (224.0.0.6). Se reserva para OSPF el número de protocolo IP 89. Cuando IP envía un mensaje OSPF, utiliza el número de protocolo y un valor de campo de tipo de servicio (TOS) de 0.

En OSPF se utilizan dos formatos de encabezado. El formato de encabezado de mensajes OSPF primario aparece en la figura 3.21

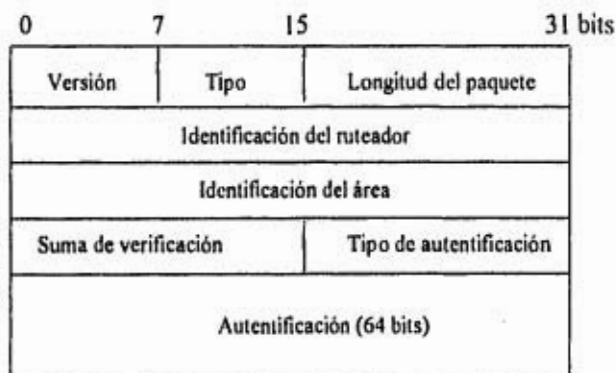


FIGURA 3.21 FORMATO DEL ENCABEZADO DE MENSAJE OSPF

El campo número de versión identifica la versión del protocolo OSPF en uso (actualmente la versión 1). El campo de tipo identifica el tipo de mensaje y puede contener un valor de los que se muestran en la tabla 3.5

Tipo	Descripción
1	Saludos
2	Descripción de la base de datos
3	Solicitud del estado del enlace
4	Actualización del estado del enlace
5	Acuse de recibo del estado del enlace

TABLA 3.5 VALORES DE TIPO DE ENCABEZADO OSPF

El campo de longitud de paquete contiene la longitud del mensaje, incluyendo al encabezado. La identificación de ruteador es la identificación de la máquina emisora, en tanto que la identificación de área identifica el área en la cual está la máquina emisora. El campo de suma de verificación utiliza el mismo algoritmo que IP a fin de verificar la totalidad del mensaje, incluyendo al encabezado.

El campo de tipo de autenticación identifica el tipo de autenticación que se utilizará. Actualmente sólo hay dos valores para este campo: 0 para ninguna autenticación y 1 para contraseña.

El segundo formato de encabezado utilizado por OSPF es únicamente para anuncios de estado del enlace, y se muestra en la figura 3.22

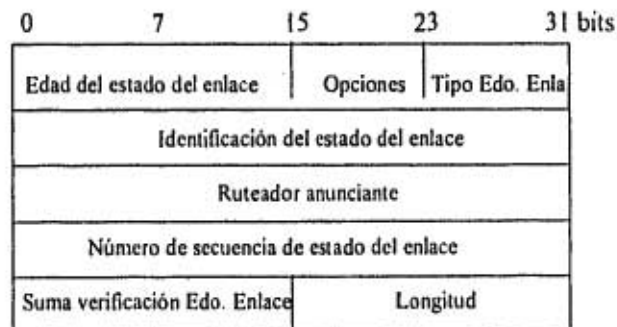


FIGURA 3.22 FORMATO DEL ENCABEZADO DE ANUNCIO DE ESTADO DEL ENLACE OSPF

El campo de edad del estado del enlace contiene el número de segundos desde que se originó el anuncio de estado del enlace. El campo de opciones contiene cualquier característica del servicio de tipo IP (TOS) soportado por la máquina emisora. El tipo de estado del enlace identifica el tipo de anuncio de enlace que utiliza uno de los valores que aparece en la tabla 3.6

Valor	Descripción
1	Enlaces de ruteador (ruteador a área)
2	Enlaces de red (ruteador a red)
3	Enlaces resumen (información sobre la red IP)
4	Enlaces resumen (información sobre el ruteador externo del sistema autónomo)
5	Enlace externo (externo al sistema autónomo)

TABLA 3.6 VALORES DE TIPO DE ENCABEZADO DEL ANUNCIO DE ESTADO DEL ENLACE

El campo de identificación del estado del enlace identifica cual es la porción de la interred descrita en el anuncio. El valor dependerá del campo de tipo de estado del enlace y puede contener direcciones IP para redes o identificadores de ruteador. El campo de ruteador anunciante identifica al ruteador originador. El número de secuencia del estado del enlace es un número creciente que se emplea para impedir que paquetes viejos o duplicados se interpreten. El campo suma de verificación es idéntico al primer encabezado. Y finalmente, el campo longitud contiene el tamaño del anuncio, incluyendo al encabezado.

Características principales del protocolo OSPF

El protocolo OSPF está basado en la tecnología "Link State" estos algoritmos llevan la información de ruteo a todos los nodos de la internet. Sin embargo, todo ruteador envía exclusivamente aquella porción de su tabla de ruteo que describe el estado de sus propios enlaces. Básicamente los algoritmos de *Link State* envían pequeñas actualizaciones por toda la internet, mientras que los de vector distancia, envía actualizaciones más grandes sólo a sus vecinos. Los algoritmos *Link State* convergen más rápidamente, pero requieren mayor poder de procesamiento y memoria que los algoritmos de vector-distancia. Una diferencia importante con el protocolo RIP es que este último actualiza sus tablas de ruteo cada 30 seg. Mientras que OSPF las revisa cada 30 segundos pero, las actualiza sólo, si ha habido un cambio en la red.

EGP (Protocolo de Compuerta Exterior)

El protocolo EGP (Exterior Gateway Protocol) es más utilizado en compuertas externas vecinas y entre internets, en las cuales los sistemas autónomos hacen uso del EGP para divulgar las rutas del sistema central.

A continuación se mencionan las principales características del protocolo EGP:

Soporte de mensajes de adquisición de vecino: Una compuerta envía un mensaje de adquisición de vecino para establecer comunicación EGP con otra compuerta. Antes de iniciar la propagación de rutas una compuerta solicita y espera un permiso para enviar información.

Verificación continua del funcionamiento de vecinos: El protocolo EGP permite dos formas de verificar si la compuerta vecina está "viva". Por medio del modo activo, en el cual las compuertas prueban periódicamente un vecino, enviando un mensaje Hello y un mensaje Polling, y espera una respuesta. Mientras que en el modo pasivo, la compuerta depende de su vecino para enviar mensajes tipo Hello o Polling.

Tablas de Ruteo

Una ruta consiste en un número de red destino, la dirección de la próxima compuerta que se pueda usar de manera directa para conectarse a una red y una métrica que proporciona la distancia de los saltos hacia la red destino.

Existen dos tipos de tabla de ruteo, las tablas kernel (para envíos de paquetes) y el proceso de tablas EGP. Las tablas kernel contienen tablas separadas para destinos de anfitrión y de redes. El protocolo EGP sólo mantiene las tablas de ruteo de red. La implementación del EGP está diseñada para correr en una compuerta que también es un anfitrión.

El proceso EGP de tablas de ruteo se mantiene como dos tablas separadas, una para rutas exteriores y la otra para rutas interiores. Tener tablas separadas para ruteos interiores y exteriores facilita la separación de mensajes de salida.

Restricciones del Protocolo EGP

El protocolo EGP también tiene algunas limitaciones técnicas:

- Limita las compuertas
- Permite que propaguen sólo aquellas redes totalmente dentro de dos sistemas autónomos
- Limita la topología

IGRP (Protocolo de ruteo de compuerta interna)

IGRP (Internal Gateway Routing Protocol) es un protocolo que permite que las compuertas coordinen sus rutas. Sus objetivos son:

- Establecer ruteo en una cierta topología de red.
- Dar una respuesta a cierta topología de red.
- Dividir el tráfico entre varias rutas paralelas.

Los protocolos como IGRP son llamados "protocolos de compuerta interna" (IGP). Este tipo de protocolos se utilizan dentro de un conjunto de redes simples, conectadas por "protocolos de compuerta externa" (EGP).

IGRP tiene algunas similitudes con los protocolos de ruteo de Xerox y RIP, pero difiere en que IGRP fue implementado para grandes redes de computadoras.

El protocolo IGRP permite a las compuertas construir y mantener tablas de ruteo para intercambiar información con otras compuertas. En un caso simple una compuerta encontrará una ruta que represente el mejor camino para alcanzar otra red o una ruta caracterizada por la próxima compuerta, para que los paquetes puedan ser enviados. Periódicamente una compuerta realiza un broadcast (difusión) en su tabla de ruteo, cuando una compuerta recibe un broadcast de otra compuerta, la compara con la tabla existente para buscar otras rutas mejores y poder sustituirla. Todos los protocolos de vector-distancia realizan este procedimiento.

Timers

IGRP mantiene un número de timers e intervalos de tiempo de contacto. Esto incluye un dato de tiempo actualizador, un timer inválido, un periodo de retención de timer y un timer de desecho.

El timer de actualización actualiza el mensaje antes de que sea enviado. El timer de invalidación especifica cuánto tiempo debe esperar un ruteador, en la ausencia de mensajes de ruteo actualizados acerca de una ruta específica, declarando antes la ruta inválida. El IGRP define el timer de invalidación como 3 veces el periodo de actualización del timer. Y la variable del periodo de retención especifica el periodo de mantenerse sujeto (IGRP por omisión es igual a tres veces el periodo de actualización del timer más 10 segundos). Finalmente, el timer de desecho indica cuánto tiempo pasará antes de que una ruta sea desechada de la tabla de ruteo. IGRP por omisión lo define igual a 7 veces el periodo de actualización de ruteo.

3.4.4 CONFIGURACION DE RUTEADORES

Los comandos más frecuentes en la configuración de un ruteador se describen en seguida:

hostname	Especifica el nombre para el servidor de la red
enable-password	Asigna una contraseña para entrar al nivel de comando
service-config	Especifica autocarga TFTP de los archivos de configuración
novell-routing	Activa o desactiva ruteo de novell y ruteo de novell RIP y servicios SAP
appletalk-routing	Activa o desactiva el procesamiento del protocolo AppleTalk
interface serial	Especifica una interfaz y empieza la configuración para la misma
description	Añade un nombre descriptivo a una interfaz
ip address	Coloca una dirección IP para una interfaz
ip tcp header-compression	activa la compresión de encabezados de TCP
bandwidth	Coloca un valor de ancho de banda para una interfaz, este es sólo un parámetro de ruteo; no afecta a la interfaz física
encapsulation	Asigna un método de encapsulación
autonomous system	Especifica un número de sistema autónomo
router igrp	Selecciona el proceso de ruteo IGRP.
network	Especifica una lista de redes a ser publicadas como originadoras

Todos los protocolos de ruteo dinámicos se configuran con el siguiente comando:

router protocol [número de AS]

donde:

protocol puede ser **igrp**, **ospf**, **rip**, **egp** o **hello**

número de AS es un número asignado a un sistema autónomo, el cual es un grupo de redes o ruteadores administrados por una sola autoridad, con el fin de adquirir conectividad con otros sistemas. Un sistema autónomo agrupa una colección de redes que comparten una estrategia de ruteo común.

Luego se deben poner las redes conectadas directamente. Sólo redes, no subredes.

network [dirección de la red]

ejemplo:

```
router igrp 119  
network 132.248.0.0
```

para intercambiar rutas entre distintos protocolos de ruteo, se utiliza el comando **redistribute**:

ejemplo:

```
router ospf 382 redistribute ospf 30 redistribute rip
```

las rutas aprendidas en OSPF 30 y por RIP son anunciadas a través de OSPF 382

A continuación se listan algunos otros comandos para el uso de ruteadores

connect [host]	Conecta a un host, también se puede conectar tecleando sólo el nombre del host
telnet [host]	Conecta a un host usando el protocolo telnet
where	Muestra las conexiones abiertas
show	Da una lista de información de comandos
slip	Entra al modo SLIP
shutdown	Administrativamente desconecta la interfaz
en	Entra al modo privilegiado
ping	Es una herramienta de monitoreo que utiliza ICMP
show int [interfaz]	Este comando muestra el estado en que se encuentra la interfaz

En seguida se muestra un ejemplo en el gateway de la ENEP Aragón

```

dgscal# ping
Protocol [ip]:
Target IP address: 132.248.44.254
Repeat count [5]:100
Datagram size [100]:
Timeout un seconds [2]:
Source address: 132.248.210.254
Type of service [0]:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Suces rate is 99 percent (99/100)

dgscal#
dgscal# telnet 132.248.44.254

```


User Access Verification

```
Username: marcos
Password:
aragon>en
```

```
Username: marcos
Password:
aragon#sh int
```

```
Ethernet 0 is up, line protocol is up
  Hardware is Lance, address is 0000.0c07.db32 (bia 0000.0c07.db32)
  Description: LAN ENEP Aragon
  Internet address is 132.248.44.254, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:09, output 0:00:06, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 2 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
    4857086 packets input, 587384064 bytes, 2 no buffer
    Received 580130 broadcasts, 0 runts, 0 giants
    1130 input errors, 1130 CRC, 952 frame, 0 overrun, 0 ignored, 0 abort
    4388995 packets output, 2029810906 bytes, 0 underruns
    59 output errors, 49939 collisions, 46 interface resets, 0 restarts
```

--More--

```
Serial 0 is up, line protocol is up
  Hardware is HD64570
  Description: ENEP Aragon - Preparatoria 3
  Internet address is 132.248.223.254, subnet mask is 255.255.255.0
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input 0:00:08, output 0:00:01, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 6000 bits/sec, 0 packets/sec
    3117008 packets input, 1617715550 bytes, 0 no buffer
    Received 346369 broadcasts, 0 runts, 0 giants
    5186 input errors, 5125 CRC, 1413 frame, 0 overrun, 0 ignored, 766 abort
    2087548 packets output, 762884104 bytes, 0 underruns
3358 carrier transitions
```

--More--

```
Serial 1 is up, line protocol is up
Hardware is IID64570
Description: ENEP Aragon - ENEP Zaragoza
Internet address is 132.248.216.253, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 0:00:00, output 0:00:01, output hang never
Last clearing of "show interface" counters never
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
 6609927 packets input, 2710782435 bytes, 0 no buffer
  Received 487345 broadcasts, 0 runts, 0 giants
 447412 input errors, 445432 CRC, 310007 frame, 38 overrun, 76 ignored, 43534 abort
7809364 packets output, 1816595909 bytes, 0 underruns
 0 output errors, 0 collisions, 2262 interface resets, 0 restarts
604795 carrier transition
7809364 packets output, 1816595909 bytes, 0 underruns
 0 output errors, 0 collisions, 2262 interface resets, 0 restarts
604795 carrier transitions
--More--
```

```
BR10 is administratively down, line protocol is down
Hardware is BRI
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 0 bits/sec, 0 packets/sec
 0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 packets output, 0 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets, 0 restarts
 0 carrier transitions
aragon#
```

CAPITULO IV

ATM

4.1 ANTECEDENTES

4.1.1 SDH

SDH es el acrónimo de Synchronous Digital Hierarchy y es un estándar que define a una señal utilizada en redes de fibra óptica. Este estándar fue desarrollado por la ITU-T (International Telecommunication Union - Telecommunication) y esta basada en el trabajo desarrollado en Bellecore, por ECSA (Exchange Carriers Standards Association) y por ANSI para la red síncrona SONET.

El formato básico de una señal SDH permite a ésta ofrecer varios servicios en su contenedor debido a que maneja un ancho de banda flexible. Esta capacidad permitirá la transmisión a alta velocidad de paquetes conmutados, videoconferencia y HDTV. Sin embargo SDH aún permite la transmisión e interconexión a niveles de 2 Mb, 34 Mb y 140 Mb respetando la jerarquía de las señales digitales existentes.

El estándar SDH fue desarrollado en base a capas, las cuales son la sección del Regenerador, sección de Multiplexaje y la Ruta. Las capas guardan una relación jerárquica. Cada capa se basa en los servicios proporcionados por las capas inferiores.

La trama SDH, señal de transporte síncrona (STS) incluye la sección de ruta, la sección de multiplexaje, la sección del regenerador así como la carga de información. La tasa base de 155.520 Mbs (STM-1) puede ser multiplicada hasta formar tasas superiores. STM-1 ha sido adoptado mundialmente debido a que se asemeja al bloque de construcción americano conocido como STS-3, las tasas inferiores se utilizan en forma regional.

Uno de los beneficios de SDH es su capacidad para transportar una gran carga de información. Sin embargo, también las señales de jerarquía digital existentes pueden ser ajustadas, protegiendo la inversión del equipo actual. Para lograr esta capacidad el contenedor virtual STM puede subdividirse en componentes o estructuras inferiores, conocidas como unidades tributarias (TU's), con el propósito de transportar y conmutar cargas de información inferiores a la tasa STM-1.

La trama SDH consiste en un encabezado más la capacidad de un contenedor virtual como se muestra en la figura 4.1



FIG. 4.1 FORMATO DE TRAMA SDH

Las primeras 9 columnas de cada trama forman el encabezado de transporte y las últimas 261 columnas forman la capacidad del contenedor virtual (VC).

El VC junto con los punteros (H1, H2, H3) que se muestran en la figura 4.2 son conocidos como la Unidad Administrativa (AU).

Transportada dentro de la capacidad del VC, el cual cuenta con su propia estructura de 9 renglones y 261 columnas, se encuentra el Encabezado de Ruta y el Contenedor. La primera columna está dedicada al Encabezado de Ruta, seguido por el contenedor de la carga de información. Los contenedores Virtuales pueden tener cualquier alineamiento dentro de la AU y este alineamiento es indicado a través del puntero en el renglón 4.

Dentro de la sección de encabezado, los primeros 3 renglones son utilizados por el encabezado de la Sección del Regenerador y las últimas 5 líneas son utilizadas por el Encabezado de la sección de multiplexaje.

El encabezado de sección se muestra en la figura 4.2

El encabezado de Sección de Multiplexor (MS) contiene la información por el equipo terminal de la sección de multiplexaje en cada extremo de la misma (esto es, entre elementos consecutivos de la red exceptuando a los regeneradores). El encabezado MS se encuentra en los renglones del 5 al 9 de las columnas 1 a 9. Byte por byte el encabezado MS aparece como sigue:

A1	A1	A1	A2	A2	A2	C1		
H1			E1			F1		
H1			D2			D3		
H1	H1	H1	H2	H2	H2	H3	H3	H3
H2			K1			K2		
D4			D5			D6		
D6			D8			D9		
D10			D11			D12		
Z1	Z1	Z1	Z2	Z2	Z2	E2		

FIG. 4.2 ENCABEZADO DE SECCIÓN

B2 - Byte de código de paridad del bit MS intercalado. Este byte es utilizado para determinar si un error de transmisión ha ocurrido sobre una sección del multiplexor. Posee una paridad par y es calculado considerando el total de bits del Encabezado MS y del contenedor virtual STM-1 de la trama previa antes de ser codificada.

K1 y K2 - Bytes de conmutación de Protección Automática (canal APS, Automatic Protection Switch) Estos dos bytes son utilizados para la señalización de la protección automática bidireccional y la detección de la alarma (AIS) como para la detección de fallas de recepción en el extremo remoto de la línea.

D4 a D12 - Bytes de Canal de Comunicación MS - Estos 9 bytes forman un canal de mensajes a 576 Kb/s entre un centro OAM y diversas entidades (alarmas, mantenimiento, almacenamiento remoto, monitorco, etc.,). Este canal de mensajes puede enviar mensajes generados interna o externamente así como mensajes específicos del fabricante.

Z1 y Z2 - Bytes de crecimiento. Estos dos bytes están parcialmente definidos. El primer byte Z1 del primer STM-1 es utilizado para la información de sincronización. Los bits 1 al 4 del byte Z1 son utilizados para transportar mensajes de sincronización, el primer byte Z2 de un STM-1 es utilizado para una función de error de bloque en el extremo remoto de la capa MS.

E2 - Byte del Circuito de transferencia de Ordenes MS. Este byte proporciona un canal de 64 Kb/s entre las entidades para una transferencia de órdenes. Es un canal de voz destinado a los operadores y será ignorado al momento de pasar a través de regeneradores.

La conmutación de protección automática (APS) es la capacidad del sistema de transmisión para detectar una falla en el equipo en uso y conmutar al equipo de reserva para recuperar el tráfico. Esta capacidad representa una gran ventaja para el sistema completo.

En SDH, la transmisión es protegida en secciones ópticas desde la cabecera (el punto donde el encabezado MS es insertado) hasta el terminador (el punto donde el encabezado termina). Los bytes K1 y K2 dentro del encabezado MS de la señal STM-1 transportan un protocolo de protección de la MS (MSP) utilizado para coordinar la conmutación de protección entre la cabecera y el terminador.

La conmutación de protección es realizada en cada una de las siguientes situaciones:

- falla de la señal
- degradación de señal
- respuesta a comandos manuales

Existen dos modos de APS: conmutación de protección 1:1 y conmutación de protección 1:n.

En la conmutación de protección 1:1, existe un equipo de protección (línea de respaldo) para cada equipo en uso. En la cabecera, la señal óptica es puentada en forma permanente (dividida en dos señales) y enviadas sobre la línea en uso y sobre la de respaldo en forma simultánea, obteniéndose una señal de uso y una de respaldo idénticas.

En el terminador, ambas señales son monitoreadas en forma independiente. El equipo receptor selecciona cualquiera de las dos señales. Esta selección está basada en los criterios de inicialización de la conmutación válidos tanto en una situación de falla de la señal como de degradamiento en la señal.

En la conmutación de protección 1:n puede existir un equipo de respaldo (el rango es de 1 a 14). La conmutación es revertida, es decir, el tráfico se restablece en el equipo en uso tan pronto como la falla es corregida. En la conmutación de protección las señales ópticas son enviadas normalmente sólo sobre los equipos en uso mientras que el equipo de respaldo se mantiene libre hasta que falla algún equipo en uso.

Como se explicó anteriormente, una de las ventajas de SDH es que es sincrónico, el puntero de carga de información indica la compensación entre la trama del VC y la STM-1 identificando la localización del primer byte del VC dentro del contenedor. En otras palabras, el VC y la STM-1 van a flotar dentro del contenedor. Para hacer esto posible, dentro de cada trama STM-1, existe un puntero α como el puntero de la carga de información del VC, el cual indica el inicio del contenedor de la carga de información actual. Este puntero se localiza dentro de la columna 1 y la 4 del renglón 4 del encabezado de sección. Los bytes H1 y H2 del encabezado pueden considerarse como una palabra. El valor del puntero indica la compensación en bytes desde el puntero del primer byte del STM VC.

Ya que los bytes del encabezado de sección no se consideran y los puntos iniciales tienen incrementos de 3 bytes, el rango posible es:

$$\text{(Total de bytes STM-1 - Encabezado de transporte) / incremento de bytes}$$

$$(2430 - 81) / 3 = 783$$

Esto es, el valor del puntero tiene un rango de 0 a 782. Por ejemplo, si el puntero de la carga de información VC tiene un valor de 0, entonces el STM VC inicia en el byte adyacente del byte K2 del encabezado de sección. El valor del puntero, el cual es un número binario, es transportado de los bits 7 al 16. Los primeros 4 bits del puntero son para indicar si hay algún cambio en el VC y por lo tanto indicar un cambio arbitrario en el valor del puntero. Estos 4 bits son conocidos como bandera de información nueva.

El encabezado de ruta es asignado y transportado con la carga de información desde el momento en el que éste es creado por el equipo de ruta de terminación hasta que la carga de información es demultiplexada en el extremo final en una sección del equipo de ruta de terminación.

El encabezado de ruta se encuentra en los renglones 1 al 9 de la primera columna del VC STM-1. Byte por byte el encabezado de ruta se muestra a continuación en la figura 4.3

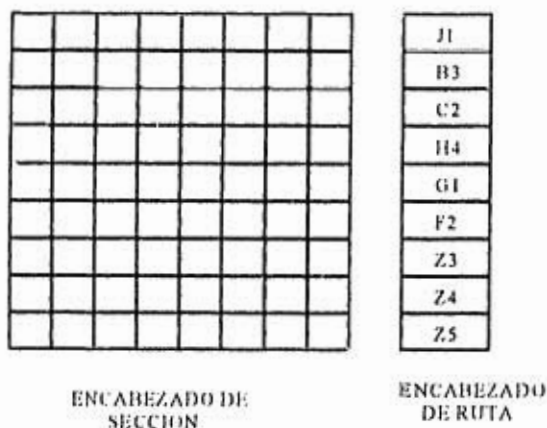


FIG. 4.3 ENCABEZADO DE RUTA

J1 - Byte de trazo de ruta STM. Este byte programable por el usuario transmite repetidamente una cadena de 64 o 16 bits. Esto permite a la terminal receptora dentro de la ruta verificar su conexión continua a la terminal emisora.

B3 - Byte de código de paridad intercalado de la ruta. Este es un código de paridad (par), utilizado para determinar si un error de transmisión ha ocurrido sobre la ruta. Ese valor es calculado considerando el total de bits del contenedor virtual (VC) previo, antes de ser codificado.

C2 - Byte de etiqueta de la señal. Este byte es utilizado para indicar si el STM no ha sido equipado (0) o equipado (1).

G1 - Byte de estatus de ruta. Este byte es utilizado para indicar el estatus de terminación de la ruta y el desempeño del equipo de terminación que la originó.

F2 - Byte de canal de usuario de la ruta. Este byte es utilizado para la comunicación del usuario con el resto de los elementos de la ruta.

H4 - Byte indicador de multitrama de la TU. Este byte proporciona un indicador de multitrama para los contenedores de la carga de información.

La porción del encabezado de ruta del VC permanecerá con la carga de información hasta que ésta sea multiplexada.

4.1.2 DQDB

El estándar 802.6 de IEEE define a la subred DQDB (Distributed Queue Dual Bus). DQDB se refiere a la topología y la técnica de control de acceso empleada, y subred se refiere a que una sola red DQDB será una componente de una colección de redes que proveen un servicio.

Una subred DQDB puede ser privada o una red pública como se muestra en la figura 4.4 Para soportar servicios a través de una área metropolitana, una red DQDB puede abarcar distancias en un rango que va desde unos pocos kilómetros hasta mas de cincuenta kilómetros operando a una gran variedad de velocidades. Las subredes DQDB pueden ser conectadas por medio de ruteadores o puentes, estas conexiones pueden ser punto a punto o pueden ser una red de conmutación de paquetes, de conmutación de circuitos o ISDN.

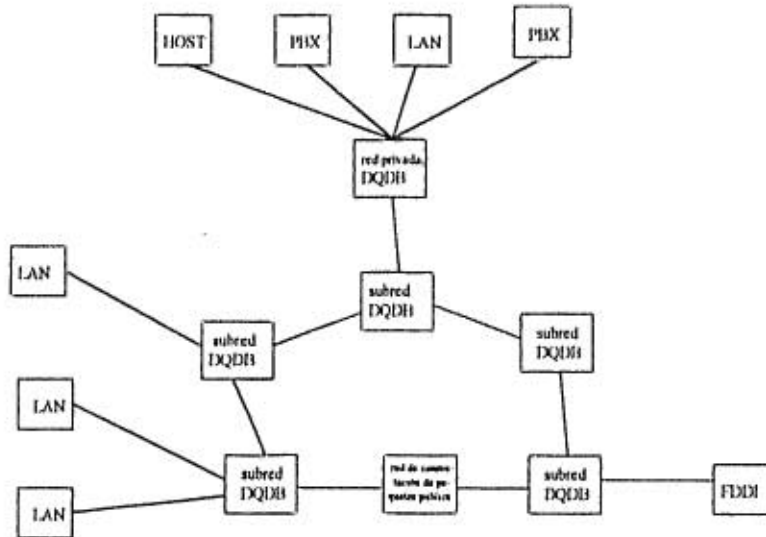


FIG. 4.4 SUBREDES DQDB

La topología que utiliza este estándar es de doble bus con transmisiones unidireccionales. La figura 4.5 describe un diagrama a bloques lógico de la configuración básica. La transmisión en los buses es independiente, de este modo, la velocidad efectiva de la red DQDB es dos veces la velocidad de un bus.

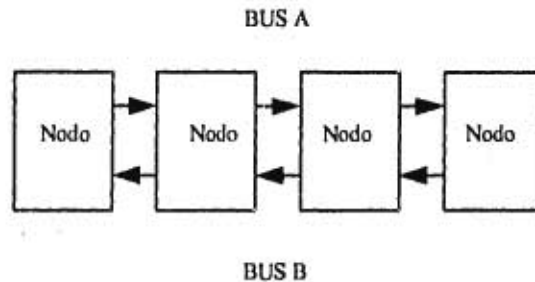


FIG. 4.5 CONFIGURACIÓN BÁSICA DE UNA SUBRED DQDB

Por claridad, usaremos el termino "upstream" para referirnos al flujo que se origina en la cabecera del bus y el termino "downstream" para el flujo en el sentido opuesto. El nodo que está en upstream del bus A, se designa como cabeza del bus A y el upstream B corresponde al mismo significado en el bus B.

DQDB define una unidad de longitud fija en su transmisión, la denomina slot y tiene una longitud de 53 octetos. Los nodos leen y copian los datos de los slots pero también tienen acceso a la subred escribiendo sobre ellos. La cabeza A es la encargada de generar los slots del bus A mientras que la cabeza B se encarga de generarlos en el bus B. Las cabezas A y B generan múltiples slots en los medios compartidos cada 125 μ s, el número de slots generados depende de la velocidad física de los datos.

La figura 4.6 describe la arquitectura del estándar 802.6 del IEEE definido como DQDB. Semejante al estándar 802. El estándar DQDB se divide en tres capas. La capa mas alta corresponde a la porción superior de la capa de enlace de OSI, en el caso del estándar para LAN de 802 corresponde a la capa LLC. En 802.6 se pueden soportar diferentes protocolos en esta capa.

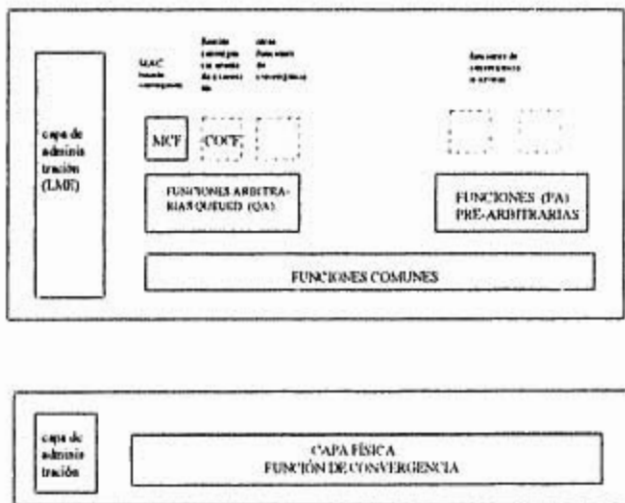


FIG. 4.6 ARQUITECTURA DEL ESTANDAR 802.6 DQDB

La capa intermedia esta referida como la capa DQDB, esta corresponde a la capa de MAC del estándar 802 para LAN, y como MAC, regula el acceso al medio compartido.

La capa mas baja de la arquitectura 802.6 es la capa fisica y esta definida para soportar diferentes esquemas de transmisión fisica. Explicaremos la capa DQDB:

Esta capa se puede organizar en tres subcapas:

- Funciones comunes
- Funciones arbitrarias
- Funciones convergentes

El módulo de **funciones comunes** tiene que ver con el retardo de los slots en las dos direcciones y provee una plataforma para servicios asincronos e isocronos. Además de la transmisión y recepción de slots, el modulo de funciones comunes es responsable de la cabeza del bus y control de configuración.

Las funciones de **cabeza de bus** son realizadas únicamente por uno o dos nodos designados como cabezas de bus. Estas funciones incluyen la generación y transmisión de slots. En la cabecera de los slots hay un bit que indica el tipo de slot, este es marcado por la cabeza del bus para indicar si se trata de un slot para datos isocronos o datos asincronos. La cabeza inserta también el identificador de canal virtual en la cabecera del slot.

La función del **control de configuración** esta involucrada con la inicialización de la subred y la reconfiguración después de una falla. Un ejemplo es la activación y desactivación de las funciones de cabeza de bus en los nodos apropiados durante el proceso de reconfiguración.

La función de **localidad de la pagina MID** participa en el protocolo de distribución con todos los nodos de la subred para controlar la localidad de los valores del mensaje ID a los nodos. El mensaje ID es usado en las funciones de segmentación y reensamblaje.

Las **funciones arbitrarias** son responsables del control de acceso al medio. Hay dos funciones, correspondientes a los dos tipos de slots que se transmiten en el bus.

Todos los slots del bus son de 53 octetos de longitud, consisten de un campo de control de acceso de 1 octeto y un segmento de 52 octetos. Los dos tipos de slots generados en la red son los Queued Arbitrated (QA) y los Prearbitrated (PA).

Los slots PA son utilizados para llevar datos sincronicos. Las funciones PA proveen el control de acceso para transferencia orientada a conexión sobre un canal con ancho de banda garantizado para octetos que forman parte de una cadena de octetos isócronos. La función PA asume el establecimiento previo de la conexión. Como resultado de la conexión establecida, la función PA será informada del ID del canal virtual (VCI) asociado con la conexión. El VCI es parte del campo de control de acceso y es generado por la función de cabeza de bus.

Los slots QA son utilizados para transportar datos asincronicos. La función QA provee el control de acceso para la transferencia de datos asincronicos en el segmento de 48 octetos de la carga de información. La función QA acepta segmentos de carga de información de la función de convergencia y le agrega una cabecera para formar su segmento.

El acceso a los slots QA en el medio DQDB es proporcionado por el protocolo DQAP (Distributed Queue Access Protocol) que es un esquema de reservación distribuida. Las dos palabras sugieren las claves del funcionamiento del protocolo:

Reservación: Para la mayoría de los esquemas de reservación, incluyendo este, el tiempo en el medio esta dividido en slots, como el TDM asincrono. Un nodo que quiera transmitir reserva el siguiente slot.

Distribuida: Para organizar lo requerimientos, el esquema de reservación debe de ser dinámico. Esto es que los nodos hacen reservación cuando tienen datos que transmitir

El esquema de reservación distribuida para una subred DQDB tiene que tomar en cuenta la naturaleza de la topología que emplea. La esencia del protocolo se puede describir de la siguiente manera:

Si un nodo X desea transmitir un paquete de datos a un nodo Y. X debe de elegir el bus en el que Y este en downstream de X, supongamos en este caso que se trata del bus A, entonces X espera un slot que venga upstream (A). Si alguna estación que este upstream (A) de X monopoliza el bus A, X no puede transmitir y necesita hacer una petición de reservación a los nodos que estén upstream de el. Para ello necesita utilizar el bus B, y ya que las estaciones que se encuentran upstream(A) de X, también se encuentran downstream(B) de X y pueden recibir la petición de reservación de X para el bus A.

El protocolo requiere que cada estación defina su propia necesidad de transmitir comparada con la necesidad de los nodos que se encuentran downstream de el.

El comportamiento actual de un nodo depende de su posición en el bus. Existen 4 posiciones significativas (con respecto al bus A) que se muestran en la figura 4.7 la cual muestra una subred DQDB con N nodos. Consideremos el primer caso: el nodo (N-1) que es la cabecera B. Este nodo no tiene nodos downstream (A) y por lo tanto no transmite datos en el bus A y no necesita hacer reservación del bus B y la única actividad en el bus A es la de recepción.

Ahora consideremos el nodo mas cercano a la cabecera B que en esta caso esta identificado como el nodo (N-2), cuando este quiere transmitir datos tiene que hacer la reservación del bus A haciendo uso del bus B, a pesar de usar el bus B para hacer reservación del bus A, este nodo nunca recibe ninguna reservación en el bus B.

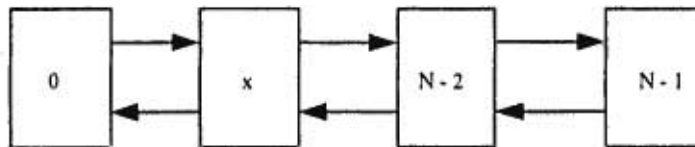


FIG. 4.7 SUBRED DQDB

El tercer caso es el nodo 0 que es la cabecera (A) que como tal es responsable de la generación de la cadena de slots para el bus A, por lo que no habrá slots QA en el bus A que vayan dirigidos a este nodo. Cuando este nodo desea transmitir lo único que tiene que hacer es insertar sus datos en el próximo slot que genere y debido a que no hay nodos upstream de él no necesita hacer ninguna reservación, mas sin embargo tiene que atender las reservaciones que se han hecho sobre el bus B y esta situación puede hacer que este nodo tenga que esperar para transmitir sus propios datos

El último caso es cuando se trata de un nodo x, que es el caso que ya discutimos.

Para que el nodo 0 pueda asignar la prioridad de cada reservación hecha sobre el bus B se vale del protocolo PDQ (Priority Distributed Queueing). Cada segmento tiene 3 bits de prioridad, uno para cada nivel de prioridad, a un nodo que desea transmitir en el bus A y tiene una prioridad en particular, enciende el bit apropiado en el siguiente slot que pasa por el bus B.

Las unidades de datos del protocolo DQDB son usadas para soportar las funciones de la capa DQDB.

Como ya habíamos mencionado, la unidad de datos en DQDB es el slot de 53 octetos, en el cual se depositan los diferentes tipos de datos. A diferencia de la mayoría de los protocolos DQDB utiliza la misma unidad de datos para datos QA y PA.

Los slots son continuamente generados por las cabezas de bus, por lo que nunca existe un periodo de silencio en el bus. Un slot está comprendido por un octeto definido como el Campo de Control de Acceso (ACF) y 52 octetos de segmento como se muestra en la figura 4.8.

El ACF contiene bits que controlan el acceso al slot incluyendo un bit que indica si se trata de un slot PA o QA. Los subcampos del ACF en el orden en que se transmiten son:

Bit de ocupado: Indica si el slot contiene información (1) o si está vacío (0).

Bit de tipo de slot: Este bit indica si es un slot QA (0) o un slot PA (1).

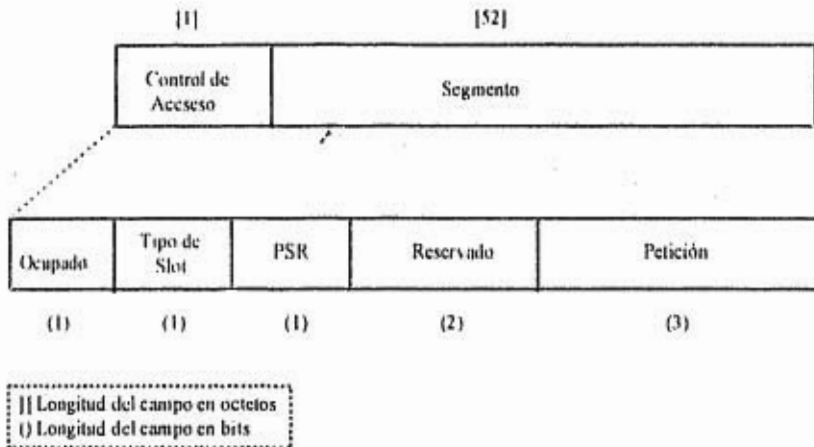


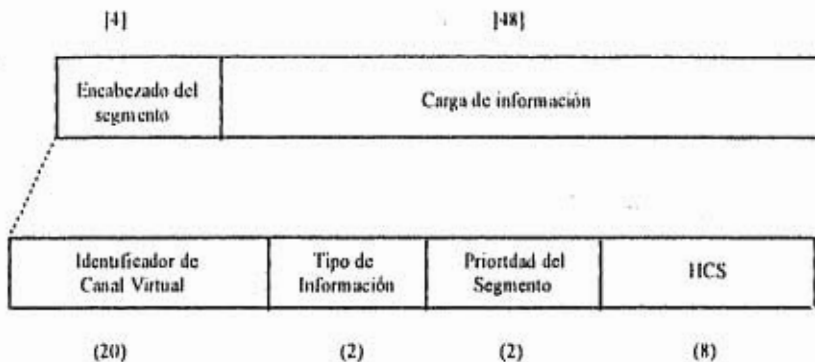
FIG. 4.8 CAMPO DE CONTROL DE ACCESO (ACF)

Bit de segmento previo recibido: Indica si es que el segmento del slot anterior debe de ser borrado (1) o no (0). Esta operación se reservo para futuros estudios.

Bits de reservación: Puestos en 00

Bits de petición: Para solicitar el acceso a un slot QA en uno de los buses, una estación debe de encender el bit de petición en un slot del otro bus. Tres bits de petición son usados para tres diferentes niveles de prioridad para el acceso a slots QA.

El segmento son los 52 octetos de la carga de información de un slot. Comprende 4 octetos de encabezado de segmento y 48 de carga de información. El encabezado de segmento es el mismo para slots QA y PA, aunque pueden ser interpretados de diferente manera. El segmento se muestra en la figura 4.9.



[] Longitud del campo en octetos
 () Longitud del campo en bits

FIG. 4.9 ENCABEZADO DEL SEGMENTO

El Identificador de Canal Virtual (VCI) es un campo de 20 bits utilizado para identificar el canal virtual a donde pertenece el segmento. Un canal virtual es una conexión lógica entre dos puntos de la red. Un valor del VCI en el que todos los bits está encendidos es el de default para servicios MAC no orientados a conexión.

El campo de Tipo de Carga de información es un valor de dos bits que indica el tipo de datos que se van a transmitir. Se intenta utilizar este campo para subredes DQDB conectadas por puentes en donde el valor puede hacer la diferencia entre datos de usuario y datos de red.

El campo de Prioridad de Segmento es otro valor de 2 bits que se piensa usar en puentes multipuertos.

Finalmente el HCS (Header Check Sequence) es usado para detectar errores de bits en el encabezado de segmento y una posible corrección de los mismos. DQDB utiliza un polinomio CRC-8 para este propósito, donde el polinomio generador es:

$$G(x) = x^8 + x^2 + x + 1$$

4.2 ARQUITECTURA ATM

4.2.1 INTRODUCCION

Modo de transferencia asincrónico, ATM (Asynchronous Transfer Mode), en sus orígenes ATM surgió como el modo de transferencia de la red digital de servicios integrados de banda ancha (B-ISDN). Pero en la actualidad ATM puede utilizarse, tanto para redes públicas como privadas y para interconectar otras tecnologías como Frame Relay, SMDS, FDDI, además de redes LAN. Esto debido a que ATM soporta velocidades de transmisión de 155 Mbps y 622 Mbps. Y en un futuro será capaz de soportar velocidades tan altas como 10 Gbps. Además como una opción, ATM opera también a velocidades DS3's (45 Mbps) y hasta DS1's (1.544 Mbps).

La definición del ITU-T contenida en la recomendación I.113 dice: "ATM es el modo de transferencia en el que la información se organiza en celdas de tamaño fijo; es asincrónico ya que la recurrencia de las celdas que contiene la información de un canal individual no es necesariamente periódica".

Como se dijo en la anterior definición, en ATM la información se transporta en celdas de tamaño fijo. Cada una con 5 bytes de encabezado y 48 bytes de información. Los sistemas de conmutación ATM procesan o regeneran los encabezados de las celdas, no así los 48 bytes de información, que pasan en forma transparente por toda la red.

El flujo de celdas se transfiere en forma continua, sin interrupciones, con una velocidad fija, y la demanda de ancho de banda es según el servicio. En ausencia de tráfico se transfieren celdas no asignadas (Unassigned Cells), y en presencia de tráfico se reemplazan celdas no asignadas por celdas asignadas (figura 4.10).

Dentro de un flujo de celdas pueden viajar celdas pertenecientes a diferentes servicios, cada uno con su ancho de banda requerido. Si dos o más servicios quieren transferir celdas al mismo tiempo, tienen que "competir" para reemplazar las celdas no asignadas con su tráfico. Algunas tendrán que esperar en fila para entrar al flujo, de aquí el término asincrónico. Esto se realiza con tecnología de multiplexaje estadístico.

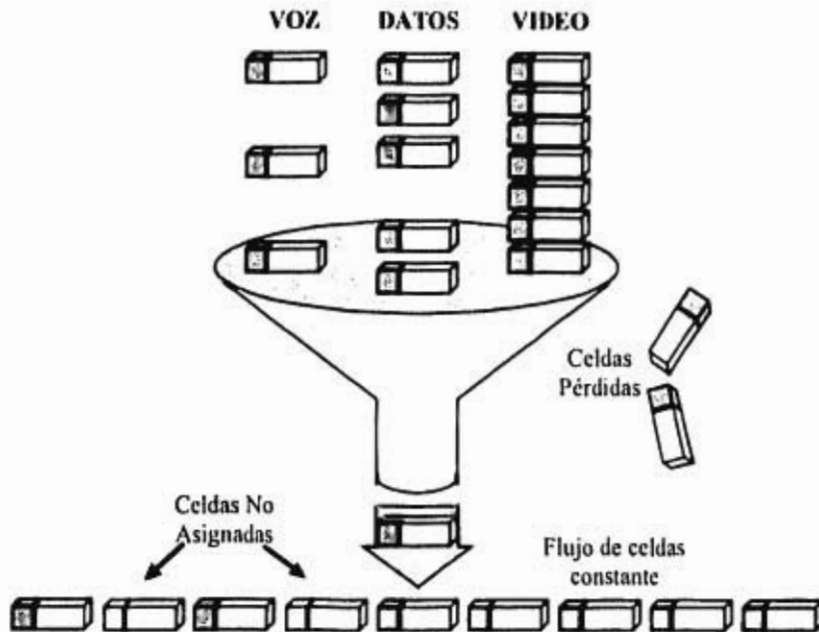


FIGURA 4.10 MULTIPLEXAJE ESTADISTICO ATM

4.2.2 MODELO B-ISDN

Como se dijo anteriormente, en sus orígenes ATM surgió como el modo de transferencia de B-ISDN, por lo tanto es importante describir brevemente la arquitectura de este modelo B-ISDN.

La arquitectura del modelo B-ISDN consiste de tres planos y cuatro capas, como se muestra en la figura 4.11. los planos de este modelo son: plano de usuario, de control y de administración.

El plano del usuario provee la transferencia de información de usuario a usuario y da control para la transferencia de información, tal como control de flujo y control de recuperación de errores.

El plano de control provee la transferencia de información para el establecimiento de la conexión, señalización y supervisión de una conexión.

El plano de administración se divide en dos partes: la capa de administración y el plano de administración. Este último realiza las funciones relacionadas con la totalidad del sistema, esto significa coordinar funciones entre todos los planos, incluyendo la obtención de información del estado de cada plano, y la información a otros planos de ese estado. La capa de administración realiza funciones de administración relacionadas con el desempeño, operación y administración de recursos para cada uno de los planos del usuario.

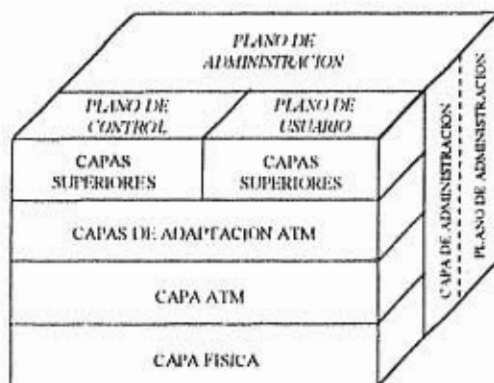


FIGURA 4.11 ARQUITECTURA DE B-ISDN

4.2.3 CAPAS Y SUBCAPAS ATM

La figura 4.12 muestra las capas, subcapas, y funciones del protocolo ATM.

Funciones de la capa física

Como se muestra en la figura 4.12 la capa física se divide en dos subcapas:

Subcapa PM (Physical Medium), la subcapa del medio físico es la interface con el medio físico, pasa y recupera el flujo de bits hacia la subcapa TC. Esta subcapa provee la capacidad de transmisión de bits, incluyendo el alineamiento y codificación de bits, y si es necesario, la conversión eléctrico-óptico (no necesariamente el medio es óptico).

Capa	Subcapa	Función
AAL	CS	Convergencia
	SAR	Segmentación y Reensamblaje
ATM		Control de Flujo Genérico Generación y Extracción del encabezado de celda Frasación de VPI/VCI Multiplexión y Demultiplexión de celdas
PHY	TC	Ajuste de la velocidad de las celdas Generación y verificación de HEC Delineación de las celdas Adaptación de las tramas de transmisión Generación/recuperación de tramas de trans
	PM	Sincronización de bits Medio Físico

FIGURA 4.12 CAPAS, SUBCAPAS Y FUNCIONES ATM

Subcapa TC (Transmission Convergence), la subcapa TC es la segunda subcapa de la capa física, esta subcapa TC realiza las cinco funciones siguientes:

- *Generación y recuperación de tramas de transmisión:* La función básica es generar y recuperar las tramas necesarias para “empacar y desempacar” celdas.
- *Adaptación de la trama de transmisión:* El proceso de generación y recuperación de la trama requiere reconocer la estructura de la trama empleada. Esta estructura de tramas debe ser adaptada para el transporte de celdas ATM.
- *Delineación de la celda:* La subcapa TC debe proveer un mecanismo para que el receptor detecte los límites de las celdas desde el flujo de bits que entran.
- *Generación y verificación del HEC:* El control de error de encabezado es empleado sólo en el encabezado de las celdas, el transmisor genera el HEC y el receptor lo chequea, si el valor recibido del HEC no concuerda, se trata de corregir el error, si esto no es posible se descarta la celda.

- *Acoplamiento de la velocidad de las celdas:* Celdas ociosas son insertadas durante la transmisión y son removidas durante la recepción. El propósito de este mecanismo es para acoplar la velocidad de las celdas ATM a la capacidad de transporte del sistema de transmisión. Sólo las celdas no ociosas pasan a la capa ATM.

Funciones de la capa ATM

Las funciones de la capa ATM son independientes del medio físico, estas funciones se realizan sobre las celdas y básicamente son cuatro: Multiplexaje, traslación de VPI/VCI, generación del encabezado y control de flujo.

- *Multiplexaje y demultiplexaje de celdas:* En el lado del transmisor la capa ATM multiplexa celdas de rutas y canales virtuales individuales a un flujo de celdas. En el lado del receptor demultiplexa celdas, de un flujo de celdas entrante, tomando en cuenta la ruta y el canal virtual.
- *Traslación de VPI/VCI:* La traslación de VPI's y VCI's es la base del switcheo ATM, esto es realizado por los switches (conmutadores) ATM. Los identificadores de ruta virtual y canal virtual que entran a un switch son cambiados para salir de este. Estos nuevos valores son obtenidos de una tabla en el switch, esta tabla es construida a la hora de la conexión por el protocolo de mensajes de señalización del plano de administración de ATM. Puede no ser necesario cambiar los valores de VPI's y VCI's, y mantenerlos en la conexión de fin a fin.
- *Generación y extracción del encabezado de la celda:* La capa ATM genera e interpreta los encabezados de las celdas y sólo la carga de información de la celda es pasada hacia las capas superiores. En el lado transmisor, después de recibir la carga ATM de la capa de adaptación (48 bytes), se añade el encabezado de la celda, excepto el campo HEC. En el lado del receptor el encabezado de la celda es extraído y los 48 bytes restantes son enviados a las capas de adaptación ATM (AAL).
- *Control de flujo genérico.* El GFC es una función definida sólo en la interface del usuario a red (UNI) para proveer el control de flujo de acceso.

Funciones de las Capas de Adaptación ATM (AAL's)

La función básica de las capas de adaptación ATM (AAL) es trasladar datos desde las capas superiores hacia las celdas ATM de longitud fija. Las capas AAL se dividen en dos subcapas: La subcapa de segmentación y reensamblaje (SAR) y la subcapa de convergencia (CS).

Subcapa de segmentación y reensamblaje (SAR): La función de esta subcapa es segmentar la información de longitud variable proveniente de capas superiores para ser transmitidas en celdas ATM. Y reensambla la carga de celdas ATM hacia las capas superiores formando los PDU's (Unidades de datos del protocolo) en su forma original. En pocas palabras, el proceso de segmentación es como cortar una larga cadena de datos en piezas de 48 bytes para manejarlas fácilmente. Y el proceso de reensamblaje es volver a unir estas piezas de 48 bytes en la cadena de datos original.

Subcapa de Convergencia (SC): Las funciones que realiza la subcapa de convergencia (CS) dependen de la clase de servicio, es decir, son dependientes del servicio. La recomendación I.362 define cuatro clases de servicios que dependen de los siguientes tres parámetros:

Relación de sincronía entre la fuente y el destino. También conocida como aplicaciones de "tiempo real". El tráfico tal como voz digitalizada debe mantener una relación de sincronía sobre la red. Esta relación de sincronía es esencial en aplicaciones de voz y otras aplicaciones de velocidad de bits constante (CBR). La frase "relación de sincronía" significa esencialmente que el retardo de tiempo para los bits que se envían a través de la red, debe de ser constante.

Velocidad de bits. Algunos servicios tienen tasa de bits constante (CBR), otros tienen tasa de bits variable (VBR). Las aplicaciones CBR incluyen video y voz digitalizada no comprimidos. Es importante notar que servicios CBR automáticamente pasan a ser VBR con la adición de la compresión.

Modo de conexión. Existen dos tipos de modos de conexión: orientada a conexión y sin conexión. En servicios que son orientados a conexión, debe establecerse una conexión antes de la transferencia de información. Dos ejemplos son Frame Relay y el tráfico de emulación de circuitos.

El modo sin conexión no requiere establecer una conexión para la transferencia de información. En este servicio, cada paquete tiene la dirección fuente y destino, tal que pueda ser conmutada individualmente en la red. Un ejemplo de tal servicio es SMDS y tráfico de LAN's.

El uso de cuatro clases de servicio A, B, C, y D (figura 3.13), descritas a continuación, minimiza el número de protocolos AAL.

Clase A: Servicio orientado a conexión, con relación de sincronía entre la fuente y el destino y velocidad de bits constante. Como ejemplos incluiremos voz digitalizada PCM, vídeo con velocidad de bits constante y circuitos DS1's.

Clase B: Servicio orientado a conexión, velocidad de bits variable y con relación de sincronía entre la fuente y el destino. Como ejemplos tenemos audio y vídeo comprimidos.

Clase C: Servicio orientado a conexión, velocidad de bits variable y sin relación de sincronía entre la fuente y el destino. Como ejemplos incluiremos tráfico Frame Relay y X.25.

Clase D: Servicio sin conexión, velocidad de bits variable y sin relación de sincronía entre la fuente y el destino. Como ejemplos tenemos tráfico SMDS y LAN.

	CLASE A	CLASE B	CLASE C	CLASE D
Relación de sincronía entre fuente y destino	Requerido		No Requerido	
Velocidad de bits	Constante	Variable		
Modo de Conexión	Orientado a Conexión			Sin conexión
Aplicaciones	Voz, Vídeo, emulación de circuitos	Voz o Vídeo comprimidos	Tráfico Frame Relay o X.25	Tráfico SMDS y LAN

FIGURA 4.13 CLASES DE SERVICIO AAL

Existen cuatro diferentes tipos de capas de adaptación ATM (AAL) para optimizar la transmisión de estas cuatro clases de tráfico.

Clase A: AAL tipo 1

Clase B: AAL tipo 2

Clase C: AAL tipo 3/4 y AAL tipo 5

Clase D: AAL tipo 3/4 y AAL tipo 5

4.3 ESTRUCTURA ATM

4.3.1 CONCEPTO DE CELDA

En ATM la información se transporta en unidades de datos de longitud fija (53 bytes), llamadas celdas. Cada una con 5 bytes de encabezado y 48 bytes para datos del usuario (figura 4.14). Existen muchas razones para el uso de la celda como la unidad básica de datos en ATM. Estas razones se detallan a continuación :

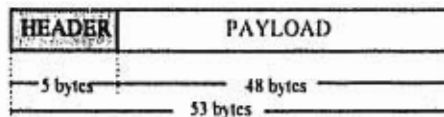


FIGURA 3.14 ESTRUCTURA DE CELDA ATM

- Nuestros anteriores sistemas de comunicaciones trataban con caudales de bits, ahora con sistemas basados en celdas tratamos con paquetes de un tamaño reducido y fijo. Aumentado la unidad fundamental, con lo que se logra aumento en el desempeño de conmutadores, terminales y dispositivos de comunicación. Este aumento de desempeño es análogo al efecto que se observa cuando se aumenta el tamaño de palabra o el ancho del bus de un sistema de computación.
- ATM busca ofrecer una amplia variedad de servicios (voz, datos, vídeo) con requerimientos diferentes sobre una plataforma única. La celda permite hacer esto. Segmentando el tráfico en celdas y multiplexando el tráfico de diferentes servicios. Controlando cuidadosamente la ubicación y la ruta de estas celdas en nuestra red, podemos agregar tráfico con diferentes retardos y requerimientos de ancho de banda en el mismo sistema.

- Las celdas también nos permiten ofrecer un ancho de banda considerablemente mayor, debido a que éstas controlan y conmutan más eficientemente, que las viejas tecnologías orientadas a caudales de bits.
- Cada celda tiene un tamaño fijo, lo cual permite implementar los sistemas de conmutación y manipulación de celdas directamente sobre el "hardware", lo que nos evita tener que manejarlas mediante programas.
- Cada celda también contiene información de direccionamiento y control, de manera que podemos colocar las funciones de conmutación directamente sobre el "hardware", incrementando el desempeño sobre los sistemas que requieren "software" y microprocesadores para examinar los caudales de datos y determinar la ruta que estos deberán tomar.
- Las celdas también nos permiten realizar sistemas de multiplexaje más eficientes. Debido a que el ancho de banda de un sistema basado en celdas puede ser otorgado en incrementos muy pequeños (celdas), podemos otorgar anchos de banda más cuidadosamente, permitiendo que las transmisiones de video y datos, voraces en cuanto ancho de banda, puedan coexistir con el tráfico de voz.
- La información de control incluida en cada celda permite extraer e insertar eficientemente información en enlaces de comunicación multiplexados. Utilizando el encabezado y el direccionamiento de la celda para multiplexar y demultiplexar el tráfico, es posible extraer solamente las partes de información que interesan en cada enlace, dejando pasar el resto (llamado multiplexaje de inserción/extracción o "Add/Drop").

La elección del tamaño de la celda tiene una importancia determinante para poder transmitir, recibir y procesar estas celdas. Como ya se dijo ATM usa celdas de 53 bytes. Una razón para preferir el tamaño pequeño de celdas es reducir el desperdicio. Cuando un transmisor coloca datos en las celdas, por lo regular, la última celda no está completamente llena, por lo tanto se desperdiciará, muchas veces, casi en su totalidad está última celda.

Otra razón para preocuparse por el tamaño de las celdas, es el retardo, considerando que una de las metas de las redes ATM, es permitir que servicios de voz, video y datos corran sobre la misma red.

El tamaño de 53 bytes para celdas ATM se definió en base a las necesidades de los diferentes tipos de servicios: Para transferencia de archivos (datos), es mejor tener celdas largas (no importa mucho el retardo), pero las aplicaciones de voz y video, que son menos tolerantes al retardo introducido, requieren celdas cortas.

4.3.2 CONEXIONES ATM: VPI's Y VCI's.

Cada encabezado de celda ATM contiene información que identifica la trayectoria que deberá seguir esta celda. Esta identificación tiene dos partes y ambas son usadas en la capa ATM, un identificador de ruta virtual (VPI) y un identificador de canal virtual (VCI).

Una ruta virtual es un paquete de enlaces de canales virtuales, todos teniendo el mismo punto final. Así, la ruta virtual es como un gran cable multipar telefónico, donde todos los circuitos terminan en una oficina central. El VPI es asignado o removido para originar o terminar un enlace de ruta virtual. Estos enlaces son concatenados en forma de una conexión de ruta virtual (VPC). Cada enlace de canal virtual dentro de una conexión de ruta virtual mantiene la secuencia de transmisión de celdas, pero no asegura la integridad de una celda individual.

La recomendación ITU-T 311 define un canal virtual como "una capacidad de conexión unidireccional para el transporte de celdas ATM". Un VCI es asignado o removido, respectivamente, al originar o terminar un enlace de canal virtual. Enlaces de canales virtuales son concatenados para formar una conexión de canal virtual (VCC), una ruta para las celdas de fin a fin en la capa ATM.

La ruta de transmisión física (figura 4.15) contiene rutas virtuales y sus VPI's así como también, canales virtuales y sus VCI's.

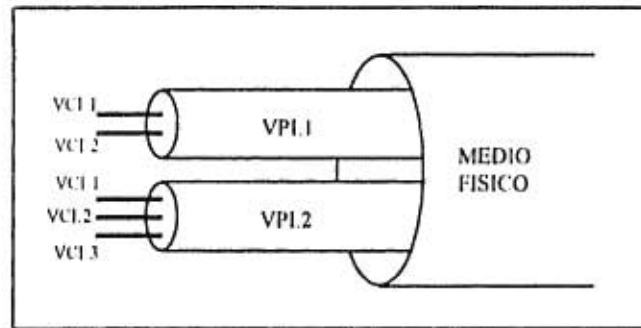


FIGURA 4.15 RELACION ENTRE VPI's Y VCI's

El enlace de canal virtual conecta a un equipo terminal (TE) con un nodo ATM (figura 4.16). La concatenación de dos o más enlaces de canales virtuales forman una conexión de canal virtual (VCC). Similarmente VPC's transportan grupos de VCC's sobre una base de fin a fin.

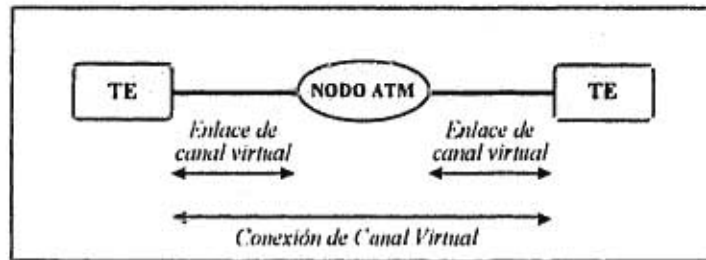


FIGURA 4.16 CONEXIÓN Y ENLACE DE CANALES VIRTUALES

4.3.3 FORMATO DE CELDAS ATM

Como se menciono anteriormente, las celdas ATM se componen de 53 bytes, de los cuales 5 bytes son para el encabezado y los 48 bytes restantes son para información de capas superiores.

Para el encabezado de la celda ATM, existen dos tipos de formatos: La interface de usuario a red (UNI), la cual es la interface entre el usuario y la red, tal como se muestra en la figura 4.17a. Y la interface entre nodos de red (NNI), la cual es la interface, como su nombre lo dice, entre nodos de red, como se muestra en la figura 4.17b.

Formato de celdas UNI

El formato de celdas UNI consiste de seis campos, como se muestra en la figura 4.18a.

GFC (Generic Flow Control): Este campo consiste de cuatro bits y provee funciones locales, tales como un sencillo control de flujo. Este campo tiene significancia local y no de fin a fin, y es sobrescrito por switches ATM intermedios. Así, el campo GFC sólo está presente en celdas entre usuario y red (UNI).

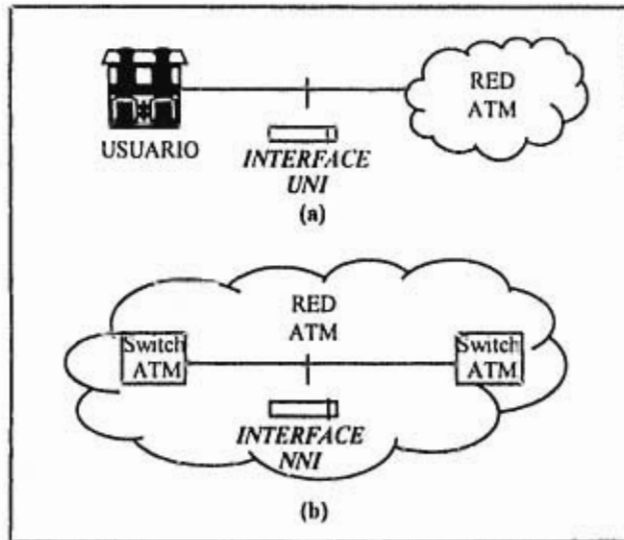


FIGURA 4.17 INTERFECES UNI Y NNI ATM

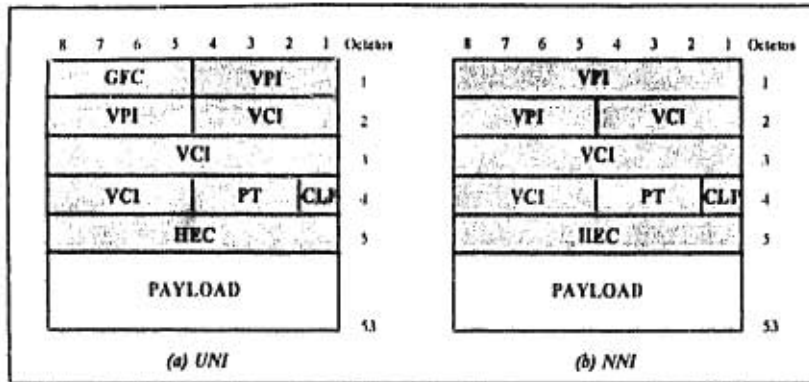


FIGURA 4.18 FORMATO DE CELDAS ATM

VPI (Virtual Path Identifier): El campo VPI consiste de 8 bits y es usado para identificar una ruta virtual, con lo que se busca establecer una conexión de ruta virtual (VPC). El campo VPI permite simplificar el ruteo en la red. El campo VPI es usado en la fijación de conexiones de rutas virtuales de fin a fin o para múltiples segmentos de ruta virtual. Una ruta virtual contiene múltiples canales virtuales.

VCI (Virtual Channel Identifier): El campo VCI contiene 16 bits, es usado para establecer conexiones de canales virtuales. La especificación UNI 3.0 define algunos valores VPI/VCI para funciones específicas, tales como usar un canal para establecer la señalización y celdas con operaciones de administración y mantenimiento (OAM). Algunos ejemplos de estos valores son:

VPI	VCI	FUNCION
0	0	Celdas no asignadas o desocupadas
0	4	Flujo de datos de fin a fin
0	5	Señalización
0	15	SMDS

PT (Payload Type): El campo PT consta de 3 bits, los cuales identifican el tipo de información contenida en la celda. Este campo tiene definidos 8 valores.

PT	INTERPRETACION
000	Datos de usuario, no congestión, SDU (Service Data Unit) tipo 0
001	Datos de usuario, no congestión, SDU tipo 1
010	Datos de usuario, congestión, SDU tipo 0
011	Datos de usuario, congestión, SDU tipo 1
100	Información OAM (Operacions Administration and Maintenance)
101	Información OAM de fin a fin
110	Reservado para futuro control de tráfico
111	Reservado para funciones futuras

CLP (Cell Loss Priority): El campo CLP consta de un sólo bit que el usuario o la red usan para indicar, explícitamente, la prioridad de pérdida de celda. Una celda con el campo CLP = 1 que entra a la red, indica que ésta puede ser descartada, bajo ciertas condiciones de tráfico en la red. Mientras CLP = 0 indica que esta celda no debe de ser descartada a menos que no haya otra alternativa.

HEC (Header Error Control): El campo HEC consta de 8 bits. El HEC realiza el calculo de CRC los primeros 4 bytes del encabezado de la celda para detección y corrección de errores. La secuencia HEC es utilizada para reducir la pérdida de celdas. El HEC realiza control de errores sólo en el encabezado de la celda ATM y no para toda la celda.

Formato de celdas NNI

El encabezado de celdas NNI (figura 4.18b) consta también de 5 bytes, con un formato que es idéntico al formato UNI, excepto por el primer octeto. El formato NNI, el cual provee grupos de VCI's entre switches, define cuatro bits adicionales para el campo VPI. En otras palabras, el formato NNI usa 12 bits para el campo VPI y 16 bits para el campo VCI.

4.4 CAPAS DE ADAPTACION ATM (AAL)

4.4.1 AAL 1

Esta capa de adaptación soporta tráfico clase A, el cual es enviado a una velocidad de bits constante (CBR); orientado a conexión; y con relación de sincronía entre la fuente y el destino. Como ejemplos de este tráfico podemos incluir voz codificada PCM o video CBR.

La AAL consiste de dos subcapas: La subcapa de convergencia (CS) y la subcapa de segmentación y reensamblaje (SAR). Para AAL 1, la subcapa CS toma la información del usuario y la divide en PDU (Unit Data Protocol) o unidades de datos del protocolo, de 47 octetos, tal como se muestra en la figura 4.19. Estos paquetes de datos son conocidos como AAL1-CS-PDU, los cuales serán la carga de información de la unidades AAL1-SAR-PDU. Note que aún no se añade información de control de protocolo (PCI) al paquete AAL1-CS-PDU.

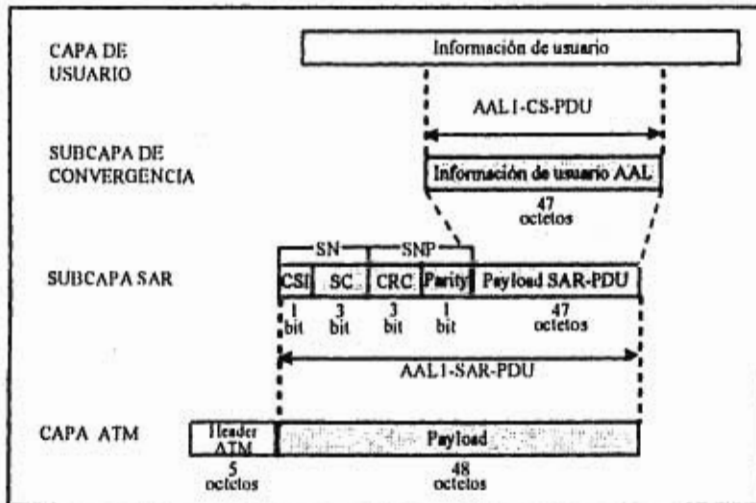


FIGURA 4.19 FORMATO PDU AAL 1

La subcapa SAR añade un encabezado con longitud de un octeto a el paquete AAL1-CS-PDU, logrando con esto formar un paquete AAL1-SAR-PDU de 48 octetos de longitud, figura 4.19. El encabezado del paquete AAL1-SAR-PDU consta de dos campos: SN (número de secuencia) y SNP (protección del número de secuencia).

Campo SN: El campo SN consta de dos subcampos: CSI (indicador de subcapa de convergencia), el cual es sólo un bit y es usado para funciones específicas. Una función del bit CSI es pasar información de sincronía entre el transmisor y el receptor. En este método llamado SRTS (Synchronous Residual Time Stamp) el campo CSI transporta marcas de paquetes AAL1-SAR-PDU sucesivos. El segundo subcampo es el SC (contador de secuencia), el cual consta de 3 bits y se encarga de contar la secuencia de paquetes, por lo tanto su función principal es detectar celdas perdidas o no insertadas.

Campo SNP: El campo SNP contiene dos subcampos: El subcampo CRC, el cual contiene 3 bits de chequeo de redundancia cíclica. Y el subcampo Parity de un bit de paridad único. Estos dos subcampos dan un control de error para los subcampos CSI y CS.

4.4.2 AAL 2

Esta capa de adaptación soporta tráfico clase B, el cual es enviado a una velocidad de bits variable; orientado a conexión; y con relación de sincronía entre la fuente y el destino. Como ejemplos tenemos voz y video con velocidad de bits variable (VBR).

La ITU-T aún está desarrollando el protocolo AAL 2. No obstante, un formato sugerido para AAL2-SAR-PDU se muestra en la figura 4.20. Esta estructura consiste de 3 campos, en encabezado, el payload y el trailer.

El subcampo SN (Sequence Number), en el encabezado PDU, detecta las celdas perdidas o sin insertar. El subcampo IT (Information Type) indica el tipo de información que esta siendo transportada, tal como BOM (comienzo del mensaje), COM (continuación del mensaje) o EOM (fin del mensaje). En el trailer PDU, el campo LI (Length Indicator) es usado para indicar el número de bytes que transporta el campo SAR-PDU payload. Por último el CRC protege al PDU contra errores.

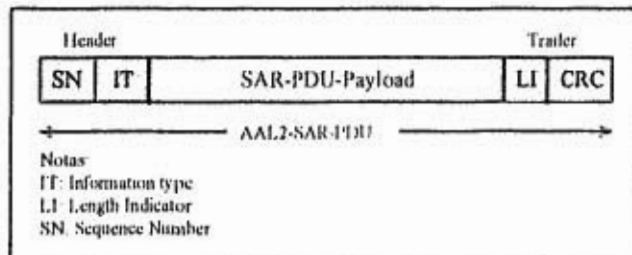


FIGURA 4.20 FORMATO PDU AAL 2

4.4.3 AAL 3/4

Esta capa de adaptación ATM soporta tráfico clase C o D, el cual es enviado a una velocidad de bits variable (VBR) y no requiere relación de sincronía entre la fuente y el destino. En un principio surgieron dos estándares: AAL 3, el cual soportaba tráfico orientado a conexión, y AAL 4, el cual soportaba tráfico sin conexión. Estos dos estándares emergieron como AAL 3/4. Esta capa de adaptación es usada por tráfico de datos, el cual es sensible a la pérdida, pero no al retardo, tal como SMDS.

La subcapa de convergencia AAL 3/4 está dividida en dos subcapas: SSCS (Service Specific Convergence Sublayer), la cual puede no estar presente (Null), soporta la capa de usuario. Y CPCS (Common Part Convergence Sublayer), la cual transfiere bloques de longitud variable de datos, mejor conocidos como AAL3/4-CPCS-SDU's, secuencialmente entre usuarios.

El proceso que realiza AAL 3/4 es inicializado cuando la información del usuario (AAL3/4-CPCS-SDU) es pasada hacia la subcapa AAL3/4-CPCS (figura 4.21), esta subcapa añade un header y un trailer, formando el paquete AAL3/4-CPCS-PDU.

Este paquete es entonces pasado a la subcapa SAR, la cual segmenta el paquete AAL3/4-CPCS-PDU a paquetes AAL3/4-SAR-PDU de 48 octetos para llegar a ser el payload de las celdas ATM.

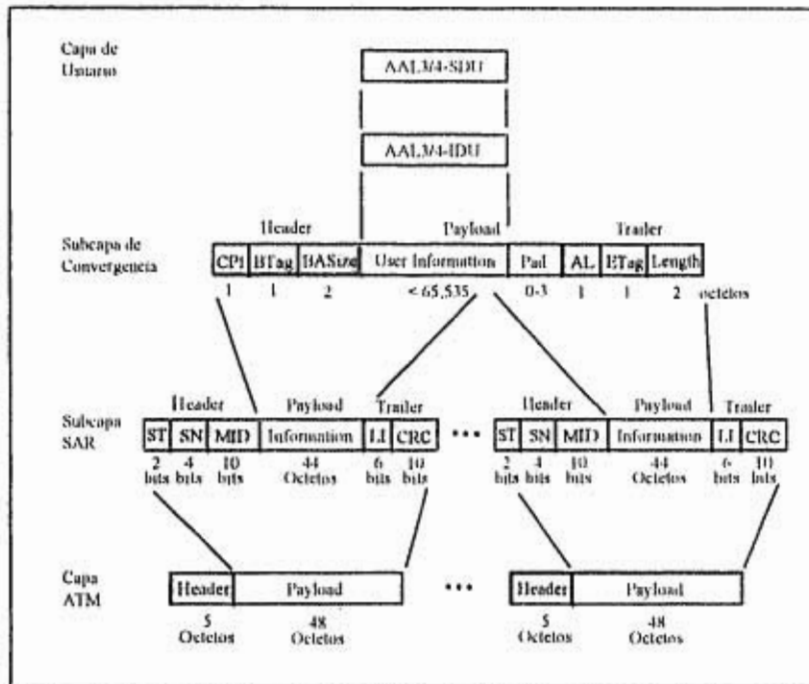


FIGURA 4.21 FORMATO PDU AAL 3/4

El header del paquete AAL3/4-CPCS-PDU contiene 3 campos: CPI (Common Part Indicator), BTag (Begin Tag) y BAsize (Buffer Allocation Size)

CPI: El campo CPI (1 octeto) identifica el tipo de mensaje y las unidades de conteo para los campos BTag y BAsize. Este campo es actualmente codificado como 00h, lo cual indica que la unidad de conteo es el octeto.

BTag: El campo BTag (1 octeto) es usado conjuntamente con el campo ETag (End Tag) en el trailer, y sirven para asociar el comienzo y el final de la unidad AAL3/4-CPCS-PDU. El mismo valor es puesto en los campos BTag y ETag, y es incrementado para paquetes sucesivos AAL3/4-CPCS-PDU.

BAsize: El campo BAsize (2 octetos) le indica al proceso de recepción AAL3/4 el máximo tamaño del buffer que este debe reservar para reensamblar las unidades AAL3/4-CPCS-PDU que entran.

En payload de la unidad AAL3/4-CPCS-PDU es donde se deposita la información del usuario y está limitado al máximo valor del campo BAsize (65,535) veces el valor contenido en el campo CPI (típicamente octetos). Un campo Pad puede ser colocado después del campo de información, este Pad puede contener cero, uno, dos o tres octetos de relleno, lo cual obliga a las unidades AAL3/4-CPCS-PDU a ser alineadas a 32 bits.

El trailer de los paquetes AAL3/4-CPCS-PDU contiene tres subcampos AL (Alignment), ETag (End Tag) y Length.

AL: El campo AL (1 octeto) provee alineación de 32 bits en el trailer AAL 3/4 y es puesto a 00h.

ETag: El campo ETag (1 octeto), como ya se dijo es usado conjuntamente con el campo BTag, para asociar el comienzo y el final del paquete AAL3/4-CPCS-PDU.

Length: El campo length (2 octetos) indica la longitud en unidades de conteo (normalmente octetos) del campo de información de usuario.

La subcapa SAR provee el transporte de paquetes de 48 octetos hacia celdas ATM. Cada paquete AAL3/4-SAR-PDU contiene un header (2 octetos), un payload o información de usuario (44 octetos) y un trailer (2 octetos).

El header del paquete AAL3/4-SAR-PDU contiene tres subcampos: ST (Segment Type), SN (Sequence Number) y MID (Multiplexing Identification).

ST: El campo ST (2 bits) indica si el paquete AAL3/4-SAR-PDU es el comienzo de un mensaje (BOM, con ST = 10), la continuación de un mensaje (COM, con ST = 00), el fin de un mensaje (EOM, con ST = 01), o un único segmento de mensaje (SSM, con ST = 11).

SN: El campo SN (4 bits) es un contador que indica la posición secuencial de cada paquete AAL3/4-SAR-PDU asociado con un paquete, de la subcapa superior, AAL3/4-CPCS-PDU.

MID: El subcampo MID (10 bits) identifica el paquete AAL3/4-SAR-PDU derivado desde un paquete AAL3/4-CPCS-PDU particular. En otras palabras, muchos paquetes AAL3/4-CPCS-PDU pueden ser transmitidos simultáneamente entre dos usuarios AAL. El campo MID identifica el paquete AAL3/4-SAR-PDU desde diferentes AAL3/4-CPCS-PDU's.

La sección de payload del paquete AAL3/4-SAR-PDU contiene información de usuario y de relleno y tiene una longitud de 44 octetos. Si el campo de información de usuario no contiene 44 octetos, el campo de relleno lo complementa con ceros.

La sección trailer del paquete AAL3/4-SAR-PDU contiene dos campos: LI (Length Indicator) y un CRC.

LI: El campo LI (6 bits) contiene la longitud en octetos del campo de información de usuario. El tipo de segmento, tal como lo indica el campo ST, restringe los valores del campo LI.

CRC: El campo CRC (10 bits) es llenado con el resultado obtenido de realizar el cálculo de un CRC sobre el encabezado del paquete AAL3/4-SAR-PDU.

4.4.4 AAL 5

Esta capa de adaptación soporta tráfico clase C y D, el cual es orientado y no orientado a conexión, velocidad de bits variable (VBR) y no requiere relación de sincronía entre la fuente y el destino. El proceso que realiza AAL 5 es considerado mucho más simple que el de AAL 3/4. AAL 5 también es conocida como la AAL simple y eficiente (SEAL, Simple and Efficient AAL).

La capa de usuario pasa información de usuario de 0 a 65,535 octetos de largo, hacia la subcapa CPCS, tal como se muestra en la figura 4.22. La subcapa CPCS genera los paquetes AAL5-CPCS-PDU, los cuales se componen de una sección de payload una de trailer.

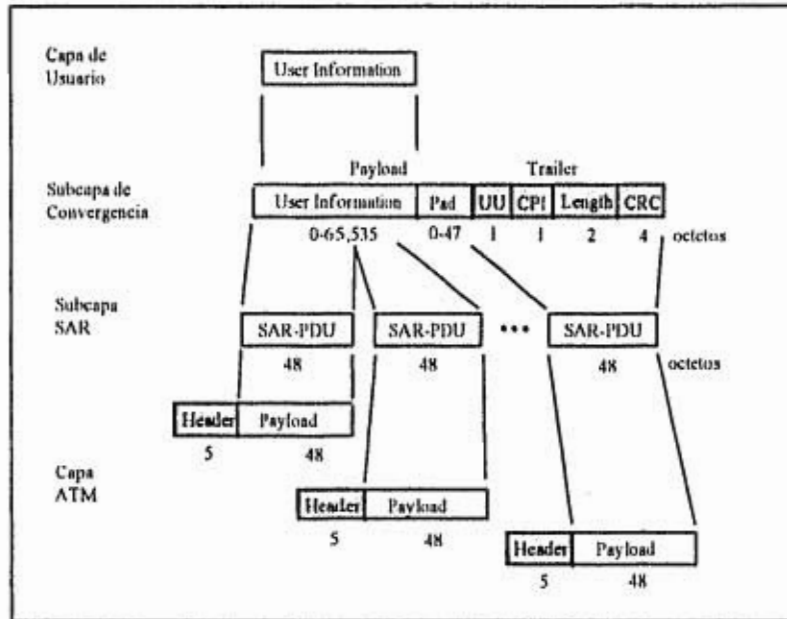


FIGURA 4.22 FORMATO PDU AAL5

La sección de trailer del paquete AAL5-CPCS-PDU consiste de cuatro campos, UU (User to User), CPI (Common Part Indicator), Length y CRC.

UU: El campo UU (1 octeto) contiene información que es transferida de forma transparente entre usuarios AAL 5. Este campo actualmente no se usa y es puesto a cero.

CPI: El campo CPI (1 octeto) se encarga de alinear la sección del trailer. Otros usos están aún en desarrollo y pueden incluir identificación de mensajes de la capa de administración.

Length: El campo Length (2 octetos) indica la longitud del payload en el paquete AAL5-CPCS-PDU.

CRC: El campo de CRC (4 octetos) contiene un calculo de CRC32 que detecta errores de bits en el paquete AAL5-CPCS-PDU, incluyendo el payload y los primeros cuatro octetos del trailer.

Cuando el paquete AAL5-CPCS-PDU es ensamblado, la subcapa SAR segmenta este paquete en otros llamados AAL5-SAR-PDU de 48 octetos, los cuales son pasados a la capa ATM.

Un bit llamado PT1 en el campo PT del encabezado de la celda ATM detecta el comienzo y el fin del paquete AAL5-CPCS-PDU. Este bit es puesto a cero para los segmentos primero e intermedio, y es puesto a uno para el último segmento.

4.5 PRIORIDADES Y CONTROL DE TRAFICO ATM

4.5.1 ACCIONES PARA EL CONTROL DE TRAFICO ATM

La ITU, en la recomendación I.311, ha definido un conjunto de funciones que todas las redes ATM deben implementar para realizar el control de tráfico. Estas funciones, actualmente cuatro, son:

Control de Admisión de la Conexión

La admisión de la conexión ATM es realizada a la hora del establecimiento de llamada, cuando un VCC (Conexión de Canal Virtual) y un VPC (Conexión de Ruta Virtual) son establecidos. La red ATM sólo aceptará una llamada, si la red tiene los recursos para entregar la calidad de servicio (QOS) de fin a fin, a la petición del usuario, a través de la red.

El aspecto más crítico de la calidad de servicio es determinar las características del tráfico fuente: ¿Exactamente qué es requerido por el usuario?. Este tráfico fuente puede ser caracterizado por cuatro parámetros.

El primero es la velocidad de bits promedio, el cual es sólo una media aritmética sobre el tiempo. El segundo es la velocidad de bits pico, estos dos valores forman un importante concepto en redes ATM: *Burstiness*, o velocidad de ráfaga. La siguiente ecuación relaciona estos dos conceptos:

$$Burstiness = \frac{Velocidad_pico}{Velocidad_promedio}$$

El tercer parámetro es la velocidad física de bits del enlace desde el usuario hasta el nodo local ATM. Las velocidades de bits física, promedio y pico, pueden ser todas diferentes, todas la misma o pueden ser todas cero. En el caso de que todas sean cero, el Forum ATM ha definido una conexión de este tipo ABR (Available Bit Rate). Esto significa que la conexión es asignada cualquiera que sea la velocidad de bits, si el proceso de admisión de la conexión ha determinado estar disponible a un tiempo particular.

El último parámetro es la duración del pico. La duración del pico es la medida de cuanto tiempo la fuente es capaz de mantener la velocidad de bits pico. Una vez más es absolutamente necesario conocer este parámetro antes de que la conexión sea aceptada.

Conociendo estos cuatro parámetros y la clase de servicio del usuario (QOS), la red ATM tiene toda la información que necesita para decidir si debe otorgar la conexión o no. Estos valores pueden ser negociados entre la red y el usuario a la hora de la conexión. En otras palabras una conexión que ha sido rechazada con una velocidad de pico de 10 Mbps, puede tratar de conseguir una conexión ajustando esta velocidad de pico a 5 Mbps. Los cuatro parámetros aquí explicados son candidatos para negociación.

Control de Parámetros Acordados

Las redes ATM deben "vigilar" la interface usuario-red (UNI) para garantizar que el volumen de tráfico de celdas no afecte el desempeño global de la red. Por ejemplo, si una conexión es otorgada sobre la red ATM basada en cierta velocidad de inserción de celdas, o ancho de banda, la red ATM monitorea la conexión para asegurar que la velocidad aceptada no es excedida.

El control de parámetros tratados de tráfico ATM está diseñado para proteger a la red de cambios en los parámetros que se tenían cuando se otorgo la conexión. El proceso de control monitorea el volumen de tráfico desde el usuario. De esta forma la red ATM no permite que sean cambiados los parámetros del tráfico fuente con los cuales se otorgo la conexión.

Control de Prioridades ATM

Debido a que las celdas son conmutadas a través de la red ATM, las colas se desarrollan como una consecuencia natural de los retardos de propagación y retardos de procesamiento (en los nodos de la red) asociados con grandes cargas de usuarios. Las celdas deben de ser almacenadas en buffers hasta que puedan ser procesadas. Algunas celdas tendrán que ser descartadas. Para permitir esto, el encabezado de la celda ATM tiene un campo de un sólo bit llamado CLP (Prioridad de pérdida de celda). Este único bit permite sólo dos estados: Prioridad alta o baja.

La decisión de como se le asigna la prioridad a cada celda puede ser hecha de dos formas:

La aplicación que envía información puede marcar sus propias celdas, esto es debido a que la aplicación, presumiblemente, conoce que celdas son menos importantes. Por ejemplo, algunas celdas en tráfico de voz pueden ser catalogadas con prioridad baja, lo que ocasionaría sólo una pequeña reducción en la calidad de la voz.

La otra opción es que la red marque las celdas con alta o baja prioridad. La red observa el flujo de celdas que entran a ésta, si el flujo excede la velocidad acordada. La red marca algunas celdas con prioridad baja, esto con el objeto de ajustar este flujo a la velocidad acordada. Esto podría tener algunas complicaciones, ya que la red típicamente no conoce la importancia relativa de cada celda en la aplicación. No obstante este método es muy amigable con el cliente, ya que sólo hará esto en periodos de alto tráfico en la red.

El proceso de buscar y descartar las celdas con prioridad baja, aún no se estandariza, pero muchos mecanismos han sido propuestos para realizar esta tarea.

Uno de estos mecanismos consiste de un buffer común que se encarga de expulsar determinadas celdas, todas las celdas llegan al mismo buffer, si el buffer está lleno y una celda que no puede ser descartada llega, entonces se busca en el buffer una celda con prioridad baja, para poder eliminarla. Este es un proceso complejo que puede llevar algún tiempo.

Existe otro mecanismo llamado separación de buffers, en el cual dos buffers separados son usados para cada posibilidad del bit CLP. Entonces las celdas con el bit $CLP = 1$ pueden fácilmente ser encontradas y descartadas. No obstante las celdas garantizarán estar en secuencia, sólo si todas éstas tienen la misma prioridad, en una conexión de ruta. Esto no es siempre posible de asegurar sobre la conexión en la red ATM.

Por último, la estrategia más prometedora es conocida como ajuste parcial del buffer. En este mecanismo las celdas de baja prioridad, sólo serán aceptadas si en buffer a menos de un x porcentaje lleno. Esto es fácil y eficiente de implantar.

Control de Congestión

La congestión en las redes de banda ancha está definida como el estado de los elementos de la red (switches, concentradores, enlaces de transmisión), en el cual debido a la sobrecarga de tráfico, la red no puede garantizar la calidad de servicio que se negoció en el establecimiento de la conexión y será necesario establecer una nueva.

La congestión puede ser causada por condiciones de falla dentro de la red, o fluctuaciones impredecibles de tráfico, es decir, un usuario o usuarios pueden usar más recursos que los que solicitaron, al otorgárseles la conexión.

4.5.2 PARAMETROS QUE DEFINEN LA CLASE DE SERVICIO (QOS)

La recomendación ITU-T I.350 define los parámetros para medir la calidad de servicio (QOS), o desempeño de una red ATM, de fin a fin, orientada a usuario. El Forum ATM ha promovido este trabajo para definir los parámetros de la calidad de servicio y las configuraciones de referencia para la interface de usuario-red (UNI).

El fabricante del switch, o el proveedor de la red, establecen los objetivos exactos del desempeño de la calidad de servicio (QOS), los cuales están basados sobre términos y parámetros definidos por la recomendación ITU-T I.350 y los documentos UNI-ATM. Estos parámetros son:

Relación de Celdas Erradas:

$$CER = \frac{EC}{SCT + EC}$$

donde: *CER*: Relación de celdas Erradas
EC: Celdas Erradas
SCT: Celdas Transferidas Exitosamente

Relación de Bloque de Celdas Erradas Severamente:

$$SECBR = \frac{SECB}{TTCB}$$

donde: SECBR: *Relación de Bloque de celdas Erradas Severamente*
SECB: *Bloque de Celdas Erradas Severamente*
TTCB: *Total de Bloques de Celdas Transmitidas*

Relación de Celdas Pérdidas:

$$CLR = \frac{LC}{TTC}$$

donde: CLR: *Relación de celdas Pérdidas*
LC: *Celdas Pérdidas*
TTC: *Total de Celdas Transmitidas*

Relación de Celdas Mal Insertadas:

$$CMR = \frac{MC}{TI}$$

donde: CMR: *Relación de celdas Mal Insertadas*
MC: *Celdas Mal Insertadas*
TI: *Intervalo de Tiempo*

En adición a estos parámetros, tres pruebas miden la velocidad de la red. El retardo de transferencia de celdas (CTD), es el lapso de tiempo entre cuando una celda deja la UNI origen, y ésta entra en la UNI receptora, para una conexión particular. La media del retardo de transferencia de celdas (MCTD), es el promedio aritmético de CTD's específicos para una o más conexiones. La variación del retardo de la celda (CDV), mide la variabilidad de los eventos de llegada a diferentes puntos en la red. El CER, SECBR y CMR, afectan la precisión en la red. El CLR afecta seriamente la red, y el CTD, MCTD y CDV afectan la velocidad de la red.

Los proveedores de la red deben definir valores objetivos para que las clases de servicio A, B, C y D (soportadas por las AAL's) sean aplicables.

QOS Clase 1: Para el desempeño de clases de servicio A, el cual debe ser equivalente a líneas privadas digitales.

QOS Clase 2: Para el desempeño de clase de servicio B, usado para audio y video comprimido, usado en aplicaciones de teleconferencia y multimedia.

QOS Clase 3: Para el desempeño de clase de servicio C, usado con protocolos orientados a conexión, tales como Frame Relay.

QOS Clase 4: Para el desempeño de clase de servicio D, usado con protocolos sin conexión, tales como IP y SMDS.

4.5.3 MULTIPLEXAJE ESTADISTICO

Una de las principales capacidades que posee ATM es el multiplexaje estadístico, el cual atiende la explosión de encendido-apagado de ráfagas de datos. La naturaleza de ráfagas de muchos tipos se ilustra en la figura 4.23. En el lado superior izquierdo se pueden ver muchas fuentes originando ráfagas de celdas: Un video display, un server, una cámara y un monitor. En la parte inferior se puede observar la suma de estas ráfagas de información. En este ejemplo en particular. Sólo dos canales son necesarios en cualquier tiempo. Por medio de la estadística la suma de estas ráfagas de información podrá ser más predecible.

El número de canales C requeridos para lograr el CLR esperado, se calcula por medio de la siguiente ecuación.

$$C \approx \frac{N}{b} + \frac{\alpha \sqrt{N(b-1)}}{b}$$

donde : N : Número de fuentes
 b : Burstinnes (velocidad de ráfaga, sección 4.5.1)
 α : Número promedio de llegadas de ráfagas por segundo

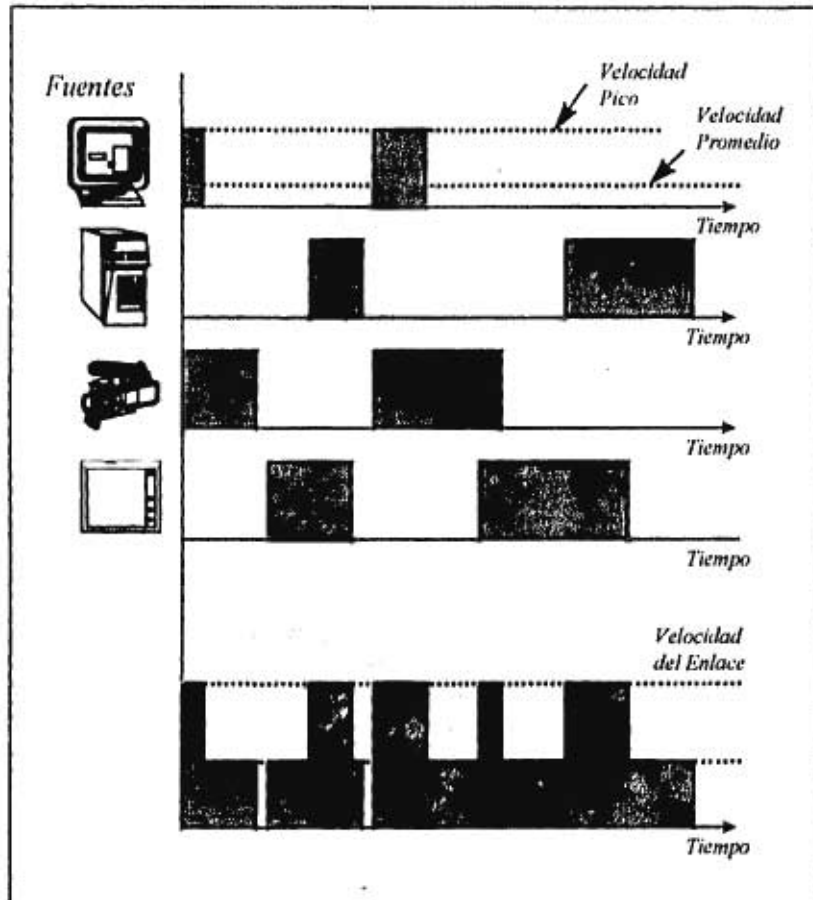


FIGURA 4.23 ESTIMACION DE CANALES REQUERIDOS POR DIVERSAS FUENTES

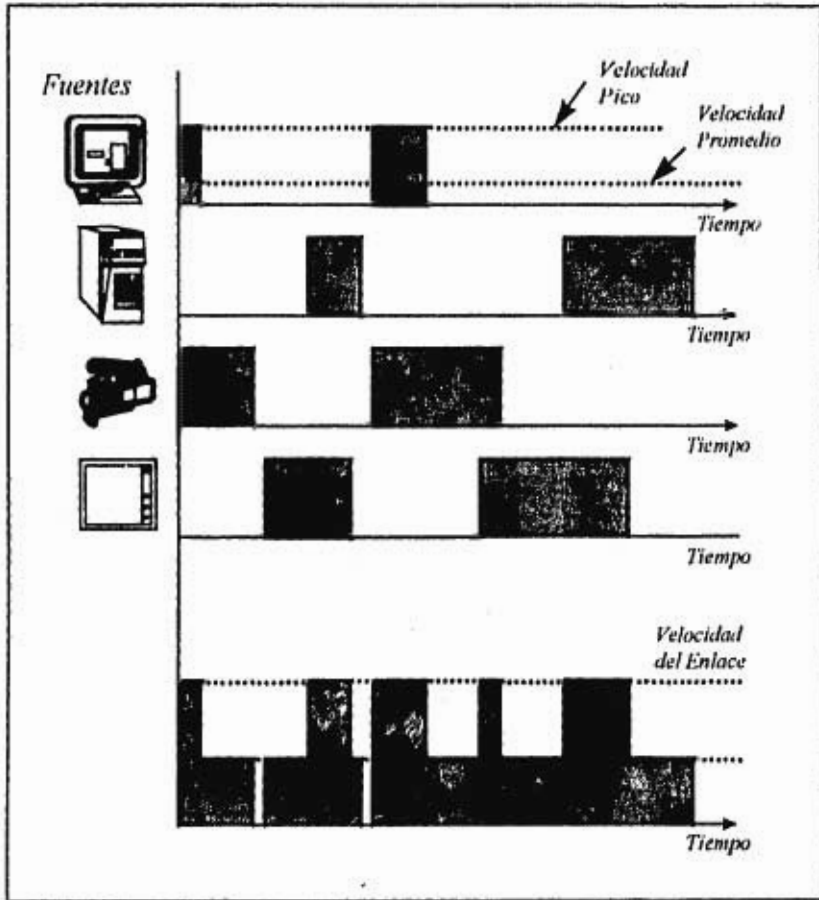


FIGURA 4.23 ESTIMACION DE CANALES REQUERIDOS POR DIVERSAS FUENTES

4.5.3 OPERACIÓN BÁSICA DE UN SWITCH ATM

La operación básica de un switch ATM es muy simple: el switch recibe una celda de un enlace con los valores VCI y VPI conocidos; entonces busca el valor de la conexión en una tabla de traslación local para determinar el puerto de salida de una conexión y entonces se asigna un nuevo valor VPI/VCI para ese enlace y se retransmiten las celdas con los identificadores apropiados de conexión.

La figura 4.24 esquematiza perfectamente la operación de un switch ATM.

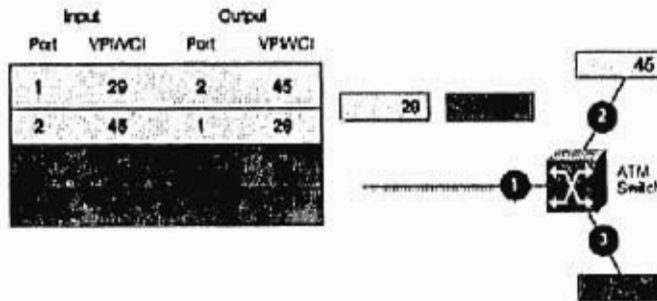


FIGURA 4.24 OPERACIÓN DE UN SWITCH ATM

CAPITULO V

INTEGRACION DE FDDI EN ATM

5.1 ANTECEDENTES

5.1.1 INTRODUCCION

El interés en la interconexión de redes LAN, a través de redes de alta velocidad, se ha incrementado enormemente debido a que nuevas aplicaciones con fuertes exigencias, en cuanto ancho de banda, han surgido.

Una de las importantes tendencias actuales en telecomunicaciones la constituye el surgimiento de redes de banda ancha que brindan un ancho de banda más allá de las velocidades T1/E1. El crecimiento explosivo de las interconexiones entre redes locales (LAN's) es en este momento causa de cuellos de botella en la tradicional infraestructura de las redes WAN. El crecimiento de las aplicaciones de banda ancha y de multimedia y el deseo de integrar voz, datos y vídeo en una infraestructura común de comunicaciones, contribuye a su vez a estos cuellos de botella.

Se ha elegido la tecnología ATM (modo de transferencia asíncrona) como la técnica de multiplexado y conmutación para usarse en redes WAN. Se ha elegido ATM por su flexibilidad a la hora de transmitir servicios de comunicaciones con diferentes características de transferencia. Puede llevar servicios de velocidades constantes o variables, servicios isócronos (voz y vídeo) o asíncronos (datos), así como soportar servicios orientados a las conexiones o sin conexiones. El entorno de conmutación ATM es dependiente de la velocidad de datos y admite la conmutación tanto de redes públicas como redes de área local a velocidades ultra altas que superan 1 Gbps.

5.1.2 CONCEPTO INTERNETWORKING

La interconexión de redes LAN comprende todas las aplicaciones entre las cuales se conectan varias LAN entre sí, formando una gran red de gran tamaño. La interconexión de redes "Internetworking" se implementa por diversas razones:

- Conectar las LAN's de distintos lugares en una sola red.
- Conectar entre sí las LAN de los distintos departamentos de la organización, formando una red que comprende a toda la empresa.

- Subdividir una gran red de gran envergadura en segmentos, por razones administrativas, de seguridad o funcionamiento.

Soluciones de interconexión más comunes

Los productos más comunes utilizados en la interconexión de redes son los repetidores, puentes y ruteadores (figura 5.1). La aplicación del usuario determina el producto a utilizar.

Repetidores: Regeneran la señal de la red en distancias más grandes. Operan en el nivel físico del modelo OSI y no interfieren ni controlan los datos. Los repetidores son sencillos y de bajo costo. Su principal desventaja es que dejan pasar todo el tráfico entre las distintas LAN, creando una congestión innecesaria.

Puentes: Conectan redes distintas en una única red lógica, operan al nivel MAC del modelo OSI y realizan la conexión decidiendo qué paquetes transferir entre las LAN. La mayoría de los puentes aprenden automáticamente la configuración de la red y toman decisiones de retransmisión en base a las direcciones de origen y de destino en los paquetes de las LAN. Los puentes son sencillos de instalar y de operar, y transparentes a la aplicación del usuario.

Ruteadores: Conectan redes separadas formando una red de mayor dimensión. Operan al nivel de red del modelo OSI (nivel 3) por lo cual dependen del protocolo. Pueden interconectar LAN's con distintos niveles MAC. Hoy en día la mayoría de los routers son multiprotocolo y cumplen funciones de puente para los protocolos no enrutables. Los routers admiten cualquier topología y brindan el método más rentable de enrutar y compartir cargas.

Los puentes pueden ser locales o remotos. Los puentes locales conectan dos o más LAN's locales en forma directa; los puentes locales conectan LAN's distantes a través de una WAN (red de área extendida).

Los puentes cumplen su función de filtrado y retransmisión comparando las direcciones de origen y de destino de la capa MAC, utilizando para ello tablas de direcciones de LAN aprendidas dinámicamente.

Los routers, al igual que los puentes pueden ser locales o remotos. Pero a diferencia de los puentes, los routers operan al nivel 3 (nivel de red) del modelo OSI, y dependen del protocolo. Esto significa el router debe soportar el protocolo específico en cuestión si es que ha de enrutar. En la actualidad los protocolos más en uso son TCP/IP e IPX de Novell.

Los routers seleccionan el modo más eficaz de transportar un paquete de datos a su destino. Esto se logra almacenando y actualizando con frecuencia una tabla completa de direcciones de destino de la red. En cualquier momento, el router sabe cual es la mejor manera de llegar a cierto destino.

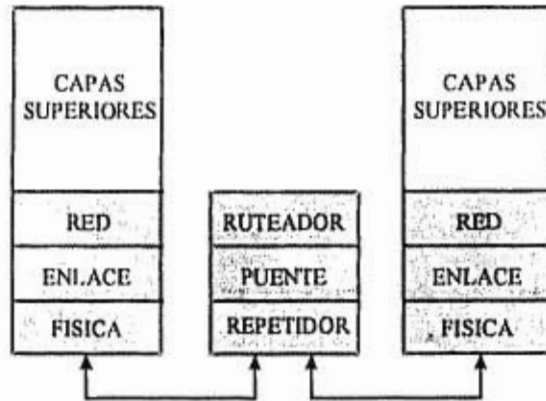


FIGURA 5.1 UBICACION DE LOS CONCEPTOS DE RUTADOR, PUENTE Y REPETIDOR DENTRO DEL MODELO OSI

5.2 PLANTEAMIENTO DEL PROBLEMA

5.2.1 ESCENARIO DE TRABAJO

El propósito de este trabajo consiste en el análisis de la interconexión de dos redes LAN FDDI's a través de una red ATM, tal como se describe en la figura 5.2

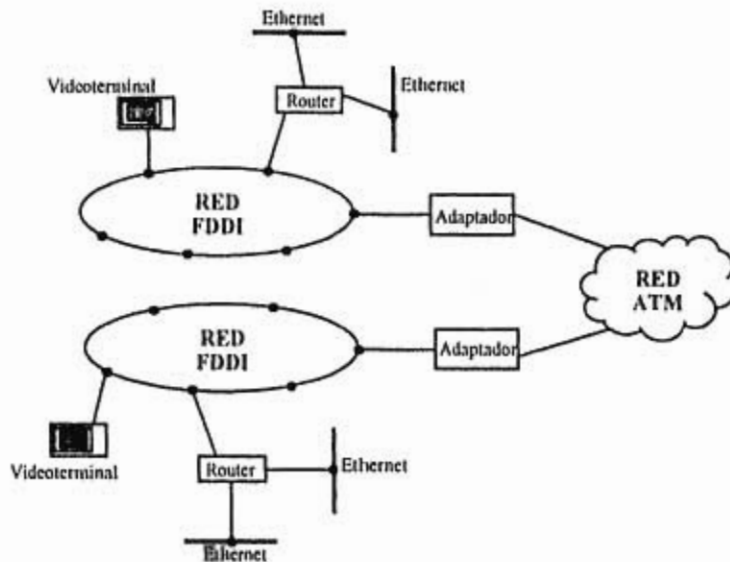


FIGURA 5.2 ESCENARIO DE TRABAJO

Los elementos que forman este ambiente de trabajo son descritos a continuación:

Redes de área local FDDI

FDDI (Fiber Distributed Data Interface) es actualmente la tecnología para redes locales de alta velocidad, esto debido al alto desempeño de la fibra óptica.

Ambas FDDI soportan 35 estaciones, uniformemente situadas a lo largo del anillo, en tal forma que la distancia entre dos estaciones FDDI's vecinas es de 200 m. En estos anillos hay dos tipos de estaciones, caracterizados por el tipo de tráfico que manejan.

Tráfico asíncrono: Este tráfico consiste de un paquete de datos provenientes de un router (ruteador), el cual enlaza muchas redes LAN Ethernet. Todas estas comunicaciones usan la serie de protocolos TCP/IP.

Tráfico sincrónico: Este tipo de tráfico corresponde a secuencias de video. La razón para empaquetar tráfico de video en tramas IP permite que estas sean transmitidas sobre cualquier tipo de red, siempre y cuando el ancho de banda y el desempeño, en cuanto a retardo, de esta red satisfagan los requerimientos de los equipos terminales.

Red ATM

Esta red está basada en canales virtuales, y este desempeño corresponde a las primeras características de B-ISDN, como se describió, en el capítulo anterior, la velocidad pico se acuerda antes de otorgar el enlace y no cambia durante el enlace. Esto lleva a las siguientes consecuencias:

- Los usuarios son responsables de no exceder la velocidad pico contratada.
- La tecnología que da soporte a esta red (F.O.) asegura una velocidad de bits errados muy baja.
- Las celdas perdidas y las variaciones de retardos dentro de la red son muy bajas, debido a las condiciones estrictas de acceso, lo cual limita la velocidad pico de las ráfagas ATM.
- El servicio sin conexión es ofrecido sobre rutas y canales semipermanentes

Adaptador FDDI-ATM

Este adaptador se comporta como un ruteador, pues transforma paquetes IP provenientes del anillo FDDI en una secuencia de celdas ATM, y reconstruye paquetes IP de un flujo de celdas que provienen de la red ATM, tal como se muestra en la figura 5.3

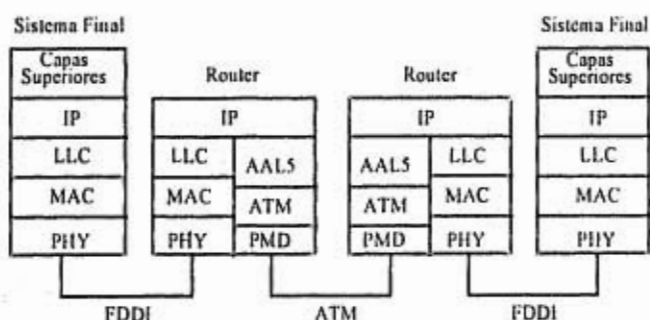


FIGURA 5.3 FUNCION QUE DESEMPEÑA EL ADAPTADOR

Mientras que el uso de bridges (puentes) MAC remotos es una estrategia apropiada para proveer comunicación dentro de una organización única. La facilidad del direccionamiento jerarquico de ruteo permite la comunicación entre LAN's de diferentes organizaciones, lo cual puede usar diferentes protocolos de capa MAC. Entonces este adaptador no intenta extender las redes FDDI, pero si incorporar éstas dentro de la comunidad Internet sobre una red ATM, así el uso de un ruteador es completamente justificado.

5.2.2 ESTRUCTURA FUNCIONAL DEL ADAPTADOR FDDI-ATM

El nivel de adaptación ATM provee muchos puntos de acceso, los cuales son apropiados para diferentes tipos de servicio, retomando la información proporcionada en el capítulo 4 de este trabajo, AAL1 para emulación de circuitos, AAL2 para conexiones con velocidad variable, AAL3/4 para realizar transferencia de datos y AAL5 para una comunicación de datos simple y eficiente.

Para el tráfico de redes LAN Ambas capas de adaptación AAL3/4 y AAL5 son aplicables. Pero hemos escogido AAL5 para este trabajo porque AAL3/4 usa muchos campos de encabezado, los cuales no tienen una aplicación clara en este ambiente, mientras que AAL5 realiza satisfactoriamente los requerimientos de este trabajo.

FDDI incluye una capa LLC/SNAP porque esta tecnología esta basada sobre un ambiente de medio compartido. Mientras que ATM no incluye tal capa debido a que a cada servicio le es asignado un canal virtual exclusivo. La estructura funcional del adaptador FDDI-ATM se muestra en la figura 5.4.

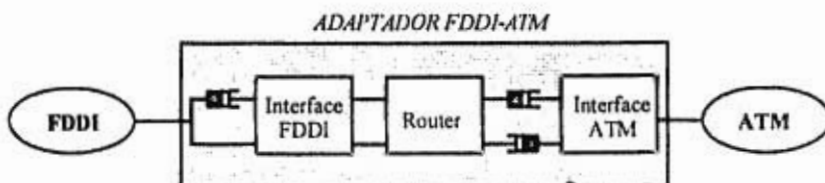


FIGURA 5.4 ESTRUCTURA FUNCIONAL DEL ADAPTADOR FDDI-ATM

Interface FDDI: Este modulo selecciona tramas FDDI direccionadas hacia el adaptador y les quita los encabezados MAC.

Router: Este modulo quita los encabezados LLC/SNAP para obtener la UDP IP (Unidad de Datos de Protocolo), este modulo también busca por cual canal virtual será transmitido el paquete IP, esto se hace buscando en una tabla indexada por el campo de dirección destino.

Interface ATM: Este modulo añade el trailer AAL5 a el UDP IP y genera el flujo de celdas sobre el canal virtual correspondiente a la velocidad acordada.

La interface entre el router y la interface ATM consiste de una área de memoria, donde el router almacena paquetes. El router indica para cada paquete, la interface de este en la interface de memoria y el canal virtual sobre el cual debe ocurrir la transmisión ATM. El modulo ATM segmenta el paquete en un flujo de celdas de quien la velocidad pico es contratada por el usuario. Los adaptadores accesan a la red ATM a través de un enlace fisico de 150 Mbps, el cual es equivalente a 354k celdas por seg. $354000 \times 53 \times 8 \approx 150$ Mbps.

5.2.3 ENCAPSULACION DE TRAMAS FDDI EN CELDAS ATM

Debería ser fácil entender como AAL5 puede usarse para encapsular un datagrama IP, y así, transferirlo a través de la red ATM. En la forma más sencilla, un emisor establece un circuito virtual permanente o conmutado a través de la red ATM hacia una computadora destino y especifica que el circuito utiliza AAL5. Entonces el emisor puede pasar un datagrama IP completo hacia AAL5 para entregarlo a través del circuito. AAL5 genera un remolque, divide el datagrama en celdas y transfiere las celdas a través de la red. En el lado del receptor, ALL5 reensambla el datagrama, utiliza la información en el remolque para verificar que los bits no hayan sido alterados o se hayan perdido y transfiere el resultado hacia el IP (figura 5.5).

En la sección 4.4.4 de esta tesis señalamos que AAL5 utiliza un campo de longitud de 16 bits, lo que hace posible enviar 64k de octetos en un sólo paquete. A pesar de la capacidad de AAL5, TCP/IP restringe el tamaño de los datagramas que pueden enviarse en una red ATM.

CAPITULO V. INTEGRACION DE REDES FDDI A TRAVES DE ATM

El estándar impone un límite de 9180 octetos¹ por datagrama. Esto es, el IP impone una MTU² de 9180 en las redes ATM. Como en el caso de cualquier interfaz de red, cuando un datagrama es mayor que el MTU de la red, el IP fragmenta el datagrama y transfiere cada fragmento hacia AAL5. Así, AAL5 acepta, transfiere y entrega datagramas de 9180 octetos o menos.

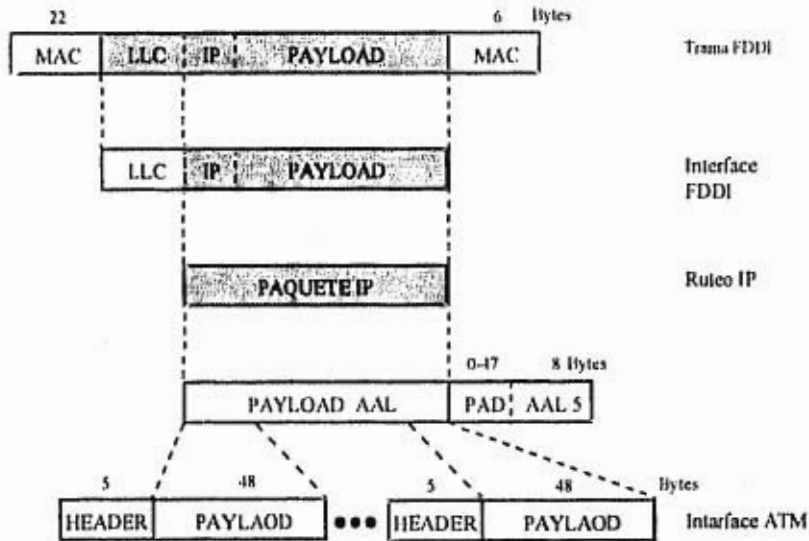


FIGURA 5.5 ENCAPSULACION DE TRAMAS FDDI EN CELDAS ATM

¹ El tamaño de 9180 fue seleccionado para hacer compatible ATM con una tecnología anterior llamada Switched Multimegabit Data Service (SMDS)

² (Maximum Transfer Unit) La mayor cantidad de datos que se puede transferir por unidad a través de una red física dada. El MTU lo determina el hardware de la red.

5.3 TCP/IP EN REDES ATM

5.3.1 INTRODUCCION

En el capítulo 3 se explicaron partes fundamentales del conjunto de protocolos TCP/IP y se muestra como los componentes operan en redes LAN y WAN convencionales de conmutación de paquetes, este capítulo explora cómo TCP/IP, que fue diseñado para redes sin conexión, puede utilizarse en una tecnología utilizada a la conexión, como ATM.

En secciones posteriores, se explica la relación entre ATM y TCP/IP. Se muestra como se relacionan las direcciones de host ATM con las direcciones de host IP. Se describe una forma modificada del protocolo de resolución de direcciones (ARP) utilizado para resolver una dirección IP hacia una conexión ATM y una forma modificada de RARP.

5.3.2 MAPEO DE DIRECCIONES IP EN UNA RED ATM

La asignación de direcciones IP puede ser difícil, debido a que, como en otras tecnologías de red, ATM asigna a cada computadora conectada una dirección física que puede emplearse cuando se establece un circuito virtual. Por un lado, como las direcciones físicas de ATM son más grandes que las direcciones de IP, una dirección física ATM, no puede ser codificada dentro de una dirección IP. Así, el IP no puede utilizar la asignación de direcciones estáticas para redes ATM. Por otro lado, el hardware ATM no soporta la difusión. Por lo tanto, el IP no puede utilizar el ARP convencional, que analizamos en el capítulo 3, para asignar direcciones en ATM.

Las tecnologías de conmutación orientadas a la conexión complican aún más la asignación de direcciones porque requieren dos niveles de asignación. En primer lugar, cuando crean un circuito virtual sobre el que serán enviados los datagramas, las direcciones IP de los destinos deben transformarse en direcciones de puntos extremos ATM. Las direcciones de puntos extremos se usan para crear un circuito virtual.

CAPITULO V. INTEGRACION DE REDES FDDI A TRAVES DE ATM

En segundo lugar, cuando se envía un datagrama a una computadora remota en un circuito virtual existente, las direcciones IP de dos destinos se deben transformar en el par VPI/VCI para el circuito. El segundo direccionamiento se utiliza cada vez que un datagrama es enviado en una red ATM; el primer direccionamiento es necesario sólo cuando un host crea su SVC (Circuito Virtual Conmutado).

Formato de paquetes ATMARP

Como con una ARP convencional, un emisor forma una solicitud que incluye las direcciones de hardware y los emisores IP y ATM, así como la dirección IP de un destino para el que es necesaria una dirección de hardware ATM. El emisor transmite entonces la solicitud hacia el *servidor* ATMARP para la subred lógica. Si el servidor conoce la dirección de hardware ATM, envía una réplica ATMARP. De otra forma, el servidor envía una réplica ATMARP negativa. La figura 5.6 ilustra el formato de un paquete ATMARP

0		7		15		23		31	
TIPO DE HARDWARE (0013)				TIPO DE PROTOCOLO (0800)					
SEND HLEN (20)		SEND HLEN2 (0)		OPERACION					
SEND PLEN (4)		TAR HLEN (20)		TAR HLEN2 (0)		TAR PLEN (4)			
DIRECCION ATM DEL EMISOR (octetos 0-3)									
DIRECCION ATM DEL EMISOR (octetos 4-7)									
DIRECCION ATM DEL EMISOR (octetos 8-11)									
DIRECCION ATM DEL EMISOR (octetos 12-15)									
DIRECCION ATM DEL EMISOR (octetos 16-19)									
DIRECCION DEL PROTOCOLO DEL EMISOR									
DIRECCION ATM DEL DESTINO (octetos 0-3)									
DIRECCION ATM DEL DESTINO (octetos 4-7)									
DIRECCION ATM DEL DESTINO (octetos 8-11)									
DIRECCION ATM DEL DESTINO (octetos 12-15)									
DIRECCION ATM DEL DESTINO (octetos 16-19)									
DIRECCION DEL PROTOCOLO DEL DESTINO									

FIGURA 5.6 FORMATO DE UN PAQUETE ATMARP EN EL QUE SE UTILIZAN 20 OCTETOS PARA LAS DIRECCIONES ATM, COMO LO RECOMIENDA EL FORUM ATM

Como lo muestra la figura, ATMARP modifica ligeramente el formato del paquete ARP. El mayor cambio comprende cambios de longitud y dirección adicional para adaptarse a las direcciones ATM. Para entender el cambio se debe mencionar que han sido propuestas varios formatos de direcciones para ATM, y que no aparece una sola forma que se defina como estándar.

Las compañías telefónicas que ofrecen redes públicas ATM se valen de un formato de 8 octetos donde cada dirección es un número telefónico ISDN definido por el estándar ITU-TS en el documento E.164. En contraste el Forum ATM permite que cada computadora conectada con una red ATM privada sea asignada a 20 octetos una dirección NSAP (Network Service Access Point). Así, se necesita una dirección jerarquizada en dos niveles para especificar una dirección E.164 para una localidad remota y una dirección NSAP de un host en un conmutador local en la localidad.

Para adaptarse a varios formatos de dirección y a una jerarquía de dos niveles, un paquete ATMARP contiene dos campos de longitud para cada dirección ATM así como un campo de longitud para cada dirección de protocolo. Como se muestra en la figura 5.6, el primero de los campos sigue el mismo formato que una ARP convencional. El campo con el nombre *HARDWARE TYPE* contiene el valor hexadecimal 0013 para ATM, y el campo con el nombre *PROTOCOL TYPE* contiene el valor hexadecimal 0800 para IP.

Como el formato de direcciones del emisor y el destino pueden diferir, cada dirección ATM requiere un campo de longitud. El campo *SEND ILEN* especifica la longitud de la dirección ATM del emisor y el campo *SEND ILEN2* especifica la longitud de la subdirección ATM del emisor.

Los campos *TAR LEN* y *TAR LEN2* especifican la longitud de la dirección ATM del destino y de su subdirección. Por último los campos *SEND PLEN* y *TAR PLEN* especifican la longitud de las direcciones de protocolo del emisor y el receptor.

Aparte de los campos de longitud en el encabezado, un paquete ATMARP contiene seis direcciones, los primeros tres campos de dirección contienen la dirección ATM del emisor, la subdirección ATM y la dirección del protocolo. Los tres últimos campos contienen la dirección ATM del destino, la subdirección ATM y la dirección del protocolo.

En el ejemplo de la figura 5.6, tanto los campos de longitud del emisor como el destino contienen 0, y el paquete no contiene octetos para subdirecciones.

Formato de los campos de longitud de dirección ATM

Dado que ATMARP está diseñado para utilizarse con E.164 o direcciones NSAP de 20 octetos, el campo que contiene una longitud de dirección ATM incluye un bit que especifica el formato de dirección. La figura 5.7 ilustra como ATMARP codifica el tipo de dirección y la longitud en el campo de 8 bits.

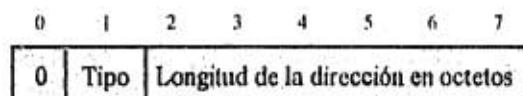


FIGURA 5.7 CODIFICACION DE UN TIPO DE DIRECCION ATM EN UN CAMPO DE 8 OCTETOS, EL BIT 1 DISTINGUE LOS DOS TIPOS DE DIRECCIONES ATM

Un sólo bit codifica el tipo de dirección ATM pues sólo se dispone de dos formas posibles. Si el bit 1 contiene cero, la dirección tiene un formato NSAP y si el bit 1 tiene un calor de uno, la dirección esta en el formato E.164.

Códigos de operación utilizados con el protocolo ATMARP

Quando una computadora envía un paquete ATMARP, debe establecer el código del campo **OPERATION** para especificar el tipo de asignación. La tabla 5.1 muestra los valores que puede emplearse en el campo **OPERATION** de un paquete ATMARP.

Código	Significado
1	Solicitud ATMARP
2	Réplica ATMARP
8	Solicitud ATMARP inversa
9	Réplica ATMARP inversa
10	Acuse de recibo negativo ATMARP

TABLA 5.1 POSIBLES VALORES EN EL CAMPO OPERATION EN UN PAQUETE ATMARP

5.3.3 UTILIZACIÓN DE PAQUETES ATMARP PARA DETERMINAR LA DIRECCIÓN

Realizar la asignación de direcciones para el hardware orientado a la conexión es ligeramente más complicado que para el hardware sin conexión. Dado que el hardware ATM soporta dos tipos de circuitos virtuales se analizarán los dos casos:

Circuitos Virtuales Permanentes (PVC)

En este tipo de conexión, un administrador de red debe configurar cada PVC. Así, a menos que la información de direcciones haya sido configurada en el host (esto es, almacenada en disco), el host no tiene conocimiento de las direcciones IP o de las direcciones ATM de la computadora a las que se conecta un PVC.

El protocolo *Inverse ATMARP* es el que resuelve el problema de encontrar una dirección cuando se emplea PVC. Para utilizar el protocolo, una computadora debe conocer cada uno de los circuitos virtuales permanentes que han sido configurados. Para determinar las direcciones IP y ATM de un punto remoto extremo, una computadora envía un paquete de solicitud *Inverse ATMARP*, cada vez que llega una solicitud en un PVC el receptor genera una réplica *Inverse ATMARP*. Tanto la solicitud como la réplica contienen la dirección IP del emisor y la dirección ATM. Así, una computadora en cada extremo de la conexión aprende la asignación para la computadora ubicada en el otro extremo.

Circuitos Virtuales Conmutados (SVC)

Dentro de una subred IP lógica (LIS), las computadoras crean circuitos virtuales conmutados en función de la demanda. Cuando una computadora A necesita enviar un datagrama a la computadora B y no existe en ese momento un circuito para B, A utiliza la señalización ATM para crear el circuito necesario. Así, A comienza con la dirección IP de B, la cual debe ser transformada en una dirección ATM equivalente. Decimos que cada LIS tiene un servidor *ATMARP* y todas las computadoras en una LIS deben ser configuradas de manera que estas tengan conocimiento acerca de como alcanzar al servidor (esto es, una computadora puede tener un PVC al servidor o la dirección ATM del servidor almacenada en disco).

Un servidor no forma conexiones hacia otras computadoras; el servidor únicamente espera que las computadoras en la LIS se pongan en contacto. Para transformar direcciones IP en direcciones ATM, la computadora A debe tener un circuito virtual abierto para el servidor ATMARP de la LIS. La computadora A forma un paquete de solicitud ATMARP y lo envía sobre la conexión hacia el servidor.

Un servidor ATMARP mantiene una base de datos de las transformaciones de las direcciones IP en las direcciones ATM. el servidor forma una réplica ATMARP y llena la dirección ATM que corresponde a la dirección IP de destino. Como en un ARP convencional, el servidor intercambia las entradas del emisor y del destino antes de regresar la réplica a la computadora que envió la solicitud.

Si el servidor no conoce la dirección ATM que corresponde a la dirección IP del destino en una solicitud, el servidor devuelve un acuse de recibo negativo.

5.4 ESTUDIO TECNICO Y ECONOMICO PARA LLEVAR A CABO LA IMPLEMENTACION DE ESTE PROYECTO.

5.4.1 ADAPTADOR FDDI-ATM

Como parte fundamental de este proyecto se ha elegido como el adaptador FDDI-ATM a un producto de alto desempeño y gran estandarización como es el Cisco 7000.

Las series 7000 y 7500 de Cisco soportan cualquier combinación de Ethernet, Fast Ethernet, FDDI, Token Ring, Seriales de hasta 8 Mbps, T1/E1, X.25, Frame Relay, ISDN PRI y ATM hasta 155 Mbps. Estas interfaces están contenidas en tarjetas procesadoras de interfaz, las cuales proveen una conexión directa entre el bus (o buses) de alta velocidad del Cisco y las redes externas. Todos los procesadores de interfaz son modulares y las tarjetas que miden 11 x 14 pulgadas pueden contener uno o mas conectores de interfaz de red. Todos los procesadores de interfaz pueden ser insertados o reemplazados sin interrumpir la energía del sistema (en caliente) y sin tener que introducir comandos de consola.

CAPITULO V. INTEGRACION DE REDES FDDI A TRAVES DE ATM

El sistema operativo Cisco IOS es el mismo software que corre en todas las líneas de routers Cisco. Este permite soportar de manera confiable todos los protocolos de red estandarizados, entre los cuales están: TCP/IP, SPX/IPX de Novell Netware, PPP, Apple Talk, DECnet, Banyan Vines, HDLC, SDLC, NetBios, SNA y APPN.

Para la comunicación entre routers puede activar RIP, IGRP, EIGRP y OSPF, entre otros. Además, es compatible con los ambientes de redes switcheadas y Virtual LAN (VLAN). En el emergente mundo ATM es capaz de brindar los servicios necesarios para el ATM LAN Emulation.

Algunas de las características generales del Ruteador Cisco 7000 se listan a continuación:

Ancho de banda: 0.5 Gbps
Slots para interfaces: 5
Manufactura: NEC (OEM para Cisco Systems)
Unidad Central de Procesamiento: M68040 (25 Mhz)
Memoria: 16 Mbytes
Máximo Consumo de Potencia: 700 W
Dimensiones: 489 x 445 x 614 mm, 68 Kg.

Numero de Redes Conectadas:

Ethernet: 30 max
Token Ring: 20 max
FDDI: 5 max
RS449: 20 max
RS232C: 20 max
X.21: 20 max
V.35: 20 max

La figura 5.8 muestra la vista posterior del equipo Cisco 7000

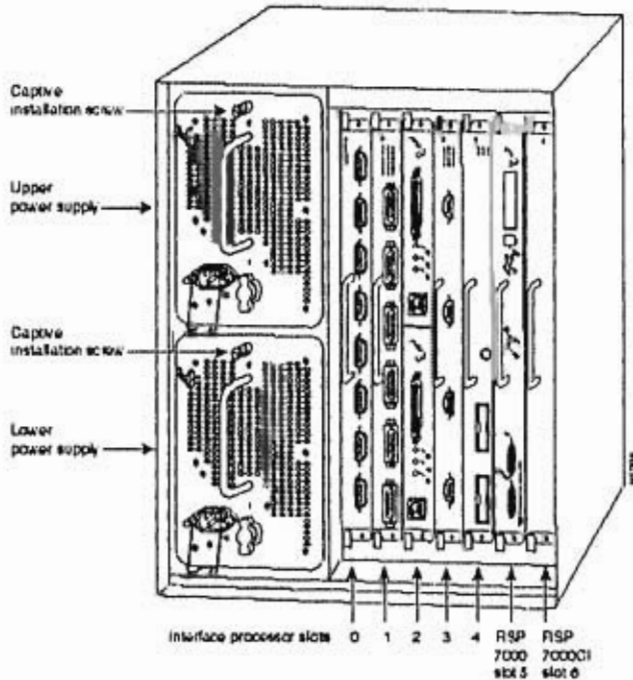


FIGURA 5.8 VISTA POSTERIOR DEL CISCO 7000

Algunos procesadores de interfaz consisten de solo una tarjeta madre, mientras que otros consisten de una tarjeta madre y de una tarjeta adicional que funciona como un módulo de interfaz de capa física (PLIM) o un adaptador de puerto. Por ejemplo, la AIP (ATM Interface Processor) que se muestra en la figura 5.9 necesita un PLIM, el cual determina el tipo de conexión ATM.

AIP

La AIP provee una interfaz nativa ATM para el Cisco 7000. La AIP esta disponible con un puerto y puede soportar los siguientes medios:

CX-AIP-SM: SONET con Fibra Óptica multimodo

CX-AIP-SS: SONET con Fibra Óptica monomodo

CX-AIP-E3: E3 con Cable Coaxial

CX-AIP-DS3: DS3 con Cable Coaxial

CX-AIP-TM: 155 Mbps con Fibra Multimodo

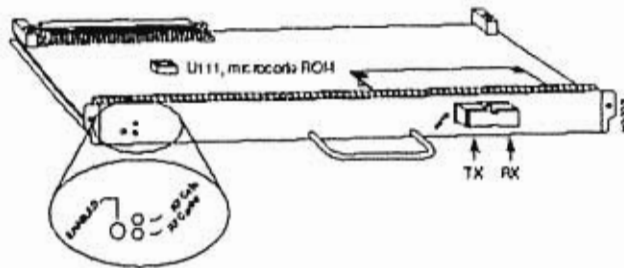


FIGURA 5.9 PLIM O ADAPTADOR DE PUERTO

FIP

La FIP (FDDI Interface Processor) provee un puerto de alta velocidad (100 Mbps) FDDI. Cuatro tipos de FIP se encuentran disponibles:

CX-FIP-MM: Multimodo a Multimodo con Bypass Óptico

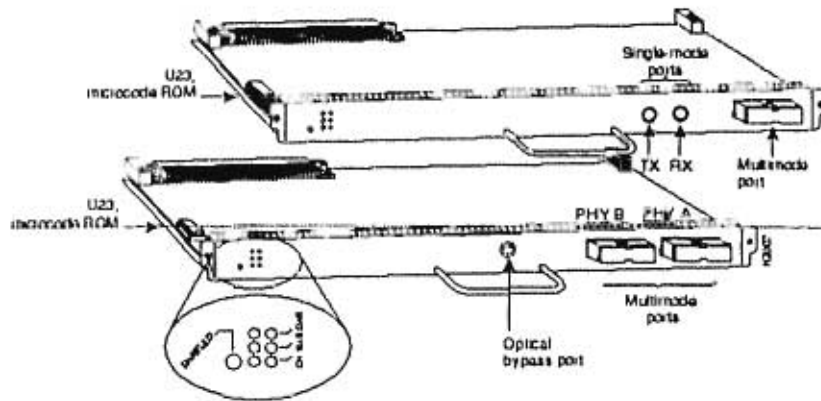
CX-FIP-MS: Multimodo a Monomodo

CX-FIP-SM: Monomodo a Multimodo

CX-FIP-SS: Monomodo a Monomodo con Bypass Óptico

La figura 5.10 muestra la interface FDDI conocida como FIP

CAPITULO V. INTEGRACION DE REDES FDDI A TRAVES DE ATM



LA FIGURA 5.10 INTERFAZ FDDI CONOCIDA COMO FIP

Algunos otros procesadores que se pueden insertar en el Cisco 7000 son:

CIP2: Conexiones de Mainframes compatibles de IBM

EIP: Procesador de Interfaz Ethernet

FEIP: Procesador de Interfaz Fast Ethernet (1 o 2 puertos)

FSIP: Procesador de Interfaz de Puertos Seriales (4 u 8)

HIP: Procesador de Interfaz HSSI (1 puerto)

MIP: Provee un multiplexaje multicanal de Nx64 y/o Nx56 a velocidades de 2 Mbps o 1.5 Mbps respectivamente

SMIP: Provee 2 canales T1 o 2 E1 para conexiones seriales

SSIP: Procesador de Interfaz de Estándares Seriales, Provee 8 puertos seriales de alta velocidad (Arriba de 8 Mbps)

TRIP: Procesador de Interfaz Token Ring (2 o 4 puertos)

A continuación se presenta una cotización en dólares del equipo necesario en cada punto terminal del enlace ATM:

CAPITULO V. INTEGRACION DE REDES FDDI A TRAVES DE ATM

CANT	DESCRIPCIÓN	PRECIO UNITARIO	IMPORTE
1	RUTEADOR MULTIPROTOCOLO MARCA CISCO SYSTEM MOD. 7000 CON 6 SLOTS DE EXPANSIÓN, UNA FUENTE DE PODER, MODULO PROCESADOR CON 2 CYBUS Y ROUTE SWITCH PROCESOR	\$ 19,900.00	\$ 19,900.00
1	OPCION CON 2 FUENTES DE PODER PARA CISCO 7000	\$ 6,000.00	\$ 25,900.00
1	MODULO ATM 155 MBPS PARA 7500 MARCA CISCO SYSTEM CX-AIP-TM	\$ 22,000.00	\$ 47,900.00
1	INTERFAZ FDDI MULTIMODO CX-FIP-MM	\$ 18,000.00	\$ 65,900.00
1	SOFTWARE IOS VS 11.0 1 ENTERPRISE PARA 7500	\$ 4,000.00	\$ 69,900.00
		SUBTOTAL.	\$ 69,900.00
	GASTOS DE IMPORTACIÓN 6%		\$ 4194.00
		TOTAL	\$ 74,094.00

5.4.2 RED ATM

Para la elección de la red ATM que se usará para este proyecto no se tienen muchas opciones para elegir. De tal forma que a la fecha, una sola compañía tiene el soporte necesario para llevar a cabo este proyecto. Red de fibra óptica Avantel

Avantel cuenta ya con una red de fibra óptica instalada en la república mexicana. La columna vertebral de esta red esta formada también por equipos Cisco 7000. La figura 5.11 muestra en forma esquemática la cobertura de esta red en su fase 1.

Desgraciadamente aún no se tiene una cotización para rentar un enlace ATM sobre esta red, esto debido a que esta red aunque ya está inontada aún no se está operando, y no se pueden proporcionar costos debido a técnicas de mercadotecnia

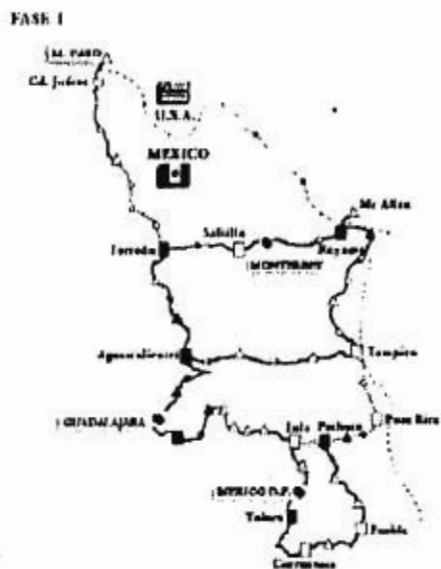


FIGURA 5.11 COBERTURA DE LA RED AVANTE EN LA PRIMERA FASE

CONCLUSIONES

Durante el desarrollo de este trabajo de tesis hemos expuesto conceptos importantes sobre diferentes tecnologías, tanto existentes y consolidadas en este país, como por ejemplo, Ethernet y FDDI. Así como nuevas tecnologías con un amplio desarrollo como ATM.

De esta manera los primeros capítulos de esta tesis comprenden conceptos indispensables para la implementación de redes de telecomunicaciones digitales y a la vez tratamos de exponer las principales limitantes que presentan las tecnologías de redes actuales.

Así el principal objetivo de este trabajo es plantear una propuesta de integración de redes FDDI, a través de una red ATM, la cual resuelve la mayoría de las desventajas que presentan las redes existentes.

Por ejemplo, actualmente Red UNAM contrata canales E1 dedicados vía RDI, para varios enlaces en la red metropolitana, estos canales presentan el inconveniente de que son tarifados sin importar la carga de tráfico en el enlace. Por el contrario una red ATM aprovecha al máximo los recursos, esto debido a que el ancho de banda es asignado en base a la demanda de los puntos terminales.

Otra de las desventajas de los actuales enlaces E1 RDI consiste en que es un enlace punto a punto, por lo que, una falla en este enlace provocaría la pérdida del mismo. Mientras que la propuesta que hacemos de usar una red ATM ofrece la posibilidad de realizar una conmutación en caso de una falla.

Además los enlaces E1 tienen un ancho de banda muy limitado (2 Mbps), por lo que no alcanzan a satisfacer la creciente demanda de ancho de banda. Así este trabajo propone el uso de ATM. Esta tecnología es capaz de proporcionar una mayor gama de ancho de banda (hasta 622 Mbps o más). Al conseguir esta escalabilidad, el eterno problema de "cuellos de botella" en redes WAN puede ser descartado.

Otro factor importante de este análisis es el uso de equipo que plantea una infraestructura para incorporar otras tecnologías tales como Frame Relay, Fast Ethernet, X.25, E1, etc.

Al termino de este trabajo de tesis podemos concluir que definitivamente es posible llevar a cabo la implementación de este proyecto, debido a que se cuenta con el equipo necesario para la interconexión de anillos FDDI y lo único que faltaría es la autorización, por parte del gobierno, para que empresas como Avantel, la cual ya cuenta con la infraestructura, puedan ofrecer el servicio de red ATM al público. Esta autorización se espera que sea para el año 1997, por lo que esperamos que esta investigación no se quede sólo en papel y pueda ser desarrollada en México, ya que en otros países de Europa, con los cuales estuvimos en contacto vía e-mail, proyectos de este tipo se encuentran operando.

Por lo anterior el presente trabajo representa una eficaz y eficiente guía de consulta debido a que reúne información actualizada y detallada, de la cual no se encuentra suficiente bibliografía disponible.

Además puede usarse como una excelente herramienta para la integración e implementación de redes de datos en el campo profesional.

BIBLIOGRAFIA

1. ALBERT, BERNHARD
FDDI AND FDDI II
Architecture, Protocols and Performance
Artech House, 1994
2. BELLAMY, JOHN
DIGITAL TELEPHONY
Second Edition
John Wiley & Sons, 1990
3. BLACK, UYLESS
REDES DE COMPUTADORAS
Protocolos, Normas e Interfaces
Macrobit Editores, 1990
4. BOISSEAU, M.
HIGH SPEED NETWORKS
John Wiley & Sons, 1994
5. COMER, E. DOUGLAS
INTERNETWORKING WITH TCP/IP
Principles, Protocols and Architecture, Vol I 2a. Edition
Prentice Hall, 1991
6. COMER, E. DOUGLAS
REDES GLOBALES DE INFORMACION CON INTERNET Y TCP/IP
Principios Básicos, Protocolos y Arquitectura
Prentice Hall, 1996
7. FLANAGAN, WILLIAM
ATM Asynchronous Transfer Mode
User's Guide
Flatiron Publishing, Inc. Book, 1994

8. GORALSKI, WALTER
ATM
The Future of High-Speed Networking
Computer Technology Research Corp. 1994
9. HOPPER & TEMPLE
DISEÑO DE REDES LOCALES
Addison-Wesley Iberoamericana, 1994
10. JAIN, RAJ
FDDI HANDBOOK
High-Speed Networking Using Fiber and Other Media
Addison-Wesley Publishing Company, 1994
11. KESSLER & TRAIN
METROPOLITAN AREA NETWORKS
Concepts, Standards and Services
McGraw-Hill, Inc. 1991
12. KUMAR, BALAJI
BROADBAND COMMUNICATIONS
A Professional's Guide to ATM, Frame Relay, SMDS, SONET, and B-ISDN
McGraw Hill Series on Computer Communications, 1994
13. MARTIN, JAMES
LOCAL AREA NETWORKS
Architectures and Implementations, Second Edition
Prentice Hall, 1994
14. MAZZAFERRO, JOHN F.
FDDI VS ATM
High Speed Networks
Computer Technology Research Corp. 1994
15. McDYSAN & SPOHN
ATM
Theory And Application
McGraw Hill Series on Computer Communications, 1995

16. MILLER, MARK A.
ANALIZING BROADBAND NETWORKS
Frame Relay, SMDS, ATM
M & Y Books, 1994
17. MILLER, MARK A.
INTERNETWORKING
A Guide to Network Communications LAN to LAN; LAN to WAN.
M & T Books, 1991
18. MILLER, MARK A.
LAN PROTOCOL HANDBOOK
M & T Books, 1990
19. MILLS, ANDREW
UNDERSTANDING FDDI
A 100 Mbps Solution For Today's Compare LANs
Prentice-Hall, 1995
20. PARKER, TIM
APRENDIENDO TCP/IP EN 14 DIAS
Prentice Hall, 1995
21. PATRIDGE, CRAIG
GIGABIT NETWORKING
Addison-Wesley Publishing Company, 1994
22. SCHATT, STAN
UNDERSTANDING ATM
Computer McGraw-Hill, 1996
23. STALLINGS WILLIAM
DATA AND COMPUTER COMMUNICATIONS
Macmillan Publishing Company, 1985

24. STALLINGS, WILLIAM
DATA AND COMPUTER COMMUNICATIONS
Fourth Edition
MacMillan Publishing Company, 1994
25. STALLINGS, WILLIAM
LOCAL AND METROPOLITAN AREA NETWORKS
Fourth Edition
Macmillan Publishing Company, 1993
26. STALLINGS, WILLIAM
NETWORKING STANDARDS
A Guide to OSI, ISDN, LAN and MAN Standard
Addison-Wesley Publishing Company, 1985